



VALTIOVARAINMINISTERIÖ

VALTION TIETOHALLINNON INTERNET-TIETOTURVALLISUUSOHJE

1/2003



VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

VALTION TIETOHALLINNON INTERNET-TIETOTURVALLISUUSOHJE

1/2003

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

VALTIOVARAINMINISTERIÖ

Snellmaninkatu 1 A
PL 28
00023 VALTIONEUVOSTO

Puhelin

(09) 160 01

Telefaksi

(09) 160 33123

Internet

www.vm.fi

Julkaisun tilaukset

Puh. (09) 160 33287

Taitto

VM/Viestintä

ISSN 1455-2566

ISBN 951-804-383-3

Editä Prima Oy
HELSINKI 2003



Ministeriöille, virastoille ja laitoksille

VALTION TIETOHALLINNON INTERNET-TIETOTURVALLISUUSOHJE

Valtiovarainministeriö antaa oheisen tietoturvallisuusohjeen (jäljempänä ohje), joka on laadittu valtiovarainministeriön asettaman Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI-toimesta. Ohjeen valmistelussa on otettu huomioon ohjelunokseen saadut noin 50 lausuntoa. Ohje korvaa valtiovarainministeriön aiemmin antaman Internetin käyttöä ja tietoturvallisuutta koskevan suosituksen (VAHTI 1/1998) ja täydentää laajaa olemassa olevaa valtionhallinnon tietoturvallisuusohjeistoa (www.vm.fi/vahti).

Ohjeen on tarkoitus olla apuvälineenä Internet-käytön ja Internetissä tarjottavien palveluiden tietoturvallisen toteutuksen ohjauksessa, suunnittelussa, valvonnassa, itse toteutuksessa ja myös näihin liittyvissä hankinnoissa. Ohjeen pääasiallisena kohderyhmänä ovat organisaation tietohallinto- ja tietoturvallisuustehtävissä toimivat. Ohjeessa keskitytään Internet-verkon ja sen tietoturvallisuuden keskeisiin asioihin. Ohjeen keskeisen sisällön muodostavat varsinkin Internetin käytön tietoturvallisuuden ohjeistus (luku 3), Internet-verkon ja sen infrastruktuurin kuvaus (luku 2) sekä näitä lukuja täydentävät liitteet.

Ohjeen kohdealueen ja siihen liittyvien tietoturvallisuusasioiden voimakkaan kehityksen johdosta on tärkeätä, että hallinnon organisaatiot edelleen jatkavat ja tehostavat Internetin käyttöön liittyvää tietoturvallisuuden varmistamista ja kehittämistä. Tässä korostuvat mm. jatkuva luonteinen, ennakoiva ja ohjeistuksen mukainen tietoteknisen tason tietoturvallisuustyö sekä organisaation henkilökunnan Internet-käytön tietoturvallisuusasiat.

Asiakirja tulee valtion tietoturvallisuuden johtoryhmän Internet-sivuille, jotka ovat osoitteissa www.vm.fi/vahti ja www.vm.fi/tietoturvallisuus.

Ohjetta kehitetään tarvittaessa mm. saatavan palautteen pohjalta. Palautteen voi toimittaa valtiovarainministeriön hallinnon kehittämisosastolle (hko@vm.fi). Lisätietoja antaa neuvotteleva virkamies Mikael Kiviniemi (Mikael.Kiviniemi@vm.fi).

Alivaltiosihteeri Juhani Turunen

Ylijohtaja Jorma Karjalainen

1	JOHDANTO	7
1.1	Ohjeen laatimisen tausta	7
1.2	Ohjeen tarkoitus, kohderyhmä ja rajaus	8
1.3	Ohjeen rakenne ja käyttöohje	8
2	TEKNINEN INTERNET-INFRASTRUKTUURI JA TIETOTURVALLISUUS	11
2.1	Verkon rakenne	11
2.1.1	Internetin fyysinen rakenne	12
2.1.2	Internetin tekninen toteutus ja perusprotokollat	14
2.1.3	Tietoliikenneportit	16
2.1.4	Internetin reititys	18
2.1.5	Nimipalvelu	20
2.2	Sovellusprotokollat	21
2.3	Perusohjelmistot ja palvelut	23
2.3.1	Selaimet	23
2.3.2	WWW-palvelinohjelmistot	25
2.3.3	Perusohjelmistojen tietoturvanäkökohtia	26
2.4	Internet-verkon ja sen käytön haavoittuvuuksista	27
2.5	Yleisiä tietoturvaratkaisuja	29
2.5.1	Tunnistaminen, todentaminen ja pääsynvalvonta	29
2.5.2	Tietoliikenteen salaus	33
2.5.3	Haittaohjelmien torjunta	35
2.5.4	Palomuuuri	37
2.5.5	Tunkeutumisen havainnointijärjestelmä	40
3	INTERNET-VERKON KÄYTTÖTAVAT JA NIIDEN TIETOTURVALLINEN TOTEUTUS	43
3.1	Lähtökohdat	43
3.1.1	Lainsäädännölliset lähtökohdat	43
3.1.2	Internetin käytön tietoturvapoliikka	44
3.2	Tietoliikenneyhteys Internet-verkkoon	45
3.2.1	Palvelimen liittäminen verkkoon	46
3.2.1.1	Järjestelmän käyttöönoton suunnittelu	47
3.2.1.2	Käyttöjärjestelmän sekä varusohjelmiston asentaminen ja vahventaminen	48
3.2.1.3	Sovellusten turvallinen asentaminen	49
3.2.1.4	Seuranta	50
3.2.1.5	Dokumentointi	54
3.2.1.6	Varmistukset	54

3.2.1.7 Testaus	55
3.2.1.8 Ylläpito	56
3.2.2 Palomuurin tietoturvallisuus	57
3.2.2.1 Topologia-, sovellus- ja protokollatarpeiden selvitys	59
3.2.2.2 Palomuuriratkaisun arviointi ja laitteen/tuotteen valinta	60
3.2.2.3 Palomuurin asentaminen	60
3.2.2.4 Palomuurisäännöstö	62
3.2.2.5 Palomuuuri osana verkon suojaustoimenpiteitä	64
3.3 Internetistä saatavien palveluiden käyttäminen	65
3.3.1 Tietojen haku ja muiden palveluiden käyttö	65
3.3.2 Asioiminen ja ostaminen Internetissä	66
3.4 Internetissä tarjottavat palvelut	67
3.4.1 Asiointipalvelut	71
3.5 Internetin käyttö organisaatioiden väliseen ja sisäiseen tiedonsiirtoon	74
3.6 Sähköposti ja muut viestintäsovellukset	76
3.6.1 Sähköpostin luottamuksellisuus ja salaus	79
3.6.2 Sähköpostin palveluosoitteista	80
3.6.3 Ei-toivottu kaupallinen viestintä	81
3.6.4 Muista viestintäsovelluksista	82
LIITE 1 Henkilökunnan Internet-käytön tietoturvaohjeen malli	83
LIITE 2 Palvelimen asennusohje	89
LIITE 3 Verkon seuranta- ja hallintatyökalut	93
LIITE 4 Internet-protokollien suojaaminen	95
LIITE 5 Lyhenteitä ja käsitteitä	97
LIITE 6 Lähteitä	103
LIITE 7 Valtiovarainministeriön ja VAHTIn tietoturvallisuusohjeistoa	105

1 JOHDANTO

1.1 Ohjeen laatimisen tausta

Valtionvarainministeriön asettama ja vetämä valtionhallinnon tietoturvallisuuden johdoryhmä (VAHTI) perusti 15.4.2002 valmisteluryhmän päivittämään Valtion Internetin käyttö- ja tietoturvallisuussuosituksen (1/1998) uudeksi Internetin käytön tietoturvallisuusohtjeeksi. Tarve ohjeen uusimiselle oli tullut teknisen kehityksen, Internetin käytön yleistymisen ja Internetissä tarjottavien palveluiden monipuolistumisen myötä.

Ohjeen laatineen työryhmän kokoonpano oli seuraava:

Timo Tuomaila	Verohallitus puheenjohtaja
Aaro Hallikainen	Poliisin tietohallintokeskus
Risto Heinonen	Tietosuojavaltuutetun toimisto
Kimmo Helaskoski	Pääesikunta
Kauto Huopio	Viestintävirasto
Jouko Raatikainen	Valtionvarainministeriö
Kaisu Rahko	Oulun yliopisto
Seppo Sundberg	Väestörekisterikeskus
Seppo Vilhonen	Sosiaali- ja terveysministeriö

Konsulttityöstä vastasivat:

Tuija Kohonen	Stonesoft Finland Oy (17.1.2003 alkaen Nixu Oy) sihteeri
Jarkko Rautala	Stonesoft Finland Oy (17.1.2003 alkaen Nixu Oy)

VAHTI linjasi ohjeen sisältöä ja jatkovalmistelua kokouksessaan maaliskuussa 2003. VM pyysi laajasti lausuntoja ohjeluonnokseen keväällä 2003 ja ohjeeseen saatiin 43 lausuntoa, joiden pohjalta ohjetta kehitettiin. VAHTI linjasi viimeistelyä kokouksessaan 12.6.2003 ja tämän pohjalta viimeisteltiin lopullinen versio.

1.2 Ohjeen tarkoitus, kohderyhmä ja rajaus

Ohjeen tarkoitus on olla apuvälineenä Internet-käytön ja Internetissä tarjottavien palveluiden tietoturvallisen toteutuksen ohjauksessa, suunnittelussa, valvonnassa, itse toteutuksessa ja tarvittaessa myös esim. näihin liittyvissä hankinnoissa. Ohjeen pääasiallinen kohderyhmä on valtionhallinnon organisaation tietohallinto ja sen asiantuntijat, mutta ohjeessa on osia joista voi olla hyötyä myös muissa tehtävissä toimiville henkilöille.

Ohjeen sisällössä on aiheen laajuuden vuoksi keskitytty Internet-verkon ja siihen liittyvien tekniikoiden tietoturvallisuuden kannalta keskeisiin asioihin ja ratkaisutapoihin. Yleisiä suunnittelumenetelmiä tai tietoturvallisuuden hallintamenetelmiä ohjeessa ei ole kuvattu. Näistä löytyy tietoa mm. muusta VAHTI:n ohjeistosta. Muissa VAHTI:n ohjeissa on myös monilta osin tarkempaa tietoa esimerkiksi tietyistä uhkatyypeistä (haittaohjelmat, tietoturvaloukkaukset) tai yksittäisten käyttötapojen tai sovellusten (esim. sähköinen asiointi/ palvelut, sähköposti) tietoturvanäkökohdista. Näihin on joissakin tekstikodissa viitattu lisätietolähteenä.

Ohjeessa on keskitytty pääasiassa niiden lisäuhkien hallintaan, joita Internetin erilaiset käyttötavat tuovat tullessaan valtionhallinnon tietojen käsittelylle. Ohjeen lähtökoh- ta on, että sisäverkon tietoturvallisuuden oletetaan perusturvallisuuden osalta olevan kunnossa, joten siihen puututaan tässä yhteydessä vain vähän. On kuitenkin syytä muistuttaa, että Internet-tekniikoita käytetään nykyään laajasti myös sisäverkkojen järjestelmissä, joten ulkoisen rajapinnan hallinnan on tästäkin syystä oltava kunnossa ja Internet-tekniikoiden käyttö nähtävä kokonaisuutena.

Tietoturvallisuutta sivuavan lainsäädännön osalta on pyritty huomioimaan varsinkin niitä säännöksiä, jotka koskevat Internetiin liittyviä ilmiöitä.

1.3 Ohjeen rakenne ja käyttöohje

Ohje on keskeiseltä sisällöltään jaettu kahteen osaan.

Internet-verkko, sen perusinfrastruktuuri, peruspalvelut ja ohjelmistot ovat käyttäjä (organisaatio)n kannalta ulkoapäin annettu tosiasia, johon oma toiminta on sovitettava, koska maailmanlaajuista verkkoa ja sen toimintaperiaatteita ei voi käyttäjän toimesta muuttaa. Luvussa kaksi (2) käsitellään tätä ympäristöä, Internet-verkkoa ja siihen liittyviä tekniikoita palvelujen käyttö- ja tarjoamiskanavana kuvaamalla melko laajasti verkon tietoturvaominaisuuksia niin, että niiden tiedostaminen ja ymmärtäminen voi olla eri käyttötapojen tietoturvallisen toteuttamisen pohjana.

Luku kolme (3) on pääasiassa varsinainen ohjeisuus, jossa esitetään ratkaisuja ja toimintaohjeita turvallisen Internetin käytön toteuttamiseksi. Jotta esim. lainsäädännön vaatimukset toteutuvat Internetiä hyödyntävän valtionhallinnon organisaation toiminnassa on sen kyettävä toteuttamaan käytön edellyttämät tietoturvalliset tekniset ja muut riskien hallinnan ratkaisut. Tietohallinnon on myös kyettävä avustamaan organisaation johtoa tietoturvaluuteen liittyvissä linjaratkaisuissa.

Ohjeen liitteenä on joitakin teknisempiä kuvauksia tai listoja suojaustoimenpiteistä sekä lista niistä asioista, joihin Internet-käytön loppukäyttäjän ohjeen tulisi ottaa kantaa. Loppukäyttäjän ohje, samoin kuin organisaation tietoturwapolitiikka Internet-käytön suhteen ovat aina organisaatiokohtaisia asioita, joiden yksityiskohdat ratkeavat, kun organisaation toiminnalle ja voimavaroille mitoitettut ratkaisut on (toivottavasti myös tätä ohjetta soveltaen) hyvän suunnitteluprosessin tuloksena löydetty.

2 TEKNINEN INTERNET-INFRASTRUKTUURI JA TIETOTURVALLISUUS

Tässä luvussa käydään läpi asioita, jotka tulee tuntea ja ottaa huomioon Internet-yhteyksiä ja eri käyttötapoja suunniteltaessa ja käyttöönotettaessa.

Internetin perusrakenne koostuu Internet-runkoverkosta, siihen liittyvistä laitteista ja eri organisaatioiden aliverkosta. Internet-verkon perusrakenne ei sisällä valmiina läheskään kaikkia tietoturvallisuuden kannalta tarvittavia ominaisuuksia. Verkon ominaisuudet eivät suojaa verkon käyttäjää salakuuntelua, vääränä henkilönä esiintymistä tai tietomurtoa vastaan.

Internet muodostuu toisistaan riippumattomista verkkoon kytketyistä palvelimista, reitittimistä ja muista tietoliikennelaitteista sekä näiden avulla toteutetuista, useiden tietoliikenneyhteyksien tarjoajien toteuttamista peruspalveluista. Tietoliikenneyhteyksien tarjoajien verkkolaitteet muodostavat yhdessä Internetin runkoverkon. Koska Internet-arkkitehtuuri on luonnostaan autonomisesti laajennettava, voi kuka tahansa alkaa teletoimintaa ohjaavan lainsäädännön puitteissa tarjoamaan palveluita Internetissä.

2.1 Verkon rakenne

Internet on vikasietoinen verkko, joka sai alkunsa Yhdysvaltojen puolustushallinnon rahoittamana tutkimushankkeena, jossa pidettiin tärkeänä tietoliikenteen ja tiedonvälityksen toimivuutta, vaikka yksi tai useampi tietoliikennekomponentti ei toimisikaan.

2.1.1 Internetin fyysinen rakenne

Internet-runkoverkko on maailmanlaajuinen reitittimien ja niiden välisten tietoliikenneyhteyksien verkko. Reitittimet vastaanottavat tietoliikennepaketteja ja välittävät niitä omien reititaulutietojensa perusteella edelleen seuraavalle reitittimelle, toivottavasti kohti oikeaa vastaanottajaverkkoa. Lisäksi verkossa on palvelinkoneita kuten nimipalvelimia, sähköposti- ja WWW-palvelimia.

Verkolla ei ole yhtä omistajaa, vaan se koostuu toisiinsa kytketyistä, tietoliikenneoperaattoreiden ja muiden tietoliikennepalvelutarjoajien (ISP, Internet Service Provider) itsenäisesti hallinnoimista verkoista, joissa nämä vastaavat runkoverkon muodostavien siirtokanavien ja reitittimien toiminnasta.

Internet-runkoverkko yhdistää organisaatioiden lähiverkot ("inter-net") ja yksityisten kotikäyttäjien tietokoneet näiden valitseman palvelutarjoajan kautta. Lähiverkkojen liikennöintitekniikka on yhteensopiva runkoverkon kanssa, verkkolaitteisto on periaatteessa sama ja erot ovat lähinnä verkkojen fyysisessä siirtotiessä ja reititysprotokollissa.

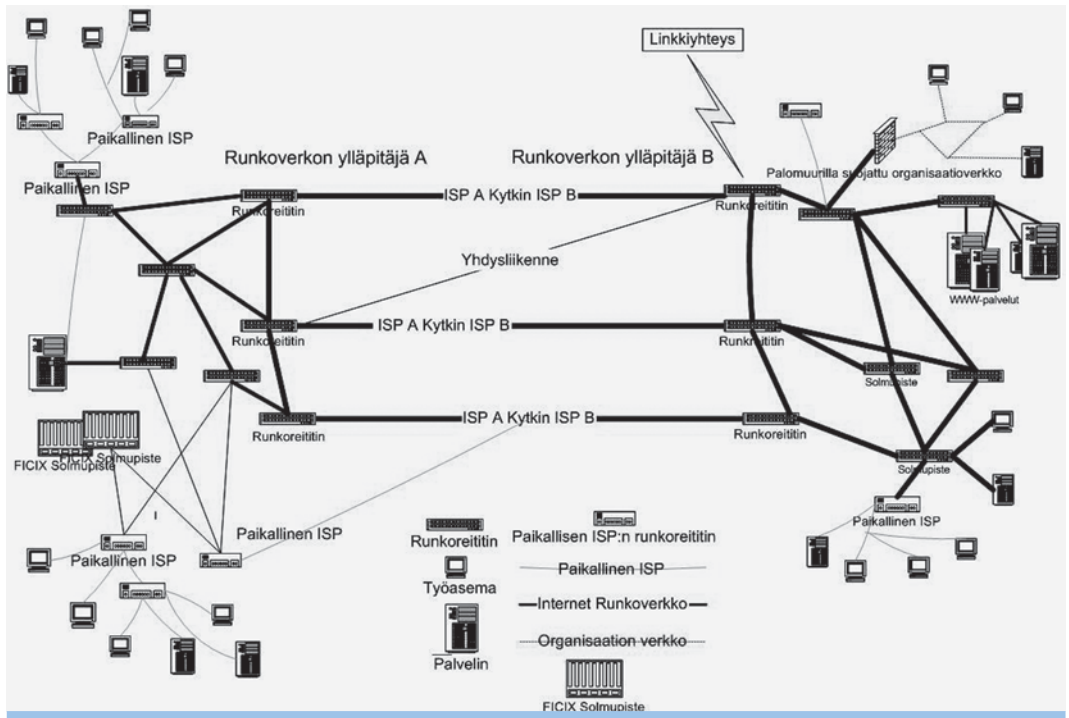
Yleisesti Internet-verkolla tarkoitetaan kaikkia liikenneyhteyksiä, palvelimia ja palveluita, mitä oman organisaation tai kotikoneiden ulkopuolelta Internet-liikennöintitekniikalla tavoitetaan, sekä palveluita, joita organisaatio tarjoaa omasta verkostaan sen ulkopuolella oleville Internet-käyttäjille. Näin laskien Internet koostuu miljoonista tietokoneista, sadoista tuhansista organisaatioiden verkoista, noin kymmenestä tuhannesta verkkopalvelutarjoajan (ISP) verkosta sekä yli kymmenestä verkon ns. liikenteenvaihtopisteestä ja niiden välisten yhteyksien ylläpitäjästä.

Organisaatioiden verkot liittyvät Internetiin oman reitittimen kautta. Palomuri ja sen yhteydessä oleva organisaation verkon julkinen osa (eteisverkko) ovat nykyään verkon käytön perusturvallisuuteen kuuluvia.

Suomessa operaattorien verkot kohtaavat FICIX-solmupisteissä, jotka helpottavat liikennöintiä Suomessa. Toiminnasta vastaa FICIX ry (Finnish Communication and Internet Exchange), jonka jäsenet ovat tietoliikenneoperaattoreita tai tarjoavat vastavia palveluita asiakkailleen. Operaattoreilla on kullakin omat runkoverkkonsa ja niistä yhteys sekä kansainvälisiin liikenteenvaihtopisteisiin että asiakkaidensa lähiverkkoihin.

Internet-runkoverkon siirtotienä käytettävät valokaapelit kulkevat yleensä maassa ja mannerten välillä merenpohjassa, lisäksi joissain tapauksissa yhteydet hoidetaan satelliittien välityksellä. Toimintahäiriöiden (fyysisen kaapelin tai satelliittiyhteyden katkeaminen, solmupisteessä toimivan operaattorin toimintahäiriö) varalta ja liikennekapasiteetin riittävyyden vuoksi tärkeimmille Internet-runkoverkkoyhteyksille on rakennettu rinnakkaisia ja vaihtoehtoisia reittejä käyttäviä varaväyliä.

Kuva 1. Esimerkki Internetin fyysisestä rakenteesta



Internet yhteyksiä jatketaan organisaatioissa erilaisilla langattomilla ratkaisuilla. Esimerkiksi GPRS-verkkojen (General Packet Radio System) yleistyessä niiden käyttö tulee riittävän suuren siirtokykynsä vuoksi yhä käyttökelpoisemmaksi organisaatioille. Liikkuvaan käyttöön organisaatioiden sisäverkkojen toimialueella käytetään lisäntyvästi langattomia yhteyksiä, WLAN-verkkoja (Wireless LAN), jotka ovat turvattomia ilman erillisiä suojaustoimenpiteitä. Myös organisaatioiden yhteisiä WLAN-verkkoja on käytössä¹.

¹ Langattomat yhteydet mahdollistavat myös sijaintitietojen teknisen käsittelyn, jolloin yhä lisääntyvässä määrin joudutaan ottamaan huomioon myös sijaintitietojen käsittelyn tietosuojaa. Tähän otetaan kantaa Sähköisen viestinnän tietosuojalakesityksessä.

2.1.2 Internetin tekninen toteutus ja perusprotokollat

Internetissä tapahtuvaa tiedonvälitystä protokollatasolla voidaan kuvata vertaamalla kansainvälisen standardointiorganisaatio ISO:n OSI-referenssimallia TCP/IP-protokollaperheeseen (kuva 2).

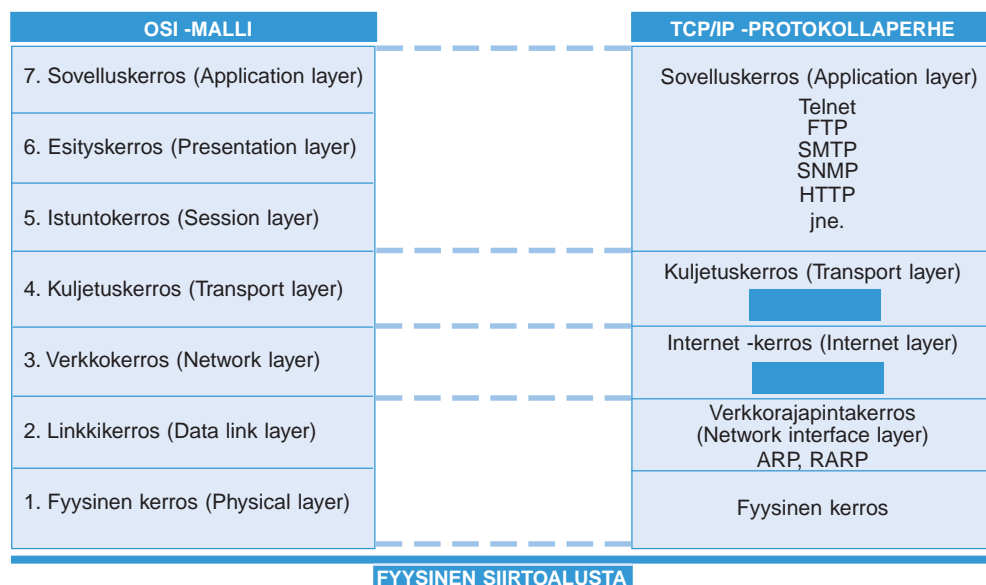
Teknisesti Internet-verkon toteutus jakautuu dataa siirtäviin protokolleihin ja niiden päällä oleviin sovellusprotokolleihin. Kokonaisuutta kutsutaan TCP/IP-protokollaperheeksi (Transmission Control Protocol/Internet Protocol).

TCP/IP -protokollaperheen alemman tason protokollat tarjoavat sovelluksia yhdistäviä TCP-yhteyksiä ja sovellusten välisiä yhteydettömiä UDP-tietosähkeitä (User Datagram Protocol). Näiden päälle rakennetaan varsinaisia sovelluksia.

Internet-verkko itsessään (eli reitittimet ja niitä yhdistävät tietoliikenneyhteydet) siirtää verkossa olevien koneiden välillä IP-tietoliikennepaketteja (Internet Protocol). IP-paketin alussa on määrämuotoinen otsikkokenttä, jossa on kentät vastaanottajan ja lähettäjän numeerisille IP-osoitteille sekä muuta tietoa. Otsikkokentän jälkeen tulee IP-tason näkökulmasta dataa, käytännössä ylemmän tason protokollan otsikkokenttä.

IP-paketin sisällä kulkevissa paketeissa kuljetetaan TCP- tai UDP-protokollan tietoliikennepaketteja. TCP-protokolla (Transmission Control Protocol) toimii ylemmän tason sovellusprotokollien kuljetustienä. TCP hoitaa tässä yhteydessä muun muassa

Kuva 2. OSI-malli vs. TCP/IP-protokollaperhe



Kuva 3. IP-paketin rakenne



vuonohjauksen, uudelleenlähettykset ja satunnaisien virheiden aiheuttamien tiedon eheysongelmien tarkistamisen.

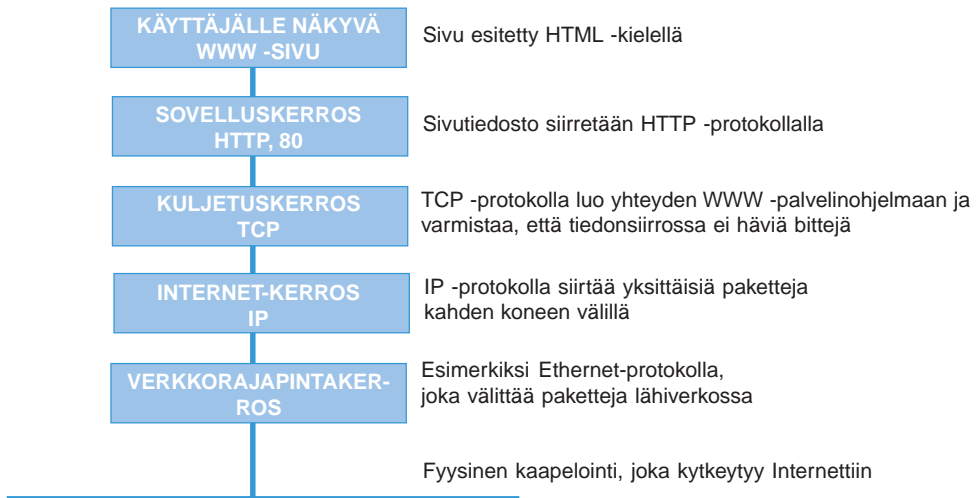
UDP-protokolla välittää yhteydettömiä tietosähkeitä sovellusten välillä. Se soveltuu yksinkertaisimpiin tarpeisiin, kuten DNS-nimipalvelun (Domain Name Service) tietokantakyselyihin. UDP-protokollaa käytetään tänä päivänä yhä enenevässä määrin myös reaaliaikaisten jatkuvien tapahtumien kuten esimerkiksi audio- ja videomateriaalin lähettämiseen verkoissa. Näitä UDP-paketteja hallinnoidaan RTP-protokollan (Real-Time Transport) avulla.

Paketit ovat sisäkkäisiä ja toimivat eri loogisilla tasoilla. Jokaisella tasolla lisätään pakettiin loogisen tason otsikkotietoja, jotka sitten puretaan kerroksittain tarvittavalle tasolle asti reititettäessä pakettia kohti kohdeosoitetta. Esimerkiksi, kuten kirje kuoressaan kulkee osan matkaa postisäkissä, joka puolestaan kuljetetaan lentokoneessa tai junassa. Kuvassa 4 on esitetty kuinka eri protokollat tarjoavat palveluja seuraavalle protokollakerrokselle. Kuvan esimerkissä käyttäjä hakee tietoa Internetistä käyttäen WWW-selainta.

Internet-protokollien ominaisuuksia ei ole suunniteltu tunnistukseen eikä todennukseen, joten niistä tulee huolehtia sovellustasolla.

Tässä dokumentissa IP-protokollalla tarkoitetaan IP-protokollan versiota neljä (IPv4), joka on vielä yleisesti käytössä. IPv4-protokollan tietoturvaluutteita on korjattu IP-protokollan versiossa kuusi (IPv6), joka on ollut kehitteillä jo useita vuosia. IPv6-tuki sisältyy yhä useamman valmistajan laite- ja ohjelmistotuotteisiin. IPv6-liikennöintiä testataan useissa verkoissa, mutta IPv6:n yleistä käyttöönottoa ei voida vielä arvioida.

Kuva 4. Eri protokollatasoja WWW -käytössä



IPv6-protokolla tarjoaa useita parannuksia tietoturvallisuuteen, mm.:

- Laajentaa osoiteavaruuden 32 bitistä 128 bittiin, jolloin osoiteavaruuden riittämättömyysongelma poistuu.
- Hallitsee vuon ja datan priorisoinnin, joiden avulla voidaan parantaa siirtovarmuutta ja nopeuttaa kriittisiä palveluita.
- Tarjoaa verkkokerrokselle parempia tietoturvaominaisuuksia, mm. eheystarkistukset.
- Tarjoaa välineitä verkkojärjestelmien automaattiseen asettamiseen
- Joukkolähetykset (Anycast), joiden avulla voidaan lähettää sama viesti vain kerran.
- Sisältää tuen IPSec-salaukselle.

2.1.3 Tietoliikenneportit

IP-protokolla välittää tietoliikennepaketteja koneiden välillä. Palvelinkoneissa on kuitenkin liki aina useita eri palveluita ja työasemistakin voi tyypillisesti olla useampia samanaikaisia yhteyksiä avoinna. Tämän takia sovellukset eivät käytä IP-protokollaa suoraan, vaan TCP- ja UDP-protokollan kautta. Nämä protokollat puolestaan tuovat mukaan koneen sisäisen osoiteabstraktion, jota kutsutaan portiksi.

TCP/IP:n portti on abstrakti käsite, jonka avulla TCP- ja UDP-protokollat pystyvät tunnistamaan eri kohdesovellukset samassa laitteessa, ei mikään fyysinen osa tietokoneessa. Jokaisella portilla on oma 16-bittinen numero. Tiettyjä porttinumeroita on periaatteessa varattu sovittuun käyttöön, esimerkiksi WWW-palvelun on sovittu käyttävän porttinumeroa 80, joten useimmat WWW-palvelimet varaavat käynnistyessään portin numero 80 itselleen ja jäävät odottamaan yhteydenottoja. Selainohjelmat ottavat sitten oletusarvoisesti yhteyden tähän porttiin käyttäjän antaessa koneen nimen osoitteeksi. UDP- ja TCP-protokollien porttinumeroavarauudet ovat erilliset, joskin käytännössä yleensä synkronoidut. Porttinumeroiden standardoinnista vastaa IANA (Internet Assigned Numbers Authority)². Sovelluksien asentaminen myös epästandardeihin porttinumeroihin on yleensä mahdollista, mutta ei suositeltavaa.

Palvelimissa sovellukset avaavat portteja kuuntelutilaan, jolloin käyttäjät voivat ottaa yhteyden sovellukseen aina tarvittaessa. Useimmat käyttöjärjestelmäsennukset avaavat erilaisia ylimääräisiä porttipalveluja. Kaikki nämä ylimääräiset palvelut tulee asennuksessa kytkeä pois päältä.

Asiakassovellukset (esimerkiksi WWW-selain tai sähköpostipalvelu) avaavat myös portin omassa laitteessaan päästäkseen verkkoon. Ne eivät yleensä käytä mitään sovittua porttinumeroa vaan pyytävät käyttöjärjestelmältä seuraavaksi vapaata porttia. Tyypillisesti asiakassovellukset saavat käyttöönsä vain porttinumerosta 1023 suurempia portteja.

Kaikki IP-protokollan päällä kulkevat protokollat eivät käytä portteja. Esimerkiksi ICMP-protokolla (Internet Control Message Protocol), jota käytetään verkon sisäisen hallintainformaation välitykseen, ei käytä portteja. Tyypillisimpiä ICMP-viestejä ovat virheilmoitukset (kuten reitittimen lähettämä tieto siitä, että koneeseen, johon yritettiin saada yhteyttä, ei ole mahdollista saada yhteyttä) ja ohjausviestit (kuten ping-ohjelman käyttämä echo-request/echo-reply -pyyntö). Nämä ovat laitteiden, ei sovellusten välistä yhteydenpitoa.

Verkkohyökkäyksissä ICMP-viestejä käytetään muun muassa erilaisiin palvelunesto-
hyökkäyksiin (DoS). Erään tällaisen hyökkäyksen tarkoituksena on tukehduttaa kohdeverkko ICMP-kaikuvastauksiin. Näin kohdeverkko ei enää kuin vastaamaan virheellisesti massaväärennettyihin ICMP-kaikupyntöihin. ICMP-pakettien (kuten ping) kokoa voidaan myös suurentaa ja näiden liian suurten IP-pakettien käsittely voi kaa-
taa koko laitteen.

² IANA määrittelemät tietoliikenneportit löytyvät listattuna osoitteesta www.iana.org/assignments/port-numbers.

Tietoliikenneturvallisudessa tulee huolehtia turvallisuudesta jokaisessa protokollatasolla, jotta tunkeutuja ei voi hyödyntää ns. alemman tason tietoturvaongelmia tunkeutumiseensa. Esimerkiksi organisaatio on huolehtinut sovellustasolla tietoliikenneturvallisuudesta ohjelmistollisesti, mutta IP-tason viestien, kuten ohjausviestit, annetaan kulkea palvelimelle kontrolloimattomina.

2.1.4 Internetin reititys

Fyysinen Internet-verkko koostuu reitittimistä tai tietokoneista ja niitä yhdistävistä tietoliikennedyhteyksistä. Reitittimet välittävät IP-paketteja siten, että ne vertaavat vastaanottamansa IP-paketin vastaanottajan osoitetietoja reititystaulukkoonsa ja lähettävät sitten IP-paketin seuraavalle reitittimelle.

Reitityspalvelu on Internetissä tärkeä palvelu, koska ilman toimivaa reititystä Internet ei toimi. Jotta IP-pakettien reititys olisi mahdollista, niin jokaisella lähettäjällä ja vastaanottajalla tulee olla yksilöivä tunniste. IP-pakettien IP-osoitteet ovat tällaisia. Erityisesti IP-osoitteissa käytetyt 32-bittiset numerot mahdollistavat sen, että ympäri maailmaa olevat IP-verkkojen laitteet pystyvät kommunikoimaan keskenään. Reitittämisessä on myös oleellista verkkopeitto (mask), joka kertoo verkon peittoalueen. Esimerkiksi, jos C-luokan verkossa ei tarvita kaikkia osoitteita voidaan se jakaa pienempiin verkkoalueisiin verkkopeitteiden avulla. Tällöin verkon 192.168.1.0/25 tarkoittaa verkkoa, jonka verkko-osoite on 192.168.1.0 ja broadcast-osoite on 192.168.1.127.

IP-osoite jaetaan kahteen osaan. Ensimmäinen osa määrittelee verkko-osoitteen ja toinen määrittelee palvelimen osoitteen. Postikorttianalogiaa käyttäen IP-osoitteen rakennetta voidaan kuvata seuraavasti:

Palvelimen osoite = Matti Meikäläinen, 3 A 9

Verkko-osoite = Mannerheimintie 200, Helsinki, Suomi

Alla olevassa kuvassa IPv4 –paketin rakenne ja sisältö on kuvattu tarkemmin.

Kuva 5. IP -paketin rakenne

Versio esim. IP v4	Otsikon pituus	Palvelu (TOS = Type of Service)	Paketin pituus	Paketin tunnistus (identifi- cation)	Liput (Flags)	Lohkon sijainti (Frag- ment offset)	Elinaika (TTL= Time to Live)	Proto- kolla esim. TCP tai UDP	Otsikon takistus- summa	Lähet- täjän IP -osoi- te	Vastaan- ottajan IP -osoi- te	DATA
--------------------------	-------------------	--	-------------------	---	------------------	---	---------------------------------------	--	-------------------------------	------------------------------------	--	------

Reitittimet muodostavat reititystauluja ja säilyttävät niissä reititystietoja, joiden mukaan ne toimivat, jos tietoliikennepaketti ei kuulu lähiverkon alueelle. Lähiverkkokyseyissä fyysiset laitteet tiedustelevat saman verkon muiden laitteiden verkkokorttien MAC-osoitteet (Media Access Control) ARP-toiminnolla (Address Resolution Protocol). Vastaavasti RARP-toiminnolla (Reverse Address Resolution Protocol) laite kysyy IP-osoitetietojaan reitittimeltä tai ARP-palvelimelta. Useissa organisaatioissa on käytössä DHCP-palvelu (Dynamic Host Configuration Protocol), jonka avulla työasemat kytkeytyvät verkkoon ja saavat automaattisesti osoitteensa. Tällöin hyödynnetään myös ARP- ja RARP-protokollia.

Runkoverkon reitittimien reititystaulut ovat yleensä dynaamisia, eli reitittimet vaihtavat tietoa keskenään siitä, millaisiin IP-osoitteisiin ne pystyvät välittämään paketteja. Dynaamisesti reitittyvä verkko pystyy automaattisesti konfiguroimaan itsensä kiertämään virhetilanteet aikaviiveellä.

Operaattoreiden asiakkaiden tiloihin asentamat reitittimet ovat yleensä staattisesti konfiguroituja. Esimerkiksi tietoliikenneoperaattorin asiakkaan tiloihin sijoittama reititin tietää tyypillisesti lähiverkkoliittymässä olevan verkon osoitteen (esim. 192.168.16.0/24) ja kaikkiin muihin osoitteisiin lähetetyn liikenteen se ohjaa runkoverkon suuntaan. Staattista reititystä käytetään muun muassa tietoturvasyistä. Dynaamisesti reitittyvä verkko on altis väärälle reititystiedolle, jonka avulla liikenne voitaisiin ohjata väärään paikkaan. Reititystietoja muuttavat esimerkiksi krakkerit, jotka haluavat aiheuttaa kiusaa organisaation tietoliikenteelle.

Erilaisia reititysprotokollia on useita, kuten esimerkiksi RIP (Routing Information Protocol) ja OSPF (Open Shortest Path First). Osa näistä protokollista osaa automaattisesti reitittää paketteja uudelleen, jos tietoliikenneyhteyksissä esiintyy häiriöitä. Tällaisten protokollien lisäksi on kehitetty tietoliikennepalvelutarjoajien välille BGP-protokolla (Border Gateway Protocol, jonka avulla verkkopalveluntarjoajat vaihtavat reititystietoja varmistaakseen yhteyksien jatkumisen vikatapauksissa.

Reitittimet eivät käsittele paljoakaan korkeamman tason sovellusprotokollia, kuten esimerkiksi SMTP-protokollaa (Simple Mail Transfer Protocol). Yleensä reitittimissä on yksinkertaisia tietoturvaominaisuuksia, kuten IP-pakettien hylkääminen lähettäjän osoitteen, kohdeosoitteen tai portin numeron (protokollan) perusteella.

Reitittimien tietoliikennerajoitukset perustuvat pääsynvalvontalistoihin. Pääsynvalvontalistoilta säädelään, mistä ja mihin verkkopalveluihin sallitaan liikennettä sisä- ja ulkoverkon välillä. Pääsynvalvontalistoilta voidaan myös estää sisäverkon osoitteiden väärentäminen lähdeosoitteeksi ulkoverkosta tulevaan liikenteeseen eli väärennettyjä IP-lähdeosoitteita ei sallita.

Reitittimien lisäksi verkkojen rakentamiseen käytetään kytkimiä ja yhdyskäytäviä. Kytkimet pystyvät hallinnoimaan siihen kytkettyjä verkkoja omina loogisina osinaan ja ehkäisemään näin verkkojen näkyminen toisilleen. Lisää turvallisuutta saadaan käyttämällä erillisiä verkkojen yhdyskäytäviä, kuten palomureja.

Internetin dynaamisuudesta johtuen ei tietoliikennepakettien kulkureittejä aina tiedetä ja niiden reitityksien selvittäminen jälkikäteen on lähes mahdotonta.

2.1.5 Nimipalvelu

Nimipalvelu (Domain Name Service, DNS) on toinen tärkeä Internet-palvelu. Nimipalvelun avulla nimet muutetaan numeerisiksi IP-osoitteiksi ja tarvittaessa osoitteet nimiksi. Esimerkiksi nimi `www.vn.fi` muutetaan IP-osoitteeksi `192.251.241.106`. Samalla logiikalla laitteiden numeeriset IP-osoitteet muutetaan vastaamaan nimiä.

Reititys toimii puhtaasti numeeristen IP-osoitteiden perusteella. Nimipalvelu on suuri hajautettu hierarkkinen tietokanta, jossa koko Internet-nimiavaruus on jaettu pienempiin osiin, nimialueisiin, niiden hallinnan helpottamiseksi. Tietokannan juuresta on varattu kullekin maalle ISO:n kaksikirjaimisen lyhenteen mukainen nimi (fi Suomelle) sekä muita tunnuksia (com, edu, org, net jne.) Näitä nimiä kutsutaan myös nimellä ylimmän tason aluenimet (top level domain)³.

Fi-alueen nimipalvelun hallinnoijana toimii Viestintävirasto (<http://www.ficora.fi/>), joka myöntää organisaatioille niiden aluenimet (domain name). Kukin organisaatio hallitsee omaa haaraansa nimipalvelusta ja voi vapaasti käyttää omaa nimialuettaan. Organisaatiot voivat pyytää myös teleoperaattoreita rekisteröimään aluenimiä ja huolehtimaan organisaation nimipalvelusta.

Nimipalvelussa olevat tiedot sijaitsevat nimipalvelimissa, joista sovellukset niitä tarpeen mukaan kyselevät. Nimipalvelimiin on konfiguroitu maailman juurinimipalvelimien IP-osoitteet kiinteästi. Juurinimipalvelimista saa puolestaan kysytyä tiedon ylimmän tason aluenimistä (Suomen fi-alueella muun muassa `prifi.ficora.fi`, `hydra.helsinki.fi`), jotka puolestaan tietävät organisaatioiden nimipalvelimien osoitteet.

Kutakin nimipalvelualueita palvelemassa tulee olla palvelun tärkeyden takia vähintään kaksi nimipalvelinta, joista yksi on primaaripalvelin (primary server), jossa ylläpidetään ko. alueen tietoja, ja muut ovat sekundaaripalvelimia (secondary server), jotka säännöllisin väliajoin hakevat tietonsa primaaripalvelimelta ja varmistavat nimipalvelun toimivuuden. Samat palvelimet voivat toimia eri alueiden kohdalla primaari- tai

³ Joidenkin erityisesti pienten valtioiden maatunnuksia on myyty kokonaisuudessaan yksityisten yritysten käyttöön.

sekundaaripalvelimen roolissa tarpeen mukaan, järjestelmä on tässä suhteessa varsin joustava.

Pääsääntöisesti maailmalle jaeltavaan julkiseen nimipalveluun kannattaa sijoittaa vain tarvittavat tiedot, yksinkertaisimmillaan WWW-palvelimen osoite, sähköpostipalvelimen osoite ja sähköpostia ohjaavat MX-kentät (Mail eXchanger) sekä nimipalvelussa vaadittavat reverse-tietueet.

Nimipalvelun on otettava vastaan myös sisäverkon nimipalvelukyselyt ja välitettävät ne ulkoverkkoon paljastamatta sisäverkon osoitteita. Sisäiseen nimipalveluun, joka on erillään julkisesta nimipalvelusta, voidaan kirjata organisaation laitteet ja palvelut, organisaation sisäverkon tarpeiden mukaan. Sisä- ja ulkoverkon nimipalvelimilla, pyritään estämään sisäverkon nimi- ja verkkotopologisten tietojen leviäminen mahdollisille ulkopuolisille.

Koska nimipalvelu on ollut järjestelmissä hyvin haavoittuva toiminto, on syytä kiinnittää huomiota nimipalvelun sijaintiin ja asentamiseen. Nimipalvelinta ei tule asentaa minkään muun sovelluksen yhteyteen, vaan sille tulee aina olla oma laitteensa. Sisäinen ja ulkoinen nimipalvelu tulee olla aina erillisiä. Ulkoinen nimipalvelu voidaan ja usein kannattaakin ostaa palveluntarjoajalta. Nimipalvelimet tulee suojata esimerkiksi palomuurin avulla ja aina kannattaa tarkistaa, mille nimipalvelimelle sisäinen nimipalvelin sallii tietojensa välityksen ns. zone transfer toiminnoilla.

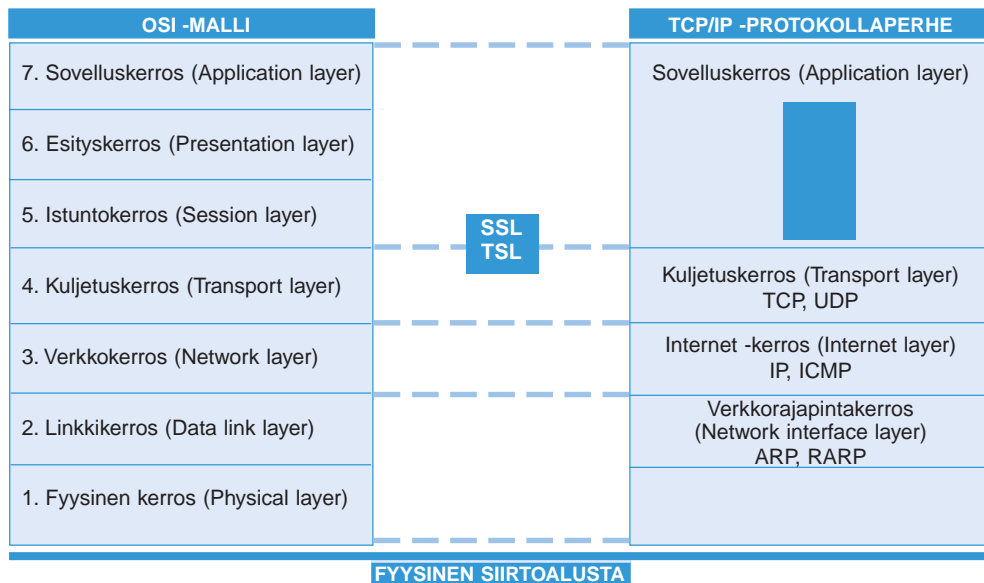
2.2 Sovellusprotokollat

Internetin perusprotokollat (esimerkiksi TCP ja UDP) ja sovellusprotokollat (esimerkiksi Telnet ja HTTP) on alunperin tehty pieneen luotettavaan verkkoympäristöön, jossa oleellista oli protokollien keveys ja vikasietoisuus, samaan aikaan kun käyttäjiin oletusarvoisesti saattoi luottaa.

Internetin ja TCP/IP-protokollaperheen suunnittelussa ei alunperin huomioitu tietoturvallisuutta vaan keskityttiin tietoliikenteen toimivuuden varmistamiseen. Esimerkiksi TCP/IP:in perusprotokollat eivät itsessään tarjoa ratkaisuja luotettavaan käyttäjien, dokumenttien ja eri tietoliikennelaitteiden tunnistamiseen tai tietoliikenteen salaamiseen. Organisaatioiden tulee huomioida TCP/IP-protokollaperheen tietoturvuudet ja ratkaista ongelmat sovellustasolla erilaisilla tietoturvaohjelmistoilla ja -ratkaisuilla. Käyttäjän kannalta valittujen tietoturvaratkaisuiden tulisi olla mahdollisimman helppokäyttöisiä ja läpinäkyviä.

Käyttäjille tarjottavat Internet-palvelut käyttävät sovellusprotokollia rajapintanaan kuljetuskerrokseen. Käyttäjän ei itse tarvitse määritellä käytettävää sovellusprotokollaa. Esimerkiksi sähköpostia käyttäessään käyttäjä näkee sähköpostiohjelmiston käyttö-

Kuva 6. Yleisemmät sovellusprotokollat



liittymän, mutta ei välttämättä tiedä, että ohjelmisto käyttää muun muassa SMTP-sovellusprotokollaa. WWW-palveluissa käytetään HTTP-protokollaa. HTTP-protokolla välittää esimerkiksi käyttäjän tunnistamistiedot selväkielisinä Internetin yli. Ne voidaan suojata käyttämällä SSL/TLS suojattuja yhteyksiä. SSL-protokolla sijoittuu TCP/IP-protokollaperheessä sovelluskerroksen ja TCP/IP-kerroksien väliin. Kuvassa 6 on esitetty yleisimmin käytössä olevat sovellusprotokollat.

Telnet-protokollalla muodostetaan pääteyhteyksiä. Telnet on turvaton protokolla, koska esimerkiksi salasana ja siirrettävä tieto kulkevat tietoliikenneverkossa selväkielisenä. Edellä mainittu tietoturvariski koskee myös FTP-tiedonsiirtoprotokollaa (File Transfer Protocol). Telnet- ja FTP-protokollat ovat haavoittuvaisia yhteyden kaappaamiselle ilman suojaavia protokollia, joiden tilalla voidaan käyttää esimerkiksi SSH:ta.

SNMP-protokolla (Simple Network Management Protocol) käytetään tietoliikenneverkon hallintaan. SNMP:tä käyttämällä voidaan esimerkiksi selvittää tietoliikenneverkoissa oleva vikaantunut laite ja estää tätä häiritsemästä tietoliikenneverkon toimintaa. SNMP käyttää liikennöintiin UDP-protokollaa ja SNMP-protokollan tietoturvasuus uusista versioista huolimatta on heikko.

Sähköpostiliikenteeseen liittyviä sovellusprotokollia kuten SMTP, POP ja IMAP käsitellään luvussa 3.6.

2.3 Perusohjelmistot ja palvelut

Internetissä tiedonvaihtoa tapahtuu monilla sovellusprotokollilla, mutta suurimmaksi osaksi tiedonvaihto tapahtuu WWW-järjestelmää (World Wide Web) käyttämällä. Yksinkertaisimmillaan WWW-järjestelmä muodostuu kahdesta osasta: WWW-palvelimesta ja WWW-selaimista. WWW-palvelin tarjoaa palveluita ja tietoa Internetissä, joi- ta käyttäjä pääsee WWW-selaimella käyttämään.

2.3.1 Selaimet

Selaimesta on muodostunut nykyaikaisen tietojenkäsittelyn peruskäyttöliittymäohjel- mistö, jonka ominaisuuksien ymmärtäminen ja hallinta on organisaation tietoturvalli- suuden kannalta tärkeää varsinkin, kun selain on usein myös tiedoston hallinnan tai tietojärjestelmien käyttöliittymä. Tästä syystä selaimen tietoturvalisuuden hallinta on ajateltava laajemmin kuin pelkästään Internet-käytön kannalta.

Selaimen perusominaisuus on ns. hypertekstidokumenttien suorittaminen siten, että ne ovat kuvaruudulta luettavissa HTML-standardin määrittelemässä muodossa. Se- laimen perustietoturvaominaisuuksiin kuuluu saman alkuperän sääntö, eli se, että eri sivustoilta peräisin tai niiden käsittelyyn liittyvät tiedot (esim. käyttäjän antamat syöt- teet, evästeet) on suojattu muiden sivustojen käsittelyltä. Esimerkiksi silloin, kun se- laimessa on avoinna useita ikkunoita joihin käyttäjä voi antaa syötteitä. Toinen keskei- nen tietoturvaominaisuus on se, että käyttäjän koneelle voi selailun yhteydessä tal- lentua vain tarkoin määriteltyjä tietoja. Selaimen tietoturvalisuudessa huomioitavia seikkoja ovat:

EVÄSTEET

Eväste on tiedosto tai merkkijono, johon sivu tai sivusto voi selailuun liittyen tallentaa haluamiaan tietoja. Eväste voi olla istuntokohtainen, pysyvä tai määräaikainen. Yleen- sä evästeen avulla sivusto muistaa sen koneen, joka on sivua aikaisemmin käsitellyt. Evästeeseen voidaan tallentaa esimerkiksi vaarattomia käyttäjän valitsema sivun ul- koasuun liittyviä profiilitietoja, mutta myös käyttäjän tietosuojan kannalta arveluttavia tietoja. Ongelma on tällöin se, että evästettä ei ole suojattu ulkopuolisilta kiintolevyllä eikä tietoliikenteessä⁴.

⁴ Sähköisen viestinnän tietosuojalakiesityksen mukaan käyttäjän on saatava aina valita tallen- netaanko evästeitä.

VÄLIMUISTIT

Selain tallentaa selaimeen haettuja sivuja työaseman levyllä sivujen mahdollista uudelleenkäyttöä varten, jotta niitä ei tarvitse (kaikilta osin) hakea alkuperäisestä osoitteesta uudelleen. Välimuisti voi olla tietosuojariski yhteiskäytössä olevilla laitteilla. Ainakin asiointijärjestelmissä on syytä ohjeistaa käyttäjää tyhjentämään välimuisti, jos järjestelmää käytetään yhteiskäyttöisessä laitteessa.

Muita vastaavia tallentuvia tietoja voivat olla

- selaushistoria
- käyttäjän tallentamat "suosikit" (bookmarks)
- käyttäjätunnusten/ salasanojen tallennus/ lomakkeiden automaattitallennys

Myös näihin liittyy samankaltaisia tietoturva- ja tietosuojariskejä, joten ko. tiedot on joko oltava suojattuna muilta käyttäjiltä tai niiden poisto tai estäminen on hallittava.

VALINNANVARAISET LISÄOHJELMAT

Selainten asennusvaiheessa on valittavissa joukko lisäominaisuuksia, esimerkiksi selailun graafisiin ominaisuuksiin liittyviä, video-, animaatio-, ääni- ym. tiedostomaattien käsittelyyn tai viestintään liittyviä lisäosia. Näiden lisäosien valinta ja käyttöönotto on syytä tehdä organisaation tietoturvapoliitikan mukaisesti lähtien siitä, millainen tietojenkäsittely on organisaation toiminnan kannalta tarpeellista ja mitä lisäuhkia eri lisäohjelmista voi seurata. Uhkia ovat mm. tietyyntyyppisten haittaohjelmien pääsy verkkoon, tietoliikenteen tukkeutuminen ja väärinkäytökset johtuen käyttäjien puutteellisesta ohjeistamisesta. Esimerkiksi päätöksellä siitä, asennetaanko selaimen yhteydessä tietyt ohjelmakomponentit, voidaan joko mahdollistaa tai estää joidenkin haittaohjelmien toiminta. Joka tapauksessa lisäosien valinta ja asennus on syytä tehdä teknisten asiantuntijoiden toimesta eikä sallia käyttäjien itse ladata ja asentaa lisäohjelmia.

VERKOSTA LATAUTUVAT TOIMINTEET

Pysyvien ohjelmakomponenttien lisäksi tietoturvallisuuden kannalta huomion arvoisia ovat HTML-dokumentteihin sulautetut suoritettavat komponentit. Näiden avulla voidaan esimerkiksi lisätä HTML-dokumentteihin dynaamisia ominaisuuksia. Suoritettavia komponentteja ovat esimerkiksi JavaScriptit, joilla voidaan komentokielityyppisesti käsitellä selaimen oliomallin kautta HTML-dokumentin osia halutulla tavalla. Muita suoritettavia ja latautuvia komponentteja ovat Java-ohjelmat joiden tietoturvaominaisuuksiin kuuluu toiminta "hiekkalaatikon sisällä", jolloin ohjelmalla ei ole pääsyä työaseman kiintolevyllä ja sovellusarkkitehtuuri sisältää luotettavan tietoturvamallin. Suo-

ritettävien komponenttien avulla voidaan suorittaa raskasta ja vaativaakin käsittelyä, kuten erilaisia tietokantahakuja ja tiedostokäsittelyjä. Jollakin suoritusohjelmilla, kuten ActiveX, voidaan suorittaa käyttäjän koneella mitä tahansa tietojen käsittelyä. JavaScript ja Java tarvitsevat toimiakseen erillisen suoritusaikaisen lisäosan.

Latautuvien toimintojen käytön mahdollistamiseen pitää suhtautua erittäin varovaisesti ottaen huomioon:

- tarvitaanko toimintoja joissakin tilanteissa
- voidaanko niiden alkuperä todentaa esim. sähköisillä allekirjoituksilla
- voidaanko käyttö konfiguroida antamalla käytölle lisäehtoja, esim. käyttäjän hyväksyntä tai riittävän luotettava alkuperän todennus

Lähtökohtana voidaan pitää, että muiden kuin JavaScriptin salliminen vaatii erityisiä perusteluja sekä käytölle että selvitystä ja tietoutta siitä, miten käyttöön liittyvät riskit hallitaan.

2.3.2 WWW-palvelinohjelmistot

Internet-käyttö perustuu nykyään pitkälti WWW-järjestelmiin. WWW on maailmanlaajuinen hypermediaverkosto, joka koostuu palvelimista ja niihin talletetuista hypermediadokumenteista. Nämä HTML-kielellä (HyperText Markup Language) koodatut tiedostot voivat sisältää tekstiä, kuvia, ääntä, grafiikkaa ja videokuvaa. Dokumentit kytketään toisiinsa hyperlinkeillä. Palvelussa tiedostojen siirtoon käytetty protokolla on HTTP (HyperText Transfer Protocol). Tällaisen linkin kautta voidaan siirtyä viitattuun dokumenttiin, joka voi sijaita myös toisella palvelimella. Järjestelmä voi myös toimia edustapalveluna taustalla olevaan tietojärjestelmään ja WWW onkin nykyään yleinen edusta erilaisille tietokannoille.

WWW-dokumenteja haetaan käyttöliittymien eli selaimien avulla. Kun käyttäjä antaa halutun dokumentin URL-osoitteen (Universal Resource Locator), selain ottaa yhteyden ko. koneeseen ja pyytää kyseistä tiedostoa. HTML-koodatun sivun yhteydessä haetaan myös yleensä sivulle määritellyt muissa tiedostoissa olevat elementit, kuten kuvat, mukaan. Tiedosto tulkitaan sen tyyppin mukaisesti (palvelin ilmoittaa tiedoston MIME-tyypin (Multipurpose Internet Mail Extension)) ja näytetään selaimen tulkitsemalla tavalla.

URL on tapa viitata verkossa oleviin dokumentteihin. URL:n rakenne on seuraavanlainen: protokolla://kone/hakemistopolku/tiedosto. On huomattava, että protokolla voi olla muukin kuin HTTP-protokolla, esimerkiksi HTTPS tai FTP. Protokollien RFC-standardit ovat haettavissa esimerkiksi sivulta <http://www.ietf.org/rfc.html>. Käytettyjä tiedonvälitysprotokollia tukevat erilaiset sovellukset, kuten WWW-, FTP- tai sähköpostiohjelmit.

2.3.3 Perusohjelmistojen tietoturvanäkökohtia

Internet-infrastruktuurin eri käyttötapojen teknisen tietoturvallisuuden suurin haaste on eri käyttötapoihin liittyvien ohjelmistojen tietoturvallisuuden hallinta. Tietoturvallisuuden hallinnan kannalta on otettava huomioon ohjelmistojen integrointi ja ohjelma- virheiden hallinta.

OHJELMISTOINTEGRAATIO

Nykyaikainen tietojenkäsittely perustuu ohjelmistoarkkitehtuureihin, joissa ohjelmat kootaan osittain yleiskäyttöisistä komponenteista. Toisaalta ohjelmistot ja sovellukset pyritään tiedon siirron ja käsittelyn tehostamiseksi integroimaan sekä esim. käyttäjän työpöydällä että koko tietojenkäsittelyketjun osalta mahdollisimman saumattomiksi kokonaisuusiksi. Tällöin ongelmaksi muodostuu se, miten hallitaan sovellusarkkitehtuurin yksittäisissä osissa tehtyjen valintojen vaikutus kokonaisuuteen (esim. selaimen tietoturvallisuusasetukset voivat vaikuttaa sähköpostiohjelman toimintaan tai tekstinkäsittelyohjelman automaattitoiminnot voivat olla ohjattavissa sähköpostiviestistä käsin). Lisäksi on tiedettävä (dokumentaatio ja/ tai lähdekoodi) yksittäisten ohjelmistojen toiminta riittävässä määrin ja ohjelmiston toiminnot on todennettava sekä erikseen että yhdessä muiden ohjelmien kanssa (testaus).

Sovellusten ja tietojenkäsittelyn integraatio on kehityssuunta, jossa ollaan menossa yhä laajempiin kokonaisuuksiin. Esimerkiksi WWW-sovelluspalvelut joissa järjestelmiä ja niiden palveluita ja tietoja voidaan integroida yli organisaatorajojen tai "grid computing" eli suoritinresurssien virtuaalinen keskittäminen⁵. Jälkimmäinen tarkoittaa tietojenkäsittelyresurssien yhdistämistä verkon kautta, jolloin päästään jopa supertietokoneiden käsittelykapasiteetteihin. Suurempien kokonaisuuksien hallinta edellyttää entistä vahvempaa pohjaa järjestelmäarkkitehtuurien tietoturvamalleilta ja -toteutuksilta.

YLLÄPITO JA MUUTOSTENHALLINTA

Monimutkaisten ohjelmistokokonaisuuksien hallinnan haasteellisuutta lisäävät tietokoneohjelmistoissa tyypillisesti esiintyvät ohjelmointi- ja/tai suunnitteluvirheet. Tämä aiheuttaa sen, että varsinkin Internetiin joko välillisesti tai suoraan yhteydessä olevien järjestelmien tietoturvallisuuden vaikuttavien ohjelmistovirheiden löytymisen seurannan ja ohjelmistovirheiden paikkausohjelmien käyttöönoton on oltava käyttäjäorganisaatioissa jatkuva prosessi. Prosessin on toimittava riippumatta siitä, mikä on ohjelmistovirheongelman syy.

⁵ Lisätietoja osoitteesta www.gridforum.org/2_SEC/SEC.htm

Tyypillinen esimerkki ohjelmointivirheestä, jonka kautta voi Internetiin yhteydessä olevaan järjestelmään muodostua järjestelmään pääsyn mahdollistava aukko, on ns. puskurin ylivuoto. Puskurin ylivuoto siitä, että järjestelmän ohjelmoinnissa ei ole huomioitu ylisuurten, liian pienten tai muuten väärän muotoisten syötteiden tarkistusta ja jatkokäsittelyn estoa. Tällöin järjestelmä saattaa joutua tilaan, jossa sille voidaan syötteenä antaa suoritettavaa koodia, jonka järjestelmä suorittaa ja tilanteesta riippuen esimerkiksi avaa jonkin tasoisen pääsyn järjestelmään tai antaa ulos tietoja, joiden pitäisi olla vain valtuutettujen käyttäjien saatavilla. Erityisesti tätä virhetyyppiä on löytynyt ja löytyy jatkossa verkko-, verkkopalvelin- ja työasemaohjelmistoista.

Koska ohjelmistovirheiden löytymis- ja sitä seuraava korjausprosessi on osittain sekä virheiden löytäjien että ohjelmistotoimittajan toiminnasta ja aktiivisuudesta riippuva asia, Internetiin liitettyjen järjestelmien tietoturvasuhteesta tulee huolehtia kattavasti. Tällöin on

järjestelmien haavoittuvuus otettava huomioon sekä Internetiin yhteydessä olevien järjestelmien muissa suojauksissa, asennuksissa ja valvonnassa että tarvittaessa huolehdittava korkeaa suojaustasoa edellyttävien järjestelmien riittävästä tai mahdollisesti täydellisestä eristämisestä Internet-palveluista.

2.4 Internet-verkon ja sen käytön haavoittuvuuksista

Internetin käytöstä aiheutuu käyttötavoista riippuen uhkia. Ne kohdistuvat tietoihin ja toimintoihin sekä organisaation omassa verkossa ja järjestelmissä että käytettäessä Internetiä tiedonsiirtoverkkona.

Tiedon siirron ja palvelukanavana käytön osalta uhkia voidaan luokitella lähtien tietoturvasuhteiden perusnäkökulmista tiedon luottamuksellisuudesta, eheydestä ja käytettävyydestä.

Internetissä kaikki salaamattomana välitetty tietoliikenne on altista luvattomalle seurannalle. Seurannan havaitseminen on usein mahdotonta. Palvelutarjoajien koneisiin saattaa jäädä kopioita välitetyistä viesteistä tai lokitietoja, joiden perusteella voidaan verkkokäyttötoimintoja hyvinkin yksilöivästi seurata. Tästä syystä tiedon luottamuksellisuuden kannalta lähtökohta on aina, että Internet on avoin verkko. Tällöin on kaikkien käyttötapojen osalta erikseen lähdettävä (a) siitä, että vain julkista tietoa välitetään Internetissä salaamatta. Tämä merkitsee sitä, että organisaation on myös hallittava käyttö niin, ettei salassa pidettävää tietoa sitä salaamatta välitetä Internetissä. Mikäli (b) Internet-verkkoa käytetään salassa pidettävän tiedon siirtoon tulee käyttää tiedon arvon kannalta oikein mitoitettuja salaamenetelmiä tiedon välittämisessä. Tiedon jou-

tuminen väärin käsiin ei välttämättä edellytä teknisesti vaativaa salakuuntelua esimerkiksi linjayhteyksiin kytkeytymällä. Se voi tapahtua tiedon normaalin kulun yhteydessä tilanteissa ja paikoissa, jossa luottamuksellisuuden menettäminen ei ole viranomaisen havaittavissa tai edes Suomen lainsäädännön ulottuvissa.

Tiedon eheyden kannalta Internetin perusprotokollat huolehtivat osittain teknisen tason oikeellisuudesta niin, että lähetetty tieto yleensä on myös luettavissa saman muotoisena. Mikäli eheyteen luetaan tiedon alkuperän todennettavuus tai se, että tiedolla on jokin arvo esimerkiksi raha-arvoa omaavien tapahtumien todisteena, niin Internetin perusominaisuudet eivät sellaisenaan tai perus- tai sovellusprotokollien kautta saatavienkaan osoite- tms. tietojen perusteella pohjaa tapahtumien aukottomalle todistamiselle. Konkreettisenä uhkana tästä seuraa, että asiointijärjestelmät ilman vahvoja tietoturvaominaisuuksia ovat erittäin alttiita ja suojattomia esimerkiksi petoksille, väärennyksille ja muille väärinkäytöksille.

Käytettävyyden kannalta Internet-verkon toimintavarmuus on käytännössä osoittautunut melko hyväksi. Perusprotokollissa on ominaisuuksia, jotka tukevat virhetilanteiden hallintaa ja tietoliikenteen uudelleenreititystä ohi ongelmallisten paikkojen. Jotkin verkon solmukohdat ovat haavoittuvia ja niissä tapahtuvat ongelmatilanteet voivat vaikuttaa laajalla alueella. Esimerkiksi nimipalvelun ollessa pois käytöstä Internetin normaali toiminta tietyllä verkon alueella estyy.

Organisaation sisäisen verkon kannalta Internet-liittymän kautta tulevat uhkat liittyvät luvattomaan järjestelmään ja verkkoon tunkeutumiseen, verkon kautta kulkeutuviin ns. haittaohjelmiin tai palvelun käytön estymiseen tahallisella palvelunestohyökkäyksellä tai näiden yhdistelmiin. Luvaton järjestelmään pääsy voi olla seurausta aktiivisesta ja tavoitteellisesta järjestelmään murtautumisesta. Se voi olla myös seurausta rutiininomaisesta tunkeutumisyrityksestä, jossa ensin testataan organisaation Internet-verkkoon päin näkyvän palvelun heikkouksia tavanomaisilla tunkeutujien apuvälineillä, ja näin löydettyjen aukkojen kautta löydetään tie verkon sisälle. Tämän jälkeen päästään käsiksi muun muassa organisaation salassa pidettäviin ja operatiivisiin tietoihin, jolloin aiheutetaan aina korjauskustannuksia organisaatiolle, mutta usein myös muuta vahinkoa.

Haittaohjelmat voivat levitä käyttäen mitä tahansa tiedonsiirtokanavaa, mutta pääasiassa ohjelmat käyttävät vertaisverkkoon perustuvia tiedostojakohjelmia, WWW-selailua ja sähköpostia leviämiskanavinaan. Haittaohjelmat aiheuttavat eri tasoista vahinkoa, kuten teknisen siivouksen tarvetta, tärkeiden tietojen turmeltumista tai häviämistä ja näistä aiheutuvia seurausvaikutuksia. Haittaohjelma voi myös sisältää ominaisuuksia, joiden avulla ulkopuolinen pääsee murtautumaan verkkoon⁶.

⁶ Varsinaisessa verkkoon murtautumisessa käytetään harvoin virustorjuntaohjelmien havaitsemia haittaohjelmia.

Taustalla verkkoon murtautumisessa voi olla luonnollisesti myös tarkoituksellinen toiminta, jossa kohteena voivat viranomaisen toiminnan luonteesta riippuen olla esimerkiksi valtakunnan turvallisuuden kannalta tärkeät tiedot tai organisaation hallussa olevat liike- tai ammattisalaisuuksia sisältävät asiakastiedot.

Edellä mainitut ovat vain pieni osa mahdollisista Internetin käytöstä aiheutuvista tietoturvahkista. Organisaation tulee järjestelmällisesti seurata Internetin tietoturvahkia ja kartoittaa niiden vaikutuksia organisaatiolle. Kriittisiin tietoturvahkiin tulee tarvittavin keinoin varautua esimerkiksi palomuurilla ja kieltämällä luottamuksellisen materiaalin lähettämisen salaamattomana Internetin välityksellä.

2.5 Yleisiä tietoturvaratkaisuja

Internet-verkon tietoturvallisuuden toteuttaminen edellyttää Internet-tekniikan ymmärtämistä. Suuri osa tietomurtotapahtumista perustuu Internet-verkon elementtien ja tietoliikenneprotokollien tuntemiseen ja osaamiseen. Jotta Internet-verkon kaikki elementit, kuten laitteet ja osoitteet, eivät olisi kaikkien väärinkäyttäjienkin käytettävissä, tarvitaan erilaisia suojausmenetelmiä.

Tärkeimpiä näistä suojausmenetelmistä on kuvattu tässä luvussa. Käyttäjien tunnistaminen ja todentaminen on yksi tärkeimmistä elementeistä Internetissä tarjottavien palveluiden turvaamiseksi. Muita suojausmekanismeja ovat mm. tietoliikenteen salaus, haittaohjelmien torjunta, sisäverkon suojaaminen palomuurilla, tunkeutumisen havainnointi sekä tietoturvahkien ja haavoittuvuuksien jatkuva seuranta.

2.5.1 Tunnistaminen, todentaminen ja pääsynvalvonta

Internet-perusprotokollat luovat mahdollisuudet löytää laitteita (IP-osoitteet), niihin liittyviä palveluita ja ohjelmia (portit), asiakirjoja ja niiden hakupolkuja (URL), joissakin sovellusprotokollissa on ominaisuuksia (käyttäjätunnus ja salasana), joilla voidaan kirjoittautua järjestelmiin (telnet ym.) etukäteen määritellyillä tunnuksilla tai tunnistaa viestin lähettäjä (sähköpostiosoite).

Alkuperäiset Internet-protokollien tunnistamis- ja varsinkin todentamiskäytännöt ovat kuitenkin vaativaa käyttöä ajatellen muun muassa helposti väärennettävissä (sähköpostiosoite) tai käytettävissä väärin (selväkielisen tai heikosti salatun salasanan paljastuminen verkossa). Tästä syystä monia Internet-käyttötapoja suunniteltaessa on otettava kantaa ja tarvittaessa ratkaistava käyttäjän tai asiakkaan tunnistamisen tarve verkossa ja tunnistamistekniikan tietoturvallisuudelta edellytettävä taso.

Asiakkaan, käyttäjän tai muun kohteen yksilöinnin osalta on eriteltävä tunnistaminen ja todentaminen. Voidaan ajatella, että tunnistaminen verkossa perustuu pelkästään johonkin tekniseen tunnukseen, joka voi olla esimerkiksi henkilön nimi, asiakasnumero, dokumentin nimi, sähköpostiosoite. Tunniste voi sinänsä olla täysin väärennettävissä ilman todentamiseen liittyviä sekä teknisiä että hallinnollisia, tarvittaessa mahdollisimman aukottomia menetelyitä.

Koska tietoverkon käyttäjällä ei voi olla toisesta tietoverkon käyttäjästä mitään havaintomateriaalia, katsotaan, että ns. vahva todentaminen edellyttää vähintään kahta seuraavista asioista:

- Jotakin mitä käyttäjä tietää (esimerkiksi salasana, PIN-koodi)
- Jotakin mitä käyttäjällä on hallussaan (esimerkiksi sähköinen tunniste- tai henkilökortti)
- Jotakin mitä käyttäjä on (esimerkiksi sormenjälkitunnistus)

Käyttäjätunnus ja salasana ovat perinteisesti riittäneet tunnistamiseen ja todentamiseen suljetuissa järjestelmissä. Myös Internetissä salasanan suojaus on järjestettävissä salauksella riittävän turvalliseksi, jolloin sitä voidaan käyttää ennalta rekisteröityjen käyttäjien todentamiseen, suositeltavimmin kertakäyttösalasanojen avulla⁷.

Tietoturvallisuuden kannalta vahvin eli suositeltavin ratkaisu on laatuvarmenteen kriteerit täyttävä toimikortti-PIN-yhdistelmä.

Vahvan tunnistamisen lisäksi avoimessa verkossa tapahtuva asiakkaan todentaminen edellyttää hallinnollisesti ja ohjelmistoteknisesti luotettavaa ja toisaalta päällekkäistä työtä ehkäisevää ratkaisua.

Ohjelmistoteknisesti ratkaisu, jossa tunnistettava henkilö täytyy fyysisesti todentaa vain kerran, on toteutettu ns. epäsymmetrisellä salauksella. Menetelmässä sähköisen identiteetin saaja saa henkilökohtaisen, julkisen ns. varmentajan myöntämän varmenteen. Varmenne käsittää myös yksityisen avaimen, jolla salatut viestit voidaan matemaattisesti todistetun algoritmin perusteella todentaa olevan peräisin yksityisen avaimen haltijalta. Viesti saadaan avattua lähettäjän asianmukaisesti varmennetulla julkisella avaimella.

⁷ Valtiovarainministeriön suositus "Tunnistaminen sähköisiä asiointipalveluita käytettäessä". Suosituksessa hyväksytään tunnistamistavoiksi valtionhallinnon sähköisessä asiointissa laatuvarmenteet sekä pankkiyhdistyksen TUPAS2- määräyksissä kuvattu tunnistamismenettely. Sähköisen asiointin todennuksessa on huomioitava "Laki sähköisestä asiointista viranomais-toiminnassa".

Todentaminen perustuu siis kolmeen asiaan: käyttäjän julkiseen avaimeseen (public key), käyttäjän yksityiseen avaimeseen (private key) ja luotettuun kolmanteen osapuoleen (TTP = trusted third party). Käyttäjän julkinen avain on sähköisen asiainn muiden osapuolten tiedossa, mutta yksityinen avain on henkilökohtainen. Käyttäjä ei saa paljastaa/luovuttaa salaista avaintaan kenellekään. Luotettu kolmas osapuoli varmistaa käyttäjän varmenteen, jolloin voidaan olla varmoja siitä, että varmenne kuuluu kyseiselle henkilölle.

Julkisen avaimen järjestelmällä (Public Key Infrastructure, PKI) voidaan taata myös tapahtuman kiistämättömyys. Kiistämättömyyteen tarvitaan sähköinen allekirjoitus, jossa yksityisellä avaimella allekirjoitetaan (luodaan datasta yksisuuntainen tiiviste). Tällöin vastaanottaja varmistaa laskemalla tiivisteeseen uudelleen lähettäjän julkisella avaimella olevien tietojen avulla ja vertaamalla tiivistettä alkuperäiseen tiivisteeseen, että oli tekemisissä juuri oikean varmenteen kanssa.

Laatuvarmenteiden käyttöön perustuvaan tunnistus- ja todennusmenettelyyn kuuluu lisäksi muun muassa:

- varmentajan ja varmenteen haltijan vastuiden määrittely
- yksityisen avaimen salassapidon varmistava tekniikka niin, ettei avain ole kopioitavissa
- menettelyt yksityisen avaimen (esim. toimikortti) joutuessa väärin käsiin (ilmoitus sulkulistalle)
- käytettävien salausmenetelmien tekninen vahvuus.

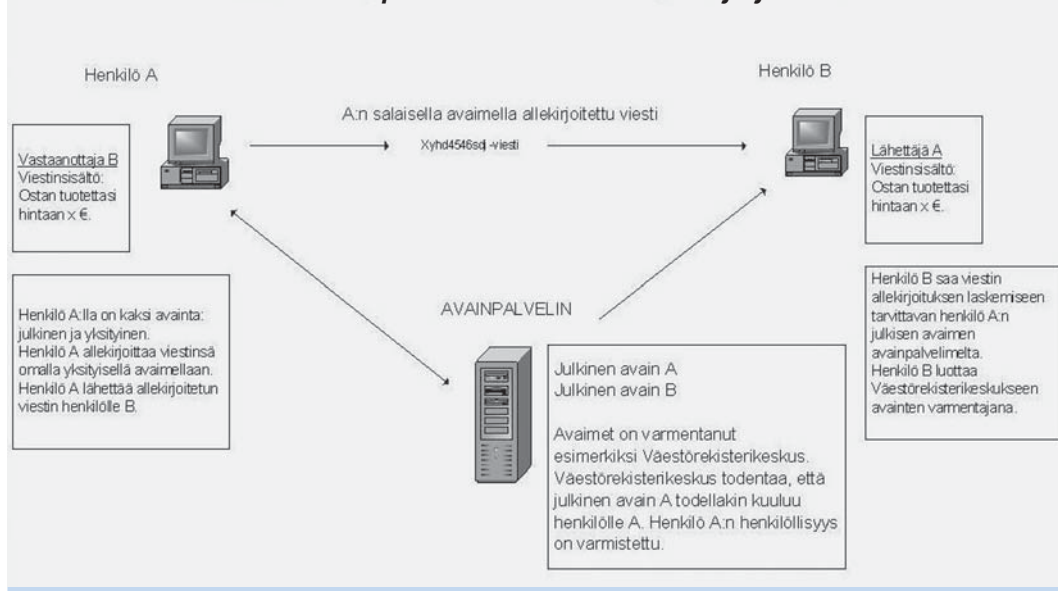
Laatuvarmenteiden käyttöä Suomessa valvoo viestintävirasto. Tällä hetkellä (kevät 2003) ainoa laatuvarmenteiden tarjoaja Suomessa on Väestörekisterikeskus. Lisätietoja Väestörekisterikeskuksen varmennepalveluista ja sähköisestä henkilökortista löytyy osoitteesta <http://www.sahkoinenhenkilokortti.fi/>. Kuvassa 7 on esimerkki osapuolten todentamisesta PKI-ratkaisussa.

Mikäli käyttäjää ei verkkokäytössä tai palvelussa tunnisteta, käytön sanotaan olevan anonyymiä. Käyttäjää tai asiakasta ei pidä tunnistaa tavallisissa tiedon, lomakkeiden tms. hakupalveluissa, joissa ei viranomaisen suuntaan tarvita asiakasta yksilöivää tiedon siirtoa.

Vahvoja tunnistusmenetelmiä voi olla tarpeen käyttää myös esimerkiksi dokumentin aitouden todentamiseen, WWW-sivuston todentamiseen tai yksittäisen palvelinlaitteen todentamiseen.

Dokumentin alkuperä voidaan todentaa käyttämällä sähköisiä allekirjoituksia. WWW-sivusto voidaan todentaa varmenteilla. Suljetussa verkossa oleva yksittäinen palvelinlaitte voidaan tunnistaa käyttämällä IPsec-suojaukseen perustuvaa menetelmää.

Kuva 7. Esimerkki viestin alkuperän todentamisesta PKI -järjestelmässä



Esimerkiksi IPSec-suojausta käytettäessä verkon ylläpitäjä allekirjoittaa jokaisen laitteen julkisen avaimen omalla yksityisellä avaimellaan. Tämän jälkeen jokaisella verkon laitteella on hallussaan:

- laitteen oma yksityinen avain (pidettävä salaisena)
- laitteen julkinen avain
- ylläpitäjän allekirjoittama laitteen julkisen avaimen varmenne ja
- ylläpitäjän julkinen avain.

Kun verkon laitteet ottavat keskenään yhteyttä, ne antavat yhteyskumppanilleen oman julkisen avaimensa ja varmenteensa sekä tarkistavat vastapuolelta saamansa varmenteen allekirjoituksen. Seuraavaksi kumpikin kone varmistaa, että toisella osapuolella on hallussa julkista avainta vastaava yksityinen avain. Tämän jälkeen osapuolet 'luottavat toisiinsa' ja voivat vaihtaa salattua tietoa⁸.

⁸ Lisätietoja palveluille asetetuista käyttäjien tunnistamiseen ja todentamisen vaatimuksista ja tekniikoista löytyy seuraavista dokumenteista: VAHTI 3/2001 ja VAHTI 4/2001

Internet-palveluiden käytön helpottamiseksi eräät ohjelmistotoimittajat tai näiden yhteenliittymät ovat kehittämässä kertakirjautumisjärjestelmiä⁹ (Single Sign On) tietojärjestelmiin ja verkkopalveluihin. Kertakirjautumisjärjestelmässä käyttäjällä on ainoastaan yksi salasana, jolla hän voi yhdellä kirjautumisella saada pääsy- ja käyttöoikeudet useampaan tietojärjestelmään. WWW-kertakirjautumistekniikat eivät ratkaise valtionhallinnon Internet-palveluiden todentamistarpeita.

2.5.2 Tietoliikenteen salaus

Tietotekniikassa salaus on menetelmä, jolla tieto voidaan muuttaa lukukelvottomaksi kaikille muille kuin oikean salausavaimen haltijalle. Hyvät tietotekniset salausmenetelmät perustuvat siihen, ettei salattua tietoa saada luettavaksi muulla tavoin kuin tietämällä oikea salausavain (= symmetrisessä salauksessa sama kuin purkuavain, epäsymmetrisessä eri) tai kokeilemalla esim. ohjelmallisesti kaikkia mahdollisia avaimen eri bittijonovaihtoehtoja. Mikäli avaimen pituus on riittävä, jälkimmäinen ei käytännössä ole mahdollinen edes suorkoneen suoritusteholla.

Salauksen toteutus eroaa hieman riippuen siitä, käytetäänkö salausta tietojen säilytyksessä vai tietojen siirrossa. Tietojen säilytyksessä on tärkeää, että salaus on aina tarpeen mukaan purettavissa, jolloin organisaatiotasolla on otettava kantaa yksityisten salausavainten varmuuskopiointiin ja palautukseen. Salaus on ainoa tehokas tapa toteuttaa salassa pidettävän tiedon välitystä Internet-verkossa.

Koska symmetrisessä salauksessa salausavain on sama kuin purkuavain, on ratkaistava avaimen välitys tiedon saajalle. Käytännössä salausohjelmisto luo istuntokohtaisen symmetrisen avaimen, joka välitetään vastaanottajalle epäsymmetrisesti salattuna. Tällöin lähettäjällä ja vastaanottajalla tarvitsee olla hallussaan vain epäsymmetrisessä salauksessa käytetyt avaimet. Lähettäjällä vastaanottajan julkinen avain ja vastaanottajalla oma yksityinen avain.

Tietoliikenteen salauksessa tulee huomioida seuraavat asiat:

- Virustorjunta- ja tunkeutumisen havainnointiohjelmistot eivät pysty tutkimaan salattua tietoliikennettä.
- Tiedon salassapidon kannalta paras vaihtoehto on salata tietoliikenne käyttäjältä käyttäjälle, mutta tällöin ongelmaksi muodostuu tietojen tarkastaminen esimerkiksi viruksista.
- Suositeltavin vaihtoehto on salata tietoliikenne palomuriin asti, jossa salattu tieto puretaan ja välitetään virustorjunta- ja tunkeutumisen havainnointiohjelmiston tarkastettavaksi.

⁹ Lisätietoja löytyy osoitteista www.projectliberty.org tai www.passport.net

Salausmenetelmää valittaessa tulee huomioida seuraavat asiat:

- Salauksen teoreettinen vahvuus ei aina vastaa salauksen vahvuutta käytännössä. Esimerkiksi käyttäjän valitsema salasana salauksen purkuvaimelle on useimmiten liian lyhyt ja salasana muodostuu pelkistä pienistä kirjaimista. Tällöin teoreettisesti vahva salaus heikkenee.
- Valitun salausmenetelmän tulee olla käyttäjälle mahdollisimman läpinäkyvä. Esimerkiksi useimmat yksityiset virtuaaliverkkoratkaisut eivät edellytä käyttäjältä muita toimenpiteitä kuin käyttäjän tunnistustietojen syöttämisen.
- Mitä vahvempi salaus, sitä enemmän salaaminen yleensä vaatii järjestelmältä suoritustehoa ¹⁰.

Seuraavassa on lyhyesti esitelty yleisimmin käytettäviä tietoliikenteen salaamisen tietoturvamekanismeja:

IPSec

- Suunniteltu suojaamaan IP-pakettien luottamuksellisuutta sekä havaitsemaan niihin kohdistuvia väärennysyrityksiä.
- Salaa ja sinetöi kuljetus- ja sovellusdatan tiedonsiirron aikana.
- Voidaan hyödyntää muun muassa palvelinlaitteiden luottamussuhteiden luomiseen.
- Käytetään VPN-yhteyksissä.

SSL (Secure Socket Layer)

- Suojataan pääasiallisesti WWW-sovellusten tai sähköpostikäyttöohjelmien välistä tiedonsiirtoa käyttäjän työaseman ja palvelimen välillä.
- Sisältyy yleisimpiin WWW-selaimiin.
- Viimeisintä SSL-parannusta kutsutaan TLS:ksi (Transport Layer Security)

¹⁰ Suoritusteho ei ole viimeaikoina ollut ongelma, koska laitteet ja algoritmit ovat kehittyneet.

SSH (Secure Shell)

- Suojattuihin pääteyhteyksiin ja tiedonsiirtoihin kehitetty tietoturvaprotokolla, joka soveltuu hyvin järjestelmien etähallintaan.
- Korvaa mm. turvattomat Telnet, FTP, ja r-komennot.
- Käytetään yleisesti myös sovellustason VPN-ratkaisuna
- Perustuu vahvojen salausmenetelmien käyttöön.
- Monenkertaiset vahvat todennusmenetelmät perustuen esimerkiksi julkiin avaimiin.

Yksityiset virtuaaliverkot (Virtual Private Network, VPN) ovat palomuuriratkaisun osatekijöitä erityisesti silloin, kun organisaation verkkoja yhdistetään epäluotettavan verkon (Internet) yli. VPN-yhteyksillä suojataan yleensä etäkäyttäjää tai organisaation verkkoja, jotka fyysisesti ovat erillisiä. Myös organisaation sisäverkko voi olla epäluotettava, erityisesti jos siirrettävä tieto ei ole tarkoitettu kaikille organisaation jäsenille. Tällöin sisäverkon liikenne on syytä suojata. VPN-yhteydet perustuvat salaaviin protokolliin, kuten IPSec, joiden avulla muodostetaan salattuyhteys kahden VPN-palvelimen välille.

- VPN (Virtual Private Network)
 - Liitetään kaksi etäpistettä Internetin välityksellä turvallisesti toisiinsa
 - VPN-yhteyksissä käytetään yleisimmin edellä mainittua IPSec-protokollaa. Muita käytössä olevia VPN-protokollia ovat mm. Microsoftin PPTP (Point-to-Point Tunneling Protocol ja Secure Tunnel Establishment Protocol (STEP)
 - Kustannustehokkaampi ja skaalautuvampi vaihtoehto kuin kiinteät yhteydet (esimerkiksi X.25 tai frame relay)

VPN-palvelut on yleensä helpointa sijoittaa palomuurilaitteeseen, koska tällöin voidaan tietoliikennettä seurata myös näiden yhteyksien osalta ja poistaa mahdolliset VPN-yhteyksien kautta tulevat haittaohjelmat. Lisäksi palomuurin ylläpito yksinkertaistuu, kun VPN-yhteydet salataan vain palomuurilaitteeseen asti¹¹.

2.5.3 Haittaohjelmien torjunta

Internetin käytön suurimpia uhkatekijöitä ovat erilaiset haittaohjelmat, kuten madot, virukset, Troijan Hevoset ja erilaiset 'vakoiluohjelmat' (Spyware). Haittaohjelmien avulla hakkerit pyrkivät vahingoittamaan organisaation tietojärjestelmiä, mahdollisuuksien

¹¹ Salausmenettelyjen suunnitteluun löytyy lisätietoja VAHTI 3/2001 Salaukäytäntöjä koskevasta valtioneuvoston tietoturvasuosituksista.

mukaan tunkeutumaan tietojärjestelmiin tai seuraamaan yksittäisten käyttäjien toiminnasta aiheutuneita tietoturva-aukkoja.

Haittaohjelmien torjunnassa tärkein puolustusmekanismi on ennaltaehkäisy, joka toteutetaan käyttöohjelmistojen oikealla asennuksella ja turvallisuusaukkojen paikkaamisella sekä yhdellä tai useammalla oikein asennetuilla automaattisesti päivittyvällä virustorjuntaohjelmalla. Koska haittaohjelmat voivat olla merkittävä tietoturva-aukko minikä tahansa organisaation toiminnalle, liittyy niiden torjunta olennaisesti myös organisaation verkon ja järjestelmien suojaamiseen. Monissa organisaatioissa haittaohjelmien torjunta vaatii monentasoista toimintaa, kuten palvelinten ja työasemien virustorjuntaohjelmat, evästeiden ja mainosten hallintaohjelmistoja sekä erillisen tietoliikenteen, lähinnä sähköpostin tarkastuksessa käytetyn, virustorjuntaohjelman⁸.

Järjestelmiin asennettuja ylimääräisiä portteja voidaan käyttää myös Troijan Hevosten ja muiden haittaohjelmien asennuksessa. Taulukossa 1 on esitetty joitakin yleisesti esiintyviä Troijan Hevosia.

Taulukko 1. Esimerkki tunnetuista TCP/IP –portteja hyödyntävistä Troijan Hevosista

TCP/IP -portteja ja troijalaisia, jotka käyttävät näitä portteja

PROTOKOLLA	PORTTINUMERO	TROIJALAINEN
FTP	20 ja 21	Senna Spy FTP Server, Blade Runner, Dark FTP, jne.
SSH	22	Adore sshd, Shaft
Telnet	23	ADM worm, Fire Hacker, Telnet Pro, jne.
SMTP	25	I love you, Stealth, WinSpy, jne.
HTTP	80	Seven Eleven, Back Orifice 2000 Plug-Ins, RTB 666, jne.
Ei varattu	1243	Sub Seven
Ei varattu	12346	Net Bus/Net Bus Pro käyttää porttia 20034
Ei varattu	54320	Black Orifice 2000 (oletusportti)

Tietoliikenteen mukana kulkeutuvien haittaohjelmien havainnointi voi olla ongelma silloin, kun tietoliikenne on salattua. Siksi on tärkeää, että organisaatiossa on selvät toimintasäännöt, kuinka haittaohjelmien torjuntaohjelmisto käsittelee esimerkiksi salattut sähköpostin mukana tulevat liitetiedostot.

2.5.4 Palomuri

Palomuri on laitteisto ja/tai ohjelmisto (abstraktimmin suojausrajapinta), jonka tehtävä on rajoittaa pääsyä sen taustalla olevaan suojattuun verkkoon. Palomuri on tietoliikenteen valvontamekanismi, joka ei yksittäisenä laitteena tai ohjelmistona tarjoa täydellistä suojaa, mutta yhdessä toimivan tietoliikenteen seurannan kanssa muodostaa tärkeimmän suojausrajapinnan organisaation Internet-yhteydelle. Palomuurista ei ole hyötyä, jos se voidaan kiertää tai se asennetaan väärin.

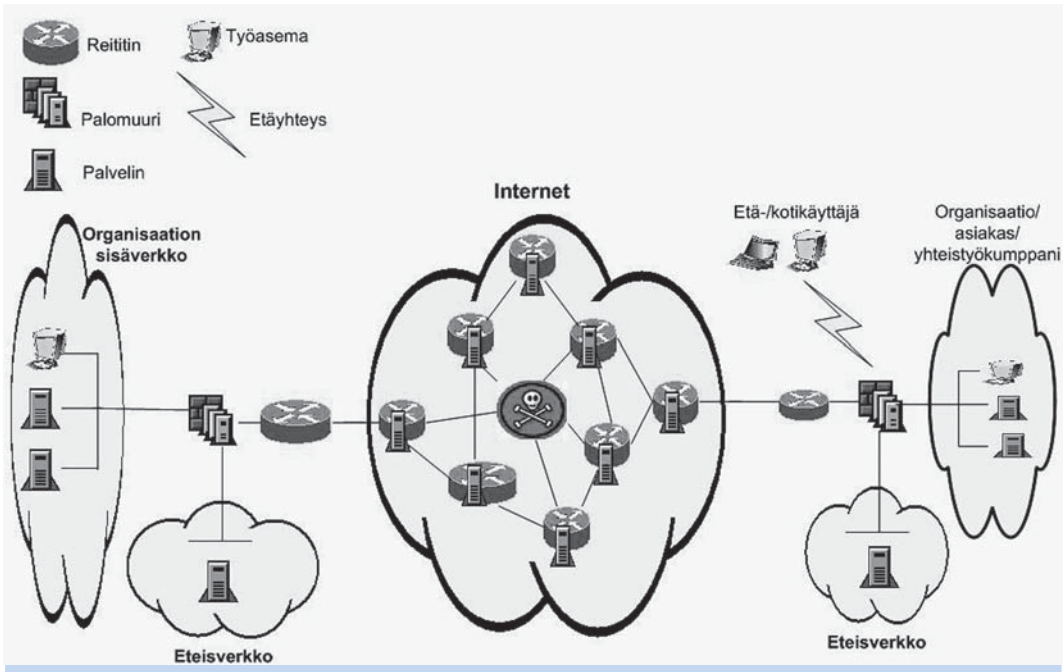
Palomuurilaitteisto sijoitetaan Internet-yhteyksien yhteydessä suojattavan lähiverkon ja avoimen Internet-verkon väliin. Kaikki yhteydet suojattuun verkkoon ja verkosta ulos kulkevat palomuurin kautta ja palomuriin määritellään, mitä yhteyksiä päästetään läpi. Palomuurin sääntöjen määrittelyyn on kaksi perusvaihtoehtoa: joko estetään pääsy tiettyihin palveluihin tai laitteisiin, tai estetään pääsy kaikkiin (paitsi erikseen sallittuihin) laitteisiin ja palveluihin. Jälkimmäinen on hallittavuuden kannalta ehdottomasti parempi.

Tehokkaan ja toimivan palomuuriratkaisun lähtökohta on perusteellinen topologinen suunnittelu ja toteutus. Koska Internetin käyttötavat vaihtelevat, voi myös tietoturva-vaatimuksiltaan erilaisten käyttötapojen palomuuritopologia vaihdella (esimerkiksi palomureja voi olla useita), mutta yleensä palomuurin/en avulla toteutetaan erillinen/erilliset eteisverkko/t.

Palomuurin topologiassa voidaan erotella toisistaan seuraavat osat (kuva 8) :

- Ulkoverkko (kuvassa Internet), johon ei luoteta.
- Eteisverkko, joka on omassa hallussa oleva verkkosegmentti, mutta käytettävän tarkoituksen tietoliikenneyhteydet ovat riittävän avoimia ja minimoituja. Ulkoverkkoon suunnatut palvelut sijoitetaan yleensä tähän verkkoon. Tämä verkko voidaan vielä jakaa julkisia Internet-palveluita tarjoavaan verkkoon ja rajoitetumpaan eteisverkkoon.
- Suljettu yksityisverkko, eli sisäverkko, jonne päästetään vain hyväksytty liikenne.

Kuva 8. Palomuurin topologia



Kehittyneemmissä ratkaisuisa palomuri voi myös rajoitetussa määrin valvoa tietoliikenteen sisältöä, esimerkiksi estää ActiveX-komponenttien lataamisen verkosta.

Palomuri ei kuitenkaan tarjoa täydellistä suojaa tietoliikenteen kautta tulevia uhkia vastaan, vaan näitä tulee hallinnoida myös muilla tietoturvamekanismeilla. Alla on esitetty ominaisuuksia, joita valmistajat ovat lisänneet palomuihinsa:

- Aikaisemmin mainitulla VPN-tekniikalla loogista sisäverkkoa voidaan laajentaa Internetin yli yhdistämään lähiverkkoja
- Verkko-osoitemuunnoksia (Network Address Translation, NAT), joiden avulla estetään sisäverkon verkko-osoitteiden näkyminen Internetiin
- Kuorman tasauksella hallitaan laitteiden suorituskykyyn liittyviä ongelmia jakamalla tietoliikennettä useammille laitteille

- Vikasietoisuusominaisuuksilla varustettua palomuurijärjestelmää voidaan käyttää, vaikka jokin osa palomuurijärjestelmästä ei toimisi
- Tunkeutumisen havainnoinnilla tehostetaan yhteyksien valvontaa (ks. 2.5.5)¹².

Palomuurit voidaan ryhmitellä toimintaperiaatteiden perusteella eri tyyppisiin, jotka ovat sovellusyhdyskäytävät, pakettisuodattimet ja hybridiratkaisut.

SOVELLUSYHDYSKÄYTÄVÄT

Sovellusyhdyskäytävä tarkoittaa sitä että palomuri itse ottaa vastaan sovelluksien tietoliikenneyhteydet ja itse toteuttaa sovelluksen palveluita (ns. proxy-toiminto). Esimerkiksi SMTP-proxy toimiva palomuri ottaa ulkoverkon koneilta vastaan sähköposteja ja välittää sähköpostit sisäverkon postipalvelimelle.

Sovellusyhdyskäytäväpalomuri voidaan toteuttaa eri tavoin, mutta olennaista on se, että palomuri käyttää suodatuskriteereinä sovelluspalveluiden ominaisuuksia eikä IP-otsikoita, kuten liikenteen lähteen tai kohteen osoitteita. Tämä edellyttää usein asennusmuutoksia ohjelmistoihin, esimerkiksi FTP-asiakasohjelmiin on annettava palomuurin proxy-palvelun osoite.

Sovellusyhdyskäytäväperiaatteeseen perustuvat palomuurit ovat aina hitaampia kuin pakettisuodatinratkaisut. Pelkästään sovellusyhdyskäytävään perustuvat palomuuriratkaisut eivät sovellu vilkasliikenteisiin verkkoihin. Lisäksi tämä menetelmä vaatii, että palomuri tunnistaa käytössä olevan sovellusprotokollan, joten ne eivät yleensä tue erikoisia tai paikallisesti kehitettyjä sovelluksia.

PAKETTISUODATUS

Pakettisuodatus päästää IP-paketit läpi sellaisenaan tiettyjen sääntöjen mukaan. Säännöt perustuvat yleensä IP-osoitteisiin, palveluiden osoitteisiin (TCP:n ja UDP:n portit) sekä tietoliikenteen suuntaan. Tavallisten reitittimien turvaominaisuudet riittävät jo tämäntyyppisiin toimintoihin. Olennaista on kuitenkin, että pakettisuodatin tarkastelee tietoliikennettä IP-paketti kerrallaan, näkemättä välttämättä tietoliikenteen kokonaisuutta. Edistyneemmät palomuurit pystyvät tunnistamaan yhteyden avauksen sisäverkosta ulkoverkkoon ja rajoittamaan yhteydet vain sisäverkosta avattuihin.

Pakettisuodatin voi tehdä tietoliikenteelle myös osoitemuunnoksia, jolloin sisäverkon koneiden osoitteet eivät näy ulospäin. Pakettisuodattimet ovat nopeita, mutta eivät yksin riitä organisaation sisäverkon suojaamiseen.

¹² Suositeltavaa on käyttää tunkeutumisenhavainnointiin omia erillisiä laitteita.

Tilapohjaiset palomuurit pitävät kirjaa istuntojen tiloista. Tämä ominaisuus mahdollistaa sen, että tilapohjaiset pakettisuodattimet voivat dynaamisesti avata liikenteen paluukanavan vasta kun sitä tarvitaan.

Käytännössä useimmat palomuurit ovat ns. hybridipalomuureja, jotka yhdistävät sekä sovellusyhdykäytävän että tilapohjaisen pakettisuodattimen ominaisuuksia. Tällöin voidaan valita, mitkä palomuuritoiminnot toteutetaan sovellustasolla ja mitkä esimerkiksi nopeussyistä pakettisuodatustasolla.

2.5.5 Tunkeutumisen havainnointijärjestelmä

Tietoliikenteen lisääntyessä ei ylläpitäjien aika riitä kaiken liikenteen valvomiseen ja joissakin ympäristöissä palomuurien suojaustoiminnot ovat riittämättömiä Internetistä tuleviin monipuolistuviin tunkeutumisyrittäisiin.

Tietoliikenteen seuraamiseksi on kehitetty tunkeutumisen havainnointijärjestelmiä (Intrusion Detection System, IDS). Järjestelmän toiminta perustuu verkon normaalin tietoliikenteen määrittämiseen, hyökkäysmallien kuvaamiseen, tietoliikenteen poikkeamien tunnistamiseen ja poikkeamien aiheuttamiin hälytyksiin.

Tunkeutumisen havainnointijärjestelmiä on kahta tyyppiä: isäntäkone- ja verkko-ohjelmia. Edellinen seuraa vain isäntälaitteen toimintoja ja ilmoittaa, jos sen levyjen tietosäilyssä ohjelmistoissa, tietoliikenteessä tai prosesseissa on mainittavia muutoksia. Isäntälaitteohjelmistot (Host Intrusion Detection System HIDS) perustuvat yleensä agenttiohjelmiin, joita voidaan 'räätälöidä' havainnoimaan myös ohjelmakohtaisia muutoksia, kuten pääsyoikeuksia.

Verkko-ohjelmisto (Network Intrusion Detection System NIDS) seuraa koko verkon tai yhden verkkosegmentin tapahtumia. Se on avuksi tietoliikenteen seuraamisessa, mutta se ei yksinään ilman huolellista ylläpitoa ja muita verkon turvamekanismeja ratkaise verkon tietoturvaongelmia. Järjestelmän käyttöä voidaan harkita vasta, kun tietoliikenteen seuranta ja muut tietoliikennejärjestelmien lokien käsittelyt on järjestetty ja seuranta on säännöllistä.

Tunkeutumisen havainnointijärjestelmää voidaan käyttää lokitietojen keskitettynä hallintajärjestelmänä. Tällöin kopioidaan kaikista verkkopalvelimista, niiden tietoliikenteestä ja verkkoanalysointiohjelmista lokitiedot joita yhdistämällä saadaan selville organisaation normaali tietoliikenne. Havainnointijärjestelmä hälyttää verkon väärinkäytöksistä tai ongelmista, jos poikkeamia normaaliin liikennöintiin tai tietojärjestelmien ohjelmauhkiin havaitaan.

Toistaiseksi tunkeutumisen havainnointijärjestelmissä on esiintynyt seuraavia ongelmia:

- Väärät hälytykset, koska järjestelmien ylläpitämät tietokannat eivät ole riittävän kehittyneitä.
- Isäntälaittejärjestelmien suuri suoritustehon tarve.
- Verkkojen havainnoinnin manipulointialttius esimerkiksi hyökkäyssekkvenssien muuntelulla ja hyökkäysfrekvenssin jakamisella osiin.
- Kytkentäiset verkot voivat muodostaa esteen järjestelmien toimivuudelle verkossa, mikäli kytkin ei tue kaiken tietoliikenteen näkymistä käytettyyn kytkinporttiin.

Tunkeutumisen havainnointijärjestelmät kehittyvät koko ajan ja järjestelmien toimittajat pyrkivät kehittämään järjestelmiään siten, että ne eivät aiheuta vääriä hälytyksiä ja niitä on vaikeampi kiertää.

Tunkeutumisen havainnointijärjestelmän käyttöönotto vaatii huolellista suunnittelua ja käyttöönoton jälkeen jatkuvaa ylläpitoa. Erityisesti verkon havainnointijärjestelmät vaativat uusien hyökkäysmallien päivityksiä järjestelmän ajan tasalla pitämiseksi.

3 INTERNET-VERKON KÄYTTÖTAVAT JA NIIDEN TIETOTURVALLINEN TOTEUTUS

3.1 Lähtökohdat

Tietoturvallisuus on merkittävä tekijä Internet-järjestelmiä suunniteltaessa, asennettaessa, kehitettäessä ja laajennettaessa. Jo järjestelmien suunnitteluvaiheessa tulee muistaa, että turvallisuus on jatkuva prosessi, ei ominaisuus.

3.1.1 Lainsäädännölliset lähtökohdat

Internet-verkon käyttötapojen suunnittelun lähtökohta on organisaation toimintaa ja Internet-verkkoa ohjaava lainsäädäntö.

Lainsäädännöstä on tiedostettava organisaation toiminnan perusteita koskevat säännökset kuten tietojen salassa pidettävyyttä ja perustehtäviä koskevat säännökset sekä yleiset tietojenkäsittelyä koskevat säännökset. Edellisten merkitys saattaa olla tarpeen arvioida uudelleen verkkomaailman osalta. Osa tietojenkäsittelyä ohjaavista säännöksistä asettaa vaatimuksia yksittäisille toiminnoille ja sovelluksille, esimerkiksi:

- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki sähköisistä allekirjoituksista (14/2003)
- Henkilötietolaki (523/1999)

Lainsäädäntöön viitataan tässä ohjeessa silloin, kun on kyseessä Internetiin liittyvän toiminnan ohjaus, Internetiin erityisesti liittyvä ilmiö ja asialla on selkeä tietoturvakäytäntö.

Internet-palveluita toteutettaessa tulee huomioida teletoimintaa koskevat säännökset. Koska Internet-verkko on maailmanlaajuinen, säännöksistä ei voida kuitenkaan löytää esimerkiksi koko Internet-verkon luotettavuutta tai palvelutasoa määrittäviä kriteereitä. Teletoimintaa koskeva lainsäädäntö ja sen nojalla annetut Viestintäviraston¹ määräykset ohjaavat lähinnä sitä, mitä suomalaisilta teleoperaattoreilta voidaan vaatia tietoturvallisuuden suhteen, esimerkiksi:

- viestinnän luottamuksellisuus,
- tietty tietoturvaso ja
- asiakkaiden (ml. käyttäjäorganisaatiot) informointi tietoturvariskeistä².

Ns. ATK-rikoksia koskevat säännökset antavat joitakin mahdollisuuksia reagoida jälkeenpäin Internet-verkosta peräisin oleviin toteutuneisiin uhkiin. Selvittämiskeinojen rajallisuus, esimerkiksi tapahtumien havaitseminen, tutkinnan vaikeus, kansainvälisen yhteistyön haasteet, lainsäädännön alueellinen ulottuvuus ja lainsäädännön kansainväliset eroavaisuudet kuitenkin antavat suljetun verkon tietoturvan hallintaan verrattuna entistä enemmän aihetta panostaa ennalta ehkäisevään toimiiin.

Muista lainsäädännöllisistä osa-alueista tulee huomioida:

- sopimusoikeus sekä Internet-verkon käyttötapojen että erilaisten palveluhankintojen vastuukysymysten kannalta
- immateriaalioikeudet esim. luvallisen kopioinnin rajojen tiedostamisen tai julkisiin lisensseihin perustuvien ohjelmistojen käytön kannalta

3.1.2 Internetin käytön tietoturvapoliittikka

Internetin käyttötapoihin liittyy kysymyksiä ja päätöksiä, joita ei voida tehdä ilman organisaation korkeimman johdon ja tietohallintojohdon myötävaikutusta. Päätökset edellyttävät myös valmistelu- ja suunnitteluprosessia, jossa toteutusvaihtoehdot arvioidaan sekä toiminnallisista että myös tietoturvanäkökohdista lähtien.

Käyttötapojen valmistelussa, investointipäätösten, hankintojen ja toteutusten teknisessä suunnittelussa on tietoturvallisuuden hallinnan ja toteutuksen näkökulma olta- va mukana alusta alkaen. Tämä vaatii riittävää vuorovaikutusta päättäjien ja teknisten asiantuntijoiden välillä niin, että päätöksiä vaativat asiat tulevat päätetyksi ja oikeilla perusteilla. Teknisten sovellusten käyttöönottolla voi olla monissa tietoturvallisuutta si-

¹ Laki Viestintähallinnosta (625/2001)

² Lakiehdotus Sähköisen viestinnän tietosuojasta

vuavissa kysymyksissä syvällisiä vaikutuksia koko organisaatioon ja sen toimintatapoihin, esimerkiksi:

- Internet-selailuyhteyksien käyttö
 - työajan käyttö ja valvonnan rajat
 - peruskäyttäjän oma vastuu
 - ongelmatilanteiden hallinta
- Sähköpostiviestintä
 - sähköpostin käyttötarkoitus ja mahdollisuuden käytön rajoittamiseen
 - käytön suunnitelmallisuus ja kytkentä asiakirjojen hallintaan
 - viestinnän luottamuksellisuuden hallinta ja siihen liittyvät vastuukysymykset
- Sähköinen asiointi
 - kytkentä operatiivisiin järjestelmiin
 - muutokset työskentelyprosesseihin
 - käsittelyprosessien nopeuttaminen
 - vuorovaikutteisuuden hallinta ja eri asiointikanavien rinnakkainen toiminta
 - asiakirjojen hallinta
- Eri organisaatioiden lähiverkkojen yhdistäminen ja järjestelmien integrointi
 - tietoturvasojen yhteneväisyys
 - valvonnan vastuut
 - palvelutasojen ja tiedon laatu vastuun määrittely

Internetin eri käyttötapojen tietoturvallisuuden hallintaan liittyvät päätökset ja ohjaavat valinnat on syytä kirjata organisaation tietoturvapoliitiikkaan.

3.2 Tietoliikenneyhteys Internet-verkkoon

Organisaation sisäverkon liittäminen Internetiin edellyttää sisäverkon eristämistä Internetistä palomuurilla. Palvelinlaitteistot sekä julkiseen että sisäiseen käyttöön tulee myös suojata.

Organisaatio voi käyttää Internet-verkkoa sisäiseen tai muiden valtionhallinnon organisaatioiden kanssa käytävään tietoliikenteeseen edellyttäen, että organisaatio ottaa huomioon osapuolten tunnistuksen, tietoliikenteen salauksen ja käytettävyyden vaatimukset. Yhdistettäessä viranomaisten tietojärjestelmiä Internetin kautta, on käytettävä vahvaa salausta tai suojattava tietoliikenne muilla keinoin.

Yleisimmän tietoturvauhan organisaatioiden järjestelmille aiheuttavat erilaiset haittaohjelmat, virukset, madot ja Troijan hevoset. Näiden ohjelmien toiminnan ennalta ehkäiseminen ja seuranta tulee huomioida Internet-palvelimissa. Parhaat tulokset järjestelmien turvallisuudelle saadaan, kun haittaohjelmien torjunta ja tietoliikenteen seurantaohjelmat ovat osana palomuuriratkaisujen suunnittelua ja toteutusta.

Tietoverkkojen suunnittelussa on huomioitava, ettei Internetin käytettävyyttä (esim. yhteyden kaistanleveyttä ei voi taata) ei ole varmistettu televerkkojen tavalla.

3.2.1 Palvelimen liittäminen verkkoon

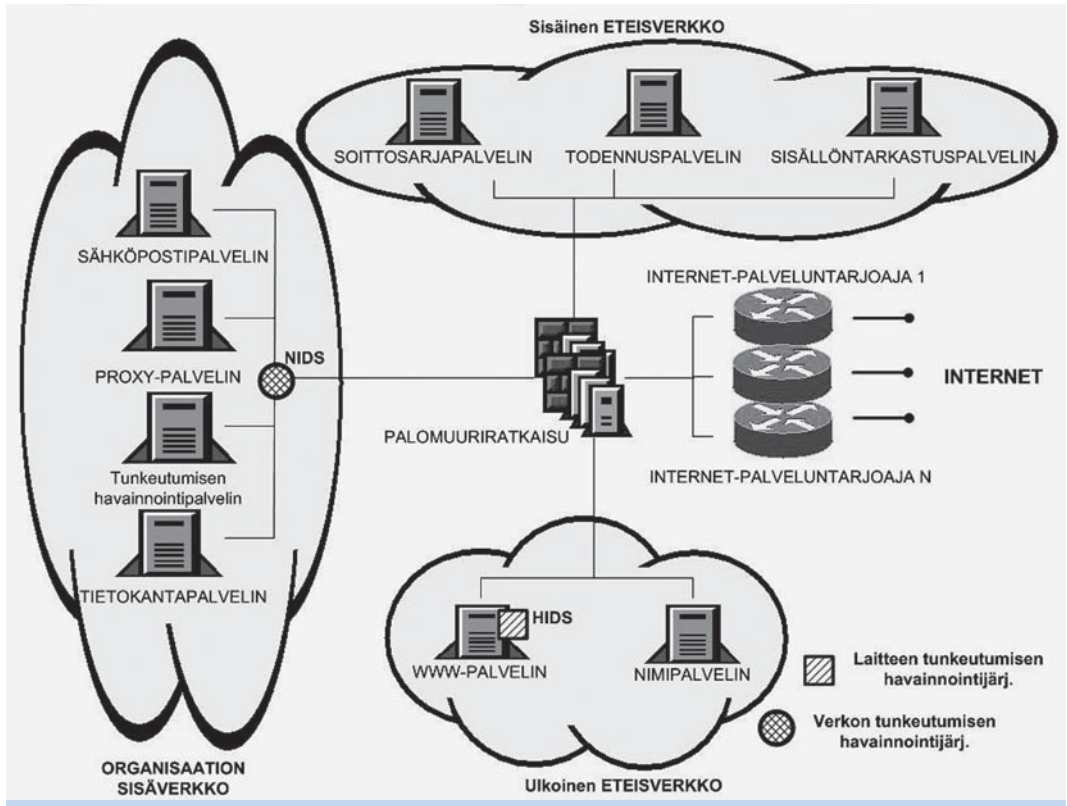
Tietoliikenneverkkoon liitettävälle laitteelle/palvelimelle tulee ensimmäiseksi suunnitella sen sijainti verkossa. Sijainnin perusteella laitteelle voidaan suunnitella tarvittavat suojausmenetelmät mahdollisimman perusteellisesti. Liitettäessä palvelin tai laite verkkoon tulee palvelimen/laitteen perusturvallisuudesta huolehtia, koska

- puutteellisesti asennetun palvelimen/laitteen tai väärän käytön seurauksena voi olla luottamuksellisen tiedon paljastuminen tai muuttuminen
- luvaton taho voi päästä käsiksi palvelimeen/laitteeseen ja käyttämään palvelimen/laitteen tietoja sekä resursseja väärin tarkoituksiin esimerkiksi roskapostien lähettämiseen
- palvelimen/laitteen toiminta voidaan estää palvelunestohyökkäyksillä eivätkä käyttäjät saa tarvitsemaansa palvelua.

Kuvassa 9 on esitetty joidenkin Internet-palveluihin liittyvien palvelinten, kuten WWW-palvelimen ja sähköpostipalvelimen, verkkotopologinen sijainti. Kuvassa on esitetty myös esimerkkinä tunkeutumisen havainnointijärjestelmien (ks. 2.5.5) sijainnit. Perussääntönä verkkotopologiassa on sijoittaa Internet-käyttäjille tarkoitetut palvelimet ulkoiseen eteisverkkoon ja palvelimet, jotka tukevat organisaation omia käyttäjiä, esimerkiksi todennuspalvelin, sisäiseen eteisverkkoon.

Kerroksellisessa suojaamisessa kaikkein kriittisimmät tiedot on sijoitettu Internet-liittymästä katsoen verkon kaikkein sisimpään osaan, tarvittaessa vaikka sisäisellä palomuurilla suojaten. Itse palvelinlaitteiston suojaus on viimeisin osa kerroksellisuutta ja tällä pyritään varmistamaan suojauksen pitävyys, vaikka yksi suojauskerros pettäisikin.

Kuva 9. Esimerkki organisaation Internet-liittymästä



3.2.1.1 Järjestelmän käyttöönoton suunnittelu

Järjestelmän käyttöönotto on monivaiheinen prosessi, jossa tietoturvaluisuus tulee huomioida mahdollisimman aikaisessa vaiheessa. Mahdollisesti jo sovelluksia suunniteltaessa, jolloin kaikki sovellukseen liittyvät toiminnot, mukaan lukien tietoturvatoinenpiteet, tulee dokumentoida. Järjestelmien käyttöönoton suunnittelussa pitää ottaa huomioon seuraavat asiat:

- Käyttötarkoituksen määrittely
- Tarvittavat ohjelmistot
- Tiedon- ja tiedostonhallinta
- Käyttäjryhmät ja käyttövaltuudet
- Lokien käsittely
- Varmuuskopiointi

- Tarvittavat ohjelmistopäivitykset
- Dokumentointi ja testaus
- Vikasietoisuusominaisuudet, esimerkiksi järjestelmiä kahdentamalla saadaan minimoitua mahdollisia käyttökatkoksia.

3.2.1.2 Käyttöjärjestelmän sekä varusohjelmiston asentaminen ja vahventaminen

Internetiin liitettäviltä järjestelmiltä edellytetään jo lähtökohtaisesti korkeaa tietoturvalisuutta. Tekninen perusta tietoturvallisuudelle on käyttöjärjestelmän ja ohjelmistojen asentaminen siten, että järjestelmän väärinkäyttömahdollisuudet on minimoitu. Tähän voidaan käyttää käyttöjärjestelmästä tai ohjelmistosta turvalliseksi esiasennettuja versioita ja/tai tehdä asentaminen jäljempänä esitetävien periaatteiden mukaan.

Useimmat käyttöjärjestelmät ovat yleiskäyttöisiä. Niissä on perusasetuksilla paljon sellaisia palveluita, joita ei tarvita silloin, kun järjestelmää käytetään rajattuun tarkoitukseen. Poistamalla käyttöjärjestelmän tarpeettomia ominaisuuksia vähennetään myös järjestelmän haavoittuvuuksia. Esimerkiksi WWW-palvelimen ei ole tietoturvalista toimia sähköpostipalvelimena, vaikka tämä olisikin helposti toteutettavissa eräillä käyttöjärjestelmillä.

Ylimääräisten ominaisuuksien karsiminen on käyttöjärjestelmä- ja sovelluskohtaista, mutta yleensä asennuksessa ja ylläpidossa voidaan huomioida seuraavat asiat:

- Pääkäyttäjän salasana vaihdettu riittävän turvalliseksi.
- Laajimmilla pääkäyttäjän tunnuksilla ei voi kirjautua järjestelmään suoraan, vaan jokaiselle pääkäyttäjälle on luotu yksilölliset tunnukset.
- Poistetaan järjestelmästä kaikki ilman salasanaa tapahtuvat etäkirjautumismahdollisuudet
- Säädetään aikaraja sisäänkirjautumisen voimassaololle. Tällöin aikarajan umpeuduttua käyttäjä kirjataan ulos järjestelmästä.
- Tarkistetaan, että tiedostoihin ei anneta liikaa käyttöoikeuksia.
- Poistetaan ylimääräiset käyttäjätunnukset.
- Poistetaan väliaikaiset ja ei kenenkään omistuksessa olevat tiedostot niin asennuksen yhteydessä kuin siitä säännöllisesti eteenpäin.
- Tarkistetaan, että käynnistystiedostot ovat vain pääkäyttäjän muokattavissa.

- Poistetaan palvelimesta kaikki tarpeettomat haavoittuvat graafiset käyttöliittymät
- Poistetaan tarpeettomat palvelut

Kaikista alkuperäisistä asennustiedostoista ja asetuksista tulee ennen ominaisuuksien ja palvelujen poistamista ottaa varmuuskopio. Varmuuskopioilla luodaan mahdollisuus järjestelmän toiminnallisuuden palauttamiseen, jos asetusten valinnoissa tehdään virheitä.

Asennuksessa on huomioitava kaikki asennuspäivään mennessä julkaistut järjestelmän turvallisuuteen vaikuttavat korjauspäivitykset.

3.2.1.3 Sovellusten turvallinen asentaminen

Sovellusten asentamisessa noudatetaan samankaltaisia periaatteita kuin käyttöjärjestelmän asennuksessa. Asennuspaketteihin kuuluu lähes poikkeuksetta tarpeettomia palveluja ja tietoaaineistoja, jotka tulee poistaa käytöstä. Sovellus tulee asentaa siten, että kyseisellä sovelluksella on oma toiminta-alueensa suhteessa muihin sovelluksiin, kuitenkin niin, että sovellukset pystyvät käyttötarkoituksen mukaisesti toimimaan yhdessä kaikissa tilanteissa.

Suuri osa palvelinohjelmistoista on perusasetuksiltaan haavoittuvia. Ohjelmistojen perusturvallisuus luodaan suunnitelmallisilla asetusten valinnoilla. Perusturvallisuutta asetettaessa tulee huomioida seuraavat asiat:

- Asennetaan ohjelmistosta vain käytettävään palveluun tarvittavat komponentit. Asennuksen yksikertaisuus vähentää inhimillisten erehdysten määrää.
- On suositeltavaa antaa ohjelmistoille vain minimisuoritusoikeudet. Tarpeen vaatiessa yksittäisten ohjelmistokomponenttien suoritusoikeuksia voidaan kasvattaa, mutta oikeudet tulee palauttaa välittömästi minimiin, kun tarve lakkaa.
- "Tarve tietää"-periaatteella jaetuin oikeuksin vähennetään myös inhimillisten virheiden määrää.
- Tärkeiden järjestelmien tietoihin ei saa päästä suoraan Internetistä.
- Tietoturvamekanismeja tulee käyttää monella tasolla. Tällöin yhden järjestelmäkomponentin haavoittuvuus ei vaaranna koko tietoliikenneverkon tai -järjestelmän tietoturvallisuutta.

Eri käyttötapoihin liittyvien ohjelmistojen asetusten valinnan erityiskysymyksiä käsitellään jäljempänä tarkemmin kunkin käyttötavan yhteydessä.

3.2.1.4 Seuranta

Käyttöjärjestelmissä on yleensä valmiina perustoiminnot, joilla seurataan järjestelmän toimintaa, mm. käyttöjärjestelmän tuottamat lokitiedot. Lokitiedoista voidaan selvittää sekä järjestelmän virhetilanteita että luvattomia toimintoja, kuten todisteita mahdollisesta tietomurrosta. Lokitietojen kerääminen, niiden suojaaminen, seuranta ja analysointi on järjestelmän valvonnan kannalta tärkeää.

Järjestelmien tietoturvallisuuden valvonnan kannalta Internetiin yhteydessä olevien palvelimien lokitietoja tarvitaan muun muassa:

- Murtoyritysten ja käynnissä olevien hyökkäysten tunnistamiseen ajoissa.
- Tietoliikenteen kapasiteettiseurantaan.
- Tapahtuneiden hyökkäysten jälkiselvittelyyn (sekä omaan verkkoon kohdistettujen että omasta verkosta lähteneiden).
- Vikatilanteiden selvittämiseen.

Järjestelmälokien ensisijainen tavoite on informoida toimintahäiriöistä ja -virheistä. Esimerkiksi WWW-palveluille lokitiedostoja on neljää eri tyyppiä:

- Tapahtumaloki tai käyttöloki, joka luo laitteen tapahtumasta lokimerkin.
- Virheloki, johon kirjataan virheet selityksineen.
- Selaintyyppi-loki, joka kerää tietoja asiakasohjelmistoista eli selaimen tyypeistä.
- Viittausloki, johon kerätään HTTP-yhteyteen liittyviä tietoja ja ne URL-tiedot, mistä asiakasohjelmisto tuli organisaation sivuille.

Seurannan kannalta tärkeitä tapahtumia ovat muun muassa:

- Järjestelmään sisään- ja uloskirjautumiset
- Muutokset järjestelmän tilassa, kuten järjestelmän alasajot ja uudelleenkäynnistykset
- Prosessorin, muistin ja levytilan seuranta sekä virhetapahtumat
- Järjestelmän ja laitteiden raportoimat tilat ja virheet
- Järjestelmässä käytettävien prosessien aloitus- ja lopetusajat, käynnistysparametrit, tilat ja kesto sekä prosessin käyttäjätiedot

- Poikkeavat verkkoliikenteen tapahtumat
- Käyttäjäoikeuksien muutokset

Lokitietojen kerääminen ja analysointi vaatii etukäteissuunnittelua ja aina tulee selvittää:

- Lokitietojen sisältö
- Lokitietojen seurantamekanismi
- Lokitietojen keräämisen sijainti
- Lokitiedostojen tallennuspaikka
- Muista järjestelmistä saatavien lokitietojen merkitys asennettavalle järjestelmälle
- Kuinka kauan lokitietoja saa tai tarvitsee säilyttää

Palomuurin tai muun palvelimen lokitiedot tulee kopioida säännöllisin väliajoin laitteesta sisäisessä verkossa olevalle palvelimelle tai muutoin järjestää niiden säilyminen siten, että niitä ei voida muuttaa tai lukea järjestelmästä itsestään. Lokitiedot voidaan ohjata suojatun yhteyden läpi erilliselle lokipalvelimelle, jonka tehtävänä on ainoastaan kerätä lokitietoja.

Lokitiedoille tulee varata riittävästi tilaa ja määritellä, mitä tehdään, jos lokitiedoille varattu tila täyttyy. Esimerkiksi kirjoitetaanko lokitietoja edellisten tietojen päälle, kuten Windows-ympäristöissä on mahdollista tai suoritetaanko palvelua lainkaan, jos lokitietoja ei voida kirjoittaa. Lokitietojen säilytysaika voidaan määritellä organisaatio-/palvelukohtaisesti.

Lokitiedot eivät saa olla yleisesti saatavilla, vaan pääsy niihin tulee rajoittaa ylläpitohenkilöstölle. Ylläpitohenkilöstö saa käyttää lokitietoja vain teknisiin ylläpitotehtäviin ja muihin tietoturvaliteikan edellyttämiin toimiin, kuten verkon turvallisuuden seuraamiseen³. Teknisen valvonnan järjestämisessä on huomioitava valvonnan järjestämistä ohjaavat säännökset⁴ sekä yksityisyyden suojasta työelämässä annetun lain (477/2001) velvoitteet teknisen valvonnan tarkoituksen ja menetelmien käsittelystä yhteistoimintamenettelyssä henkilökunnan kanssa. Mm. teknisen valvonnan tarkoituksen selkeä määrittely ehkäisee mahdollisia ongelmia myös tietosuojan kannalta. Erityisesti tulee välttää verkon käytön yksilöintiä henkilötasolle eikä lokitietoja saa yhdistellä toisiinsa ilman erityistä syytä.

³ Lisää menettelyohjeita lokitietojen käsittelyyn on Valtionhallinnon sähköpostien ja lokitietojen käsittelyohjeessa (VAHTI 5/2001).

⁴ Velvoite teknisen henkilökunnan vaitiolovelvollisuudesta . (Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999) 7 §; lakiesitys sähköisen viestinnän tietosuojaiksi)

Lokitietojen keräämistä ja käsittelyä säätelee myös henkilötietolaki⁵. Lokitiedoista, jotka sisältävät tunnistettavia henkilöä koskevia merkintöjä, muodostuu henkilörekisteri. Henkilörekisteristä tulee tehdä asianmukainen yleisesti saatavana oleva rekisteriseloste, joka tulee tarvittaessa toimittaa Tietosuojavaltuutetun toimistolle.

Lokitietoja seurattaessa on pyrittävä kiinnittämään huomiota normaalista poikkeaviin tapahtumiin esimerkiksi järjestelmien toiminnassa tai tietoliikenteessä. Tämän takia on seurattava myös lähtevää tietoliikennettä. Epänormaali lähtevä liikenne (esim. Telnet- tai FTP-yhteyden avaukset silloin, kun tiedetään, ettei kukaan henkilökunnasta ole käyttämässä kyseistä laitetta) voi olla osoituksena siitä, että järjestelmässä on tunkeutuja ja/tai Troijan Hevonen, joka avaa yhteyksiä.

Teknisen valvonnan suurin haaste on löytää luvattomat yhteydenottoyritykset lokitiedoista. Tähän on olemassa erilaisia myös lokitietojen valvonta-ohjelmistoja, jotka tarkkailevat lokia, ja mikäli ohjelmisto löytää epänormaalin lokiviestin, se tekee asianmukaisen hälytyksen. Esimerkiksi lokitietojen puuttuminen tietyltä aikajaksolta voi olla merkki ulkopuolisen tunkeutujan toimista.

EHEYDEN VALVONTA

Järjestelmän muuttumattomuuden seurantaan helpottavat tiedostojen eheydenhallintaohjelmat, joiden toiminta perustuu tiivistealgoritmeihin⁶. Eheydenhallintaohjelmat laskevat halutusta kohteesta yhdensuuntaisen funktion avulla tiivisteeseen, joka muuttuu aina, jos alkuperäinen laskettava data muuttuu. Kun tiivisteitä lasketaan ja tallennetaan halutuista kriittisistä tiedoista, laskemalla uudelleen tiiviste saadaan selville, onko luvattomia muutoksia tehty.

Eheydenhallintaohjelmat (kuten Tripwire, Aide) seuraavat valituista tiedostoista edellä mainitulla tekniikalla muutoksia jotka voidaan hylätä tai sallia. Jos muutosta ei sallita, palautetaan tiedot varmistuksilta, joko automaattisesti tai manuaalisesti⁷.

ONGELMATILANTEIDEN JA TIETOTURVALOUKKAUSTEN HALLINTA JA SELVITTÄMINEN

Osana järjestelmien tietoturvallisuuden valvontaa on suunniteltava myös toimintatavat tilanteissa, joissa epäillään luvattomia järjestelmään tunkeutumista tai muuta tietoturvallisuuden loukkausta. Usein tällaiseen tilanteeseen reagoinnin pitää olla nopeaa sekä järjestelmän palauttamisen ja toimintakuntoon saattamisen kannalta että tekijän selvittämiseksi. Organisaatioissa tulee olla nimetty henkilö, joka vastaa seurannasta ja edellä mainittujen tilanteiden käsittelystä.

⁵ Henkilötietolaki (532/1999).

⁶ Esimerkiksi MD5 ja SHA-1.

⁷ Lisää seurantatyökaluja on liitteessä 3.

Valvonnan ongelma on toistaiseksi tietoturvamekanismien, kuten tunkeutumisen havainnointijärjestelmien, vajavainen toiminta ja "porttien kolkuttelujen" suuri määrä. Tunkeutumisen havainnointijärjestelmät eivät ole vielä pystyneet riittävällä tarkkuudella erottamaan todellisia tietoturvaloukkauksia. Järjestelmät paranevat koko ajan ja niiden merkitys tietoliikenteen seurannan apuvälineinä tulee kasvamaan merkittävästi.

Säännöllisellä tietoliikenteen seurannalla ja erilaisia seurantamenetelmiä (tunkeutumisen havainnointi, palomuurin lokitiedot, virustorjunnan lokitiedot) käyttämällä voidaan tietoturvaloukkauksia havaita. Jos merkkejä tietoturvaloukkauksesta ilmenee tulee tilanteesta riippuen:

- Varmistua, että tietoturvaloukkaus on todella tapahtunut
- Selvittää tunkeutumisyrityksen luonne ja tunkeutumisen vaikutuspiiri
- Arvioida aiheutuneet vahingot
- Estää lisävahingot
- Arvioida (muiden) viranomaisten avun tarve, esimerkiksi CERT-FI⁸
- Kerätä todistusaineistoa ja huolehtia sen käytettävyydestä tarkoitukseensa
- Estää uudet tunkeutumisyritykset
- Palauttaa järjestelmä tarvittaessa puhtaalta varmuuskopiolta
- Tehdä tarvittavat ilmoitukset asianomaisille viranomaisille
- Analysoida tilanne ja oppia tapahtuneesta

Järjestelmiin tunkeutujat peittävät jälkensä usein asentamalla järjestelmään "rootkit":ksi kutsutun ohjelmistopakettin, joka muuttaa yleisimpiä järjestelmiä siten, että murtautumisen jäljet ovat vaikeammin havaittavissa.

Mikäli murtautumisen yhteydessä ei pystytä varmasti selvittämään, mitä kaikkea järjestelmään päässyt hyökkääjä on tehnyt, on käytännössä yleensä asennettava käyttöjärjestelmä ja sovellusohjelmat uudestaan alkuperäiseltä medialta tai riittävän varhaiselta varmuuskopiolta⁹.

⁸ Suomessa toimiva tietoturvaloukkauksia seuraava ja ennaltaehkäisevä Viestintäviraston seurantarayhmä lisätietoja ks. <http://www.cert.fi>. Paikallinen poliisi ja Keskusrikospoliisi toimivat myös neuvovina viranomaisina.

⁹ Lisää menettelyohjeita tietoturvaloukkaustilanteiden varalle on ohjeessa VAHTI 7/2001

3.2.1.5 Dokumentointi

Järjestelmään tehdyt tietoturva- ja muut asetukset tulee dokumentoida. Dokumentoinnin tarpeellisuus korostuu järjestelmään tehtävien uudelleen- /lisäasennusten aikana, jolloin pitää tarkkaan tietään järjestelmän tila.

Järjestelmiin tehtävät uudelleen-/ lisäasennukset voivat johtua seuraavista syistä:

- tekniset häiriöt, esimerkiksi levyrikko
- tietojen muuttuminen tahattomien toimintojen, kuten ohjelmointivirheiden, seurauksena
- tietojen muuttuminen tahallisten tekojen seurauksena, esimerkiksi järjestelmään tunkeutujan toimesta
- ohjelmiin tehtävät korjauspäivitykset
- järjestelmän uusiminen toiminnallisista syistä

Kriittisistä järjestelmistä tulee tehdä elpymissuunnitelma. Elpymissuunnitelmassa tulee määritellä kaikki ne toimenpiteet, joilla järjestelmä saadaan rakennettua mahdollisimman nopeasti sen jälkeen, kun järjestelmän toiminta keskeytyy esimerkiksi laiterikon seurauksena.

Järjestelmien dokumentaatio tulee säilyttää erillään järjestelmästä, jotta esimerkiksi tulipalon sattuessa dokumentaatio ei tuhoutuisi. Dokumentaatiota voidaan säilyttää yhdessä nauha- ja digitaalisten varmistusten kanssa, mutta ei samalla tietovälineellä.

3.2.1.6 Varmistukset

Palvelinten tietosisällöstä tulee aina ottaa varmuuskopiot esimerkiksi nauhavarmistuksina. Varmuuskopioinnin tulee tapahtua säännöllisesti esimerkiksi päivittäin, viikoittain, kuukausittain tai näiden yhdistelminä riippuen muun muassa järjestelmän merkityksestä organisaation toiminnan kannalta. Ensimmäiset varmuuskopiot tulee ottaa heti ensiasennuksen jälkeen. Varmuuskopioita tulee aina säilyttää turvallisessa tilassa ja erillään varmistettavista järjestelmistä.

Internet-palvelimet, kuten DNS-, WWW- ja FTP-palvelimet, varmistetaan kaksivaiheisesti. Palvelinten tietosisältö säilytetään sisäisellä palvelimella. ja tarvittaessa tiedot viedään varsinaiselle palvelimelle. Varsinaisesta palvelimesta ei tarvitse ottaa varmuuskopioita kuin käyttöjärjestelmästä ja palvelimen asennusvalinnoista. Tällöin palvelinten tietosisältö, esimerkiksi WWW-sivusto, voidaan tarvittaessa palauttaa ennalleen nopeastikin.

Sähköpostipalvelin ja palvelimet, joiden tietosisältö muuttuu usein, varmistetaan aluksi viikoittain täysvarmistuksilla ja tämän jälkeen muuttuneiden tietojen osalta varmistuksia otetaan päivittäin. Palvelinten kahdentamista suositellaan silloin, kun palvelun merkitys toiminnalle on huomattava. Järjestelmien kahdentamisessa tulee huomioida myös seuraavat asiat:

- Kustannustehokkuus suhteutettuna hallittavaan riskiin
- Vaikutukset järjestelmien ylläpitoon, esimerkiksi ohjelmistopäivitykset tulee tehdä kumpaankin järjestelmään
- Usein pelkkien järjestelmien kahdentaminen ei riitä, vaan joudutaan kahdentamaan esimerkiksi reitittämiä, kytkimiä ja tietoliikenneyhteyksiä

Palomuurista tulee ottaa täysvarmistus heti asennuksen jälkeen. Tämän jälkeen varmistuksia tulee ottaa säännöllisesti. Mikäli palomuuuri tuottaa esimerkiksi suuria määriä lokitietoja ja lokitiedot säilytetään, tulisi viikoittain ottaa täysvarmistus ja muuttuneiden tietojen osalta päivittäin. Turvallisin menetelmä varmistaa palomuuuri on varmuuskopioiden ottaminen paikallisesti esimerkiksi varmistusnauhalle. Tällöin ei tarvitse avata uusia tietoliikenneyhteyksiä, jotka mahdollisesti lisäisivät tietoturvaaukkia. Joissain palomuuuri ratkaisuisissa ei itse palomuurilaitteesta tarvitse ottaa varmuuskopioita vaan riittää, kun varmuuskopio otetaan palomuuureja hallinnoivasta hallintalaitteesta.

3.2.1.7 Testaus

Palvelinta voidaan testata mm. ohjelmistoilla, joilla analysoidaan tunnettuja tietoturvaaukkoja. Testausta on suositeltavaa tehdä säännöllisesti osana järjestelmällistä tietoturvallisuuden seuranta, ainakin korkeaa tietoturvallisuutta edellyttävissä ympäristöissä. Lisäksi voidaan käyttää tunkeutumisen testausmenetelmää, jossa käytetään tunkeutujien käytössä olevien ohjelmistojen kaltaisia välineitä sen testaamiseen, onko järjestelmässä sellaisia haavoittuvuuksia, että niiden kautta voi joko murtautua järjestelmään tai aiheuttaa muuta vahinkoa. Menetelmän käyttö vaatii korkeaa ammattitaitoa ja välineiden käyttötarkoituksesta johtuen tulee käytön olla valvottua.

Uusia tietoturvaaukkia ja haavoittuvuuksia ilmenee päivittäin, koska käytettäviä ohjelmia ja niiden uusia ominaisuuksia kehitetään ja lisätään jatkuvasti. Esimerkiksi päivitetäessä järjestelmissä olevia ohjelmia, niihin tulee lisää ominaisuuksia ja samalla uutta ohjelmakoodia, joka saattaa sisältää uuden haavoittuvuuden.

Ennen järjestelmän tuotantoonottoa palvelimet tulee testata jokaiselta rajapinnaltaan. Internetistä on saatavilla haavoittuvuusanalysointiohjelmia¹⁰, jotka helpottavat palve-

¹⁰ Esimerkiksi NMAP, Nessus tai Retina <http://www.eeye.com/html/products/Retina/index.html>

linten asennusvalintojen testaamista. Näitä ohjelmia on hyvä käyttää säännöllisesti tarkistamaan kaikkien omien verkkolaitteiden tietoturvatilannetta.

Järjestelmään käyttöön otettaessa on hyvä testata muun muassa laitteisto, käyttöjärjestelmä, sovellusohjelmisto, verkkoliitäntöjen osat, reititystiedot, loki- ja hälytystoiminnot sekä palomuurin yhteydessä myös kytkimet, keskittimet ja pakettisuodatukset.

Myöhemmin voidaan toteuttaa säännöllisiä testauksia testaussuunnitelman mukaisesti, johon voi liittää esimerkiksi tietojärjestelmien ja –verkon kuormitustestejä.

3.2.1.8 Ylläpito

Ohjelmista löytyy jatkuvasti uusia tietoturva-aukkoja, jotka voivat avata sisäverkkoa ulkopuolisille. Jotta tietoturvaluottu pystyttäisiin hallitsemaan, tulee organisaatiossa olla jatkuva ja systemaattinen ohjelmistojen ylläpitoprosessi tuotannossa oleville palvelimille ja verkoille. Prosessin tulee kattaa sekä ongelmatilanteet että kehityspäivitykset, jotta organisaation toiminnalle aiheutetaan mahdollisimman vähän ongelmia päivitysten yhteydessä.

Muutostenhallintaprosessin tulee kattaa ainakin seuraavat toimenpiteet:

- Korjauspäivitysten testaus
- Korjauspäivitysten käyttöönotto
- Uusien versioiden käyttöönotto

Tietoturvaohjelmistot, kuten tunkeutumisen havainnointi, haittaohjelmien torjunta- ja sisällöntarkistusohjelmat vaativat jatkuvaa ylläpitoa, koska niiden tietokantojen tulee jatkuvasti päivittyä uusien tietoturvaohjelmien ilmaantuessa. Lisäksi näiden ohjelmien säännöstöjä voidaan ylläpitäjien toimesta itsekkin muuttaa, jolloin voidaan nopeasti ehkäistä esimerkiksi uuden haittaohjelman leviäminen, kun tiedetään jotain haittaohjelman sisällöstä tai toiminnasta¹¹.

Ohjelmistoihin tehdään jatkuvasti uusia korjauspaketteja. Näiden korjauspakettien tarkoituksena on korjata ohjelmassa esiintyneet raportoidut ohjelmistovirheet, joista on aiheutunut tai aiheutuu tietoturvaongelmia. Korjauspakettien asentaminen järjestelmään on harvoin yksinkertaista ja voi aiheuttaa uusia tietoturvaongelmia, koska ohjelmakoodia on paljon ja korjaus voi avata jonkin uuden tietoturva-aukon järjestelmään. Siksi on tärkeää, että korjauspakettien viemiselle tuotantoon on selvät prosessit, jotka kattavat esitestauksen, asennuksen, testauksen ja seurannan.

¹¹ Näitä asioita voi seurata erilaisista tiedoitusryhmistä, kuten www.cert.fi.

Organisaatioiden tulisi analysoida säännöllisesti järjestelmiensä käyttöjärjestelmät, tärkeimmät sovellukset sekä niiden versiopäivitykset. Haavoittuvuusanalyysien tulokset tulee dokumentoida ja havaitut haavoittuvuudet tulee poistaa. Seuraavat korjaavia toimenpiteitä tulee soveltaa:

- Päivitetään järjestelmä tai ajetaan tarvittava korjausajo, joka pienentää löydetyn haavoittuvuuden hyväksyttävälle tasolle.
- Poistetaan tarpeettomat tai haavoittuvat palvelut.
- Mikäli järjestelmää ei voida heti päivittää, tulee järjestelmän haavoittuvuusalttiutta yrittää pienentää, jollain muilla teknisillä tai hallinnollisilla keinoilla.
- Tiukennetaan järjestelmän ylläpitotoimia niin, että taataan järjestelmän päivitysten säännöllisyys.
- Muutetaan organisaation tietoturvasäilytystä, arkkitehtuuria tai muuta dokumentaatiota siten, että voidaan varmistua siitä, että järjestelmäpäivityksiä tehdään säännöllisesti.

Ylläpitäjien tulee seurata myös ohjelmavirheitä itse järjestelmässä sekä ohjelmavirheilmoituksia Internetissä, jotta tiedetään, mitkä ohjelmaversiot ovat turvallisimpia. Lisäksi ylläpitäjien toimenkuvaan kuuluu seurata järjestelmien lokitietoja järjestelmähäiriöiden havaitsemiseksi, ellei organisaatiolla ole keskitettyä seurantamekanismia.

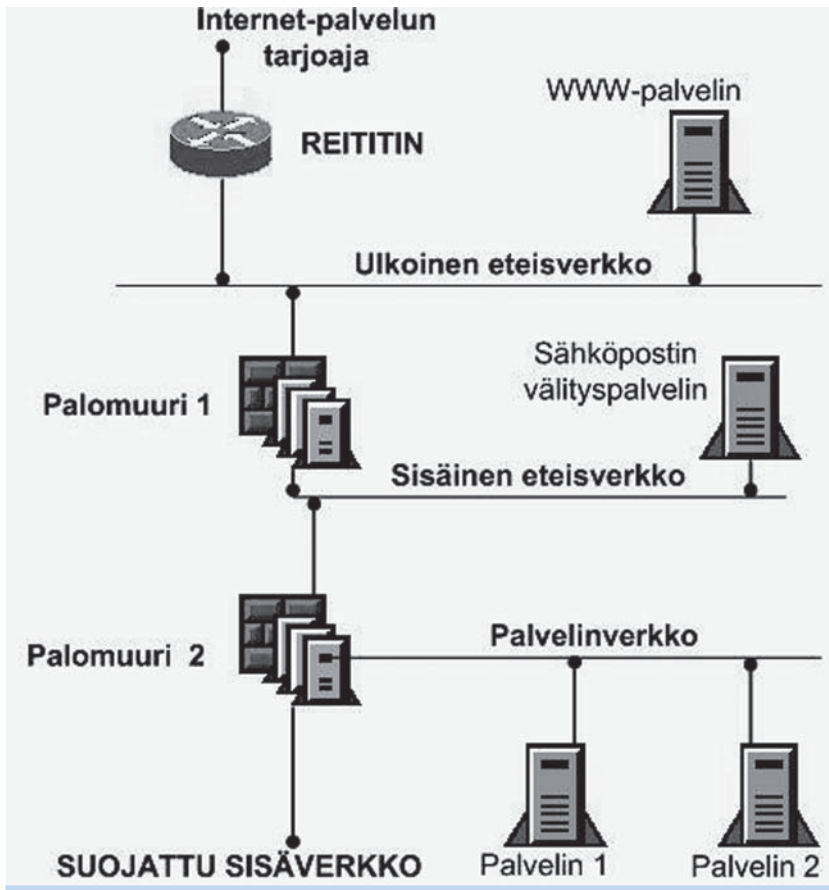
Internetistä on myös saatavilla paljon hyviä tietoturvaohjelmistoja ilmais- ja jakeluohjelmoina. Yksi niiden ongelmista on usein virallisen, sopimus pohjaisen tukipalvelun puute. Toimimattomuusongelmiin tulee ylläpitäjän itse etsiä vastaukset. Joskus vastauksen voi saada teknisten henkilöiden keskusteluryhmiltä. Mikäli ongelma ratkaistaan ylläpitäjän toimesta, tehdään järjestelmään usein uusia ohjelmaosia. Ilmaisohjelmissa saattaa olla myös paljon yhteensovittamista, joihin ylläpitäjät tekevät omia liitännäsohjelmia. Nämä ohjelmamuutokset jäävät helposti dokumentoimatta ja ovat ylläpitäjän vaihtuessa uusi tietoturvaohjelma toimintaympäristölle.

3.2.2 Palomuurin tietoturvasuus

Palomuri on tietoturvamekanismi, joka sellaisenaan ei riitä turvaamaan organisaation tietoja. Palomuri ei ole ratkaisu esimerkiksi ohjelmistojen haavoittuvuuksien hallintaan.

Pienissä organisaatioissa ja kotikäytössä riittää myös ns. pienpalomuurilaitteet, jotka suodattavat tietoliikennettä Internetistä ja sallivat vain ns. perustoimintoja, kuten sähköpostin ja WWW-selailun. Nämä palomuurit on helppo asentaa, yksinkertaisia ylläpi-

Kuva 10. Esimerkki palomuuriratkaisun toteutuksesta



tää ja ne ovat edullisia. Isoimmissa organisaatioissa tarvitaan palomuurilta ominaisuuksia, joita pienpalomuurilaitteet eivät tarjoa, kuten laajennettavuus.

Palomuuuri toimii suojana Internetin ja suojattavan verkon tai sisäverkossa segmentoitavien suoja-alueiden välillä. Palomuuuri on osa ratkaisua ja tarjoaa erilaisia suojaominaisuuksia, kuten esimerkiksi:

- estää muun kuin tarpeellisen tietoliikenteen
- ohjata sisään tulevan tietoliikenteen luotettaviin kohteisiin
- piilottaa sisäverkon suojausta tarvitsevat järjestelmät
- kirjoittaa lokia sisään ja ulos menevästä liikenteestä

- piilottaa tietoja järjestelmien nimistä, verkkotopologiasta, verkkolaitteiden tyypeistä ja sisäisiä käyttäjätunnuksia.

Palomuurilaite tai -sovellus on verkon suojaamisen tärkeimpiä komponentteja. Palomuri ei kuitenkaan ole ratkaisu kaikkeen tietoliikenteen suojaamiseen, koska:

- Sen avulla ei voida kontrolloida tietoliikennettä, joka kiertää palomuurin, kuten erilaiset modeemiyhteydet.
- Kaikki palomuurit eivät tarkastele TCP/IP-pakettien dataosia, ainoastaan protokollat tarkastetaan.
- Aktiivisten yhteyksien tarkistus voidaan suorittaa vain osittain.
- Niin pian kuin yhteys palomuurin läpi on saatu, on mahdollista muodostaa tunneli kyseisestä protokollasta ja ajaa muuta protokollaa tunnelin sisällä.
- Palomuurit eivät suojaa palvelunestohyökkäyksiltä, paitsi järjestelmiä, joihin ei päästetä liikennettä palomuurin läpi.

Pelkästään palomuurin fyysinen asentaminen ei takaa tietoturvallisuutta, vaan palomuriin on asennettava suojaava säännöstö. Palomuuriratkaisua suunniteltaessa ja asennettaessa tulee huomioida kaikki tässä ohjeessa esitetyt toimenpiteet. Näiden lisäksi palomuurin asentamisessa ja ylläpidossa tarvitaan seuraavia toimenpiteitä:

- Selvitetään topologia- sovellus- ja protokollatarpeet
- Arvioidaan palomuuriratkaisuja ja valitaan laite/tuote
- Palomuurin asentaminen
- Palomuurisääntöjen huolellinen testaus
- Suunnitellaan ja toteutetaan lokien kerääminen ja seuranta.

Palomuurin oikea asennus on erityisen tärkeää. Palomuri on asennettava ja ylläpidettävä asiantuntevasti. Lisäksi organisaation verkon Internet-liittymäpisteiden tulee olla kontrolloituja ja palomuurin kiertävät Internet-liittymät tulee kieltää. Palomuurin ohittavia suoria yhteyksiä yksittäisiltä koneilta sisäverkkoon voidaan muodostaa vain käyttäen vahvaa salausta ja käyttäjän vahvaa tunnistusta ja todennusta.

3.2.2.1 Topologia-, sovellus- ja protokollatarpeiden selvitys

Internetiin liitettävän palvelimen toimintaan liittyy aina tietoliikennettä. Uuden tai uudelleen asennettavan järjestelmän topologia-, sovellus-, ja protokollatarpeet tulee selvittää ennen kuin järjestelmä liitetään Internetiin. Selvitystyö ei välttämättä ole helppo,

koska tiedonvälitystarpeet kasvavat kokoajan. Organisaatiossa saattaa olla mitä moninaisempia tietoliikennetarpeita, mutta ilman tarpeiden keräämistä ja dokumentoimista on hankalaa suunnitella toimivaa ja turvallista ratkaisua. Ennen palomuurin asennusta tai päivitystä on tärkeää tietää organisaatiosta ulospäin suuntautuvat sovellukset ja protokollat.

3.2.2.2 *Palomuuriratkaisun arviointi ja laitteen/tuotteen valinta*

Palomuuriratkaisun ja sen teknisen laitteen/tuotteen valinta perustuu organisaation tarpeisiin. Laajennettaessa olemassa olevaa palomuuriratkaisua tai hankittaessa uutta tulee arvioida hankittavan laitteen/tuotteen seuraavia ominaisuuksia:

- Kapasiteetti ja laajennettavuus tulee olla riittävällä tasolla. Mikäli palomuurin tarvitsee tukea myös VPN-ratkaisuja, vaaditaan myös enemmän prosessoritehoa.
- Liittymät jo olemassa oleviin tietoturvamekanismeihin, joita voi olla muun muassa palomuri, todennuspalvelu ja virustorjunta.
- Toiminnot, joista palomuurin tulee suoriutua huomioiden sekä loki- että seurantatoiminnot.
- Hallintaliittymä on ylläpitäjän kannalta sovelias.
- Ratkaisun soveltuvuus organisaation tarpeisiin.
- Palvelintoimittajan luotettavuus ja tuotteen laatutakuut. Laatumittareina toimivat mm. tietoturvasertifikaatit

3.2.2.3 *Palomuurin asentaminen*

Pienpalomuurilaitteiden asentaminen saattaa olla hyvinkin yksinkertaista, mutta mitä monimutkaisempaa ympäristöä palomuri/palomuurit suojaa sitä tärkeämpää on muistaa seuraavat tekijät:

- Palomuuriratkaisun tulisi olla mahdollisimman staattinen ja yksinkertainen, koska näin ylläpidettäessä palomuuria tehdään vähemmän virheitä ja näin ollen muodostuu vähemmän haavoittuvuuksia.
- Laitteita tulee käyttää alun perin suunniteltuihin käyttötarkoituksiin. Esimerkiksi pakettisuodattimet (reitittimet) eivät yleensä riitä suojaamaan organisaation kriittisimpiä tietoja, mutta saattavat riittää suojakerrokseksi WWW-palvelimelle.

- Palomuuriratkaisun tulisi olla monikerroksinen, jotta suojauksen pettäminen yhdessä kohdassa ei avaisi pääsyä koko sisäverkkoon tai organisaation kriittisimpiin tietoihin. Kannattaa käyttää myös palvelinten tarjoamia suojausominaisuuksia, kuten Linux-järjestelmissä olevaa iptables-suojausominaisuutta (netfilter).
- Yhä enenevässä määrin mahdolliset murtohat voivat tulla sisäverkon suunnasta, koska usein kontrolloidaan vain ulkoapäin tulevaa tietoliikennettä. Tunkeutujat voivat käyttää sisäverkkoa hyväkseen sen jälkeen, kun ovat ensin tunkeutuneet palomuurin ohi ja kiertävät sisäkautta haluamiinsa kohteisiin.

Palomuurin asentaminen vaatii huolellisen suunnittelun ja ennalta määritellyn turvallisuus- ja sääntöpolitiikan lisäksi seuraavia toimenpiteitä:

- Palomuurin ensimmäiset asennukset tulisi tehdä testiympäristössä.
- Dokumentoidaan kaikki asennusvaiheet .
- Asennetaan pienin toimiva käyttöjärjestelmäkokoanpano, jos palomuurisovelluksen asennus ei tätä tee.
- Asennetaan kaikki soveltuvat korjaukset, jotka tulee testata ennen tuotantoympäristöön asennusta.
- Rajoitetaan ja minimoidaan käyttäjien ja isäntäkoneiden pääsy palomuurijärjestelmään.
- Estetään pakettien välittäminen, kunnes palomuuriohjelmisto on täysin valmis.
- Otetaan toimivasta järjestelmästä varmuuskopio.
- Valitaan IP-reitityksen asetussäännöt ja otetaan käyttöön IP-osoitteet.
- Määritellään reititysasetukset.
- Toteutetaan palomuurin suodatussäännöstö, kuten pakettisuodatus (ks. 3.2.2.4)
- Asennetaan palomuurin loki- ja hälytysmekanismit.
- Testataan palomuurijärjestelmä.
- Asennetaan järjestelmä tuotantoympäristöön ja testataan uudelleen.

Palomuurin asennuksen ja muutosten yhteydessä järjestelmä tulee aina testata. Palomuurin testaamisessa kannattaa käyttää apuvälineitä aivan kuten palvelimenkin testaamisessa.

Palomuurin asennuksessa tulee myös huomioida, kuinka tehdään vai tehdäänkö ollenkaan osoitteenmuutokset (NAT, Network Address Translation). Palomuuuri suojaa sisäverkon topologian näkymisen ulkoverkkoon vaihtamalla sisäverkon osoitteet virallisiksi Internet-osoitteeksi. Osoitteenmuunnos voidaan tehdä joko staattisesti tai dynaamisesti. Staattisissa osoitemuunnoksissa haluttu sisäverkon (192.168.1.23) osoite muutetaan ulkoiseksi osoitteeksi (192.49.24.199). Dynaamisessa osoitemuunnoksessa käytetään myös portteja hyväksi, jolloin sisäverkon kaikki osoitteet saavat yhden ulkoverkon osoitteen. Avattaessa yhteys, palomuuuri kirjaa, mikä portti on annettu käyttöön avatulle yhteydelle.

3.2.2.4 Palomuurisäännöstö

Palomuurisäännöstöt määrittelevät sallitun ja kielletyn tietoliikenteen Internetistä organisaation sisäverkkoon ja päinvastoin. Palomuurisäännöstöt tulisi pitää yksinkertaisina ja mahdollisimman staattisina ja ne tulee aina dokumentoida. Säännöstöjen ylläpitoa helpottaa säännöstöjen selkeä nimeäminen, ryhmittely ja säännöstöjen ja asetusvalintojen dokumentointi.

Yksinkertaisimmillaan palomuurisäännöstö voisi olla kuten taulukossa 2 on esitetty.

Etäyhteydet lisäävät palomuurin sääntöjä, koska tietoturvalliset etäyhteydet vaativat vahvaa todennusta ja salausta. Käyttäjien etäyhteydetkin on hyvä kontrolloida palomuurin toimesta. Lisäksi tarvittaessa yhteyksiä muihin organisaation osiin tulee esimerkiksi VPN-yhteyksien avaintenneuvottelut sallia palomuurisäännöissä.

Palomuurisäännöstön tulee aina estää seuraavien tietoliikennepakettien välittäminen:

- Todentamattomasta järjestelmästä otetut ylläpito-yhteydet itse palomuurilaitteeseen.
- Internetistä saapuvat tietoliikennepaketit, joiden lähdeosoite on sisäverkon osoite. Tämä voi olla merkki IP-lähdeosoitteen väärennöksestä.
- Internetistä saapuvat tarpeettomat ICMP-paketit¹².
- Ns. varattuihin IP-osoitteisiin luokitellut osoitteet, jotka sekä saapuvat tai lähtevät Internet-rajapinnalta.
- Todentamattomasta järjestelmästä tulevat SNMP-paketit.
- Internetistä saapuvat tietoliikennepaketit, jotka sisältävät lähdereititystietoja.

¹² Pakollisista Palomuurissa sallittavista ICMP-paketeista löytyy lisätietoja RFC2979.

Taulukko 2. Esimerkki palomuurisäännöstöstä pakettisuodatinpalomuurille

NRO	LÄHDE-OSOITE	LÄHDE-PORTTI	KOHDE-OSOITE	KOHDE-PORTTI	TOIMINTO	KUVAUS
1	Any	Any	192.168.1.0	> 1023	Allow	Sallitaan sisäverkkoon palaavat TCP-yhteydet (ei SYN yhteyksiä)
2	192.168.1.1	Any	Any	Any	Deny	Palomuurista itsestään ei sa suoraan yhteyttä mihinkään
3	Any	Any	192.168.1.1	Any	Deny	Kukaan ei pääse suoraan palomuurilaitteelle Internetistä
4	192.168.1.0	Any	Any	Any	Allow	Sisäverkon käyttäjät pääsevät Internetin palveluihin
5	Any	Any	192.168.1.2	SMTP (25)	Allow	Sallitaan sähköpostin lähettäminen sähköpostipalvelimella Internetistä
6	Any	Any	192.168.1.3	HTTP (80)	Allow	Internet -käyttäjät pääsevät WWW-palvelimelle
7	Any	Any	Any	Any	Deny	Estetään kaikki muu liikenne kuin edellä sallitut

- Saapuvat tai lähtevät tietoliikennepaketit, joiden lähde- tai kohdeosoitteena on ns. localhost-osoite (127.0.0.1). Yleensä nämä paketit viittaavat hyökkäykseen itse palomuurilaitetta vastaan.
- Saapuvat ja lähtevät tietoliikennepaketit, joiden lähde- tai kohdeosoite on 0.0.0.0. Jotkut järjestelmät tulkitsevat osoitteen joko localhost-osoitteeksi tai kaiutusviestiksi (broadcast).
- Kaiutusosoitteisiin saapuvat ja lähtevät tietoliikennepaketit.

Alla on esitetty esimerkki palomuurin tietoturvapoliitikasta, jonka oletuksena on, että mikä ei ole erikseen sallittua on kiellettyä. Yksinkertaisimmillaan palomuri sallii tämän politiikan mukaan seuraavat toiminnot:

- DNS-nimipalvelun kyselyt, jotka tapahtuvat porttiin 53 UDP-protokollalla ja TCP-protokolla tehdään siirrot luotettavaan nimipalvelimeen.
- Sähköpostin välitys sisäisestä postipalvelimesta palveluntarjoajan palvelimelle tai suoraan vastaanottajan palvelimeen.

- Sähköpostin välitys palveluntarjoajan palvelimelta tai suoraan lähettäjän koneelta sisäverkon sähköpostipalvelimelle.
- WWW-selailu (HTTP) sisäverkosta ulkoverkkoon.
- Palomuurilaitteen etähallinnointi esimerkiksi SSH-protokollalla.

Palomuurijärjestelmän asennuksessa ja ylläpidossa on huolehdittava erityisesti palomuurin säännöstöstä. Säännöstön tulisi olla mahdollisimman yksinkertainen. Usein isoissa organisaatioissa palomuurisäännöstöt kasvavat ja niiden hallinnointi on hankalaa. Säännöstöjen ylläpitoa helpottaa säännöstöjen ja sääntöjen selkeä nimeäminen, ryhmittely sekä säännöstöjen ja asetusvalintojen dokumentointi.

3.2.2.5 Palomuuuri osana verkon suojaustoimenpiteitä

Palomuuuri on keskeisin osa verkon tietoturvallisuutta, mutta se ei pelkästään riitä. Palomuurin lisäksi voidaan tarvita välimuisti-, sisällönsuodatus- ja tunkeutumisen havainnointijärjestelmiä. Näiden järjestelmien yhteentoimivuus palomuurin kanssa tulee ottaa huomioon palomuurin valinnassa ja asennuksessa.

Välimuistipalvelin toimii sisäverkossa Internetistä haettujen tietojen tallentaja. Palvelin tallentaa käytetyimmät WWW-sivut levyilleen, jolloin kaikkea tietoa ei tarvitse hakea Internetistä käsin. Tämä nopeuttaa tietojen hakua ja vähentää palomuurin tietoliikennettä. Lisäksi välimuistipalvelimella on mahdollista tehdä kattavampaa sisällönsuodatusta kuin palomuurissa. Koska Internetin haittaohjelmien määrä on jatkuvasti kasvanut ja niitä on jo esiintynyt HTTP-liikenteessä, tulee jatkossa miettiä pitääkö kaikki HTTP-liikenne suodattaa haittaohjelmilta.

Useimmat organisaatiot ovat haittaohjelmien poistamiseksi hankkineet erillisen sisällönsuodatuspalvelimen, joka suodattaa lähinnä sähköpostiliikenteen mukana kulkeuvia haittaohjelmia. Sisällönsuodatuspalvelin pystyy havaitsemaan HTTP-, FTP- ja SMTP-tietoliikenteen mukana tulevat haittaohjelmat, mutta ei esimerkiksi salatun HTTPS-liikenteen. Ongelmana on koko ajan kasvanut tietoliikenteen määrä ja tästä syystä kaikkea tietoliikennettä ei suodateta sisällöllisesti. Sisällönsuodattimet purkavat dataliikennettä, kun taas tunkeutumisen havainnointijärjestelmät seuraavat muun muassa tietoliikennepaketteja, datavirtaa ja levyaluemuutoksia.

Kun verkon tunkeutumisen havainnointijärjestelmiä asennetaan, tulee organisaation normaali tietoliikenne jo olla mahdollisimman tarkasti tiedossa, jotta pystyttäisiin havaitsemaan oikeat hyökkäystapahtumat vääristä hälytyksistä. Tietoliikennettä on voitu seurata palomuurin ja muiden Internet-palvelinten lokitiedoista sekä muista tietoliikenteen seurantamenetelmistä, kuten verkonkuunteluohjelma (esim. Sniffer). Verkon

tunkeutumisenhavainnointi-palvelimet valvovat tietoliikennettä yleensä yhdessä aliverkossa ja pyrkivät havaitsemaan hyökkäyksiä vertaamalla tunkeutumisjälkiä havainnointijärjestelmissä olevien tunnettuihin hyökkäysmalleihin ja -jälkiin.

3.3 Internetistä saatavien palveluiden käyttäminen

Internetissä on tarjolla lukuisia erilaisia palveluita tiedonhausta verkkokauppoihin. Organisaation tulee ohjata omistamiltaan laitteilta tapahtuvaa työntekijöiden Internet-käyttöä tarvittavilta osin.

Seuraavissa kappaleissa on esitetty asioita, joita organisaation ja sen työntekijöiden tulee huomioida käyttäessään Internetiä.

3.3.1 Tietojen haku ja muiden palveluiden käyttö

Internet-verkon peruskäyttöä on verkossa saatavilla olevien erilaisten tieto- tai muiden resurssien käyttö. Internet-käytön tietoturvallisuuden kannalta oleellista on käyttöön liittyvien tietoturvariskien hallinta. Suositeltavin ja tehokkain tapa huolehtia organisaation Internet-liittymän tietoturvallisuudesta on teknisesti estää sellaiset protokollat, sovellukset ja yhteydet joita työtehtävien kannalta ei tarvita. Toisaalta palveluja tarvittaessa, voidaan osa toteuttaa siten, että vain ne työntekijät/ työntekijäryhmät joilla on erikoissovelluksiin työtehtävien kautta tuleva käyttötarve, pääsevät näitä sovelluksia käyttämään. Esimerkiksi joidenkin teknisten asiantuntijoiden uutisryhmiin osallistuminen, jolloin he sitä kautta saavat tarvittavaa tietoa teknisten ongelmien ratkaisuun.

Peruskäyttöyhteyksien kautta voi olla pääsy myös sellaisiin palveluihin ja sovelluksiin, joita ei tarvita normaalissa työympäristössä ja joihin liittyy erityisiä tietoturvariskejä. Näiden käyttö on syytä yksityiskohtaisesti ohjeissa kieltää¹³.

Internetissä kuka tahansa voi julkaista mitä tahansa. Vaikka Internet-pohjaisen tiedon luotettavuuden arviointi ei ehkä ole suurempi ongelma kuin normaaliin yleissivistykseen kuuluva lähdekritiikki, organisaatiossa voi olla järkevää organisoida ja systematisoida tietolähteiden käyttö. Organisaatio voi antaa esimerkiksi sisäisen tietopalvelun tehtäväksi organisaation toimialaan liittyvien tietolähteiden kartoittamisen jolloin luotettavuuden arviointi ei jää yksittäisen työntekijän vastuulle.

¹³ Ks. ohjemalli liitteessä 1

Joissakin organisaatioissa voi olla tarvetta korostaa myös sitä, että tekijänoikeussäännöt ovat voimassa myös Internetissä. Vaikka Internet on nimenomaan tiedon jakelukanava, tulee varsinkin tietoa lähdeaineistona käytettäessä huomioida ns. moraaliset tekijänoikeudet, eli tiedon lähteet pitää mainita samalla tarkkuudella kuin muidenkin kirjallisten aineistojen. Tekijänoikeuksilla suojattujen aineistojen väärinkäyttö (esim. musiikin imurointi P2P järjestelmillä työpaikoilla) on laitonta eikä sitä sinänsä tarvitse erikseen kieltää. Sen sijaan voidaan tehdä selväksi, että joillakin sovelluksilla ei ole hyväksyttävää käyttötarkoitusta työympäristössä.

Tekniseen tietoturvallisuuteen kuuluu järjestelmien tietoturva-asetusten valinta mahdollisimman turvallisiksi kuitenkin niin, ettei normaali työkäyttö esty. Selainten ja muiden ohjelmien tietoturva-asetukset tulee mahdollisuuksien mukaan toteuttaa niin, ettei niitä päästä muuttamaan työntekijän toimesta. Selaimet ovat merkittävä komponentti Internet-käytön tietoturvasuojauksessa, joten myös niihin pätevät samat perussäännöt kuin Internet-yhteyspalvelinten asentamisessa ja ylläpidossa:

- käytetään turvallisiksi arvioitua selainversiota
- asennetaan selaimet järjestelmiin keskitetysti ja poistetaan jo asennusvaiheessa selainohjelmista mahdollisimman paljon niiden tietoturvaheikkouksista
- selainten turvapäivityksiä seurataan aktiivisesti
- järjestetään tehokas päivitysten asentaminen työntekijöiden työasemille ja pidetään kirjaa päivitystilanteesta.

Haittaohjelmien torjunnassa käyttäjien työasema on aina tärkeä kohde. Torjunnan tehoon vaikuttaa selaimen ja muiden työasemaohjelmistojen asetukset, itse selainohjelmisto ja -versio sekä automaattisesti päivittyvä virustorjuntaohjelmisto. Joissakin tilanteissa lisäarvoa voi suojaukseen tuoda myös työasemassa oleva palomuuriohjelma, joka havaitsee epäasiallisen (esim. Troijan Hevosen tuottaman) verkkoliikenteen.

Välityspalvelimen välimuistiin jää tietoja muun muassa käyttäjien WWW-selailusta tai sähköposteista. Välimuistipalvelimien ylläpidon kannalta on huomioitava työntekijöiden tietosuoja, varsinkin jos sellaisia viestintään liittyviä sovelluksia on käytössä, joista tallentuu tietoja välimuistipalvelimeen.

3.3.2 Asioiminen ja ostaminen Internetissä

Internet on tehokas ja nopea kanava esimerkiksi hankintojen ja niihin liittyvien toimintojen suorittamiseen. Pääsääntöisesti vastuu ulkopuolisten palveluiden toteutusten tietoturvasuojauksesta on palvelun tarjoajalla, mutta tilanteesta riippuen palveluiden käytössä voi siirtyä myös tietoja joiden oikeellisuus tai luottamuksellisuus voi olla tilaajan

vastuulla. Lisäksi Internetiä palvelu- tilaus- tai toimituskanavanaan käyttävien tahojen sopimusten vastuunjakoon voi sisältyä seikkoja, jotka edellyttävät myös tilaajan pysyvän tiedostamaan käytettävän sovelluksen tekniseen toteutukseen sisältyvät riskit. Soveltuvien osin Internetistä saatavien palveluiden tietoturvallisuuden arviointiin voi soveltaa tässä ohjeessa esitettäviä teknisiä ratkaisuja.

Edellä mainitusta syystä tietohallinnon asiantuntijoiden on syytä osallistua palveluiden käyttöönottovaiheessa niiden tekniseen arviointiin ja tarvittaessa käytön ohjeistamiseen. Tilaus- ym. valtuuksiin ja työjärjestyksen määräyksiin voi tätä kautta tulla lisävelvoitteita tietoturvallisuuden osalta.

3.4 Internetissä tarjottavat palvelut

Valtionhallinnon organisaation Internetissä tarjoamat peruspalvelut ovat yleensä tiedotusta ja yleistä neuvontaa viranomaisen toiminnasta ja sen palveluista sekä kansalaisten oikeuksista ja velvollisuuksista palveluiden käyttäjänä.

Internetin WWW-palvelimet ovat tyypillisiä hyökkäysten kohteita, koska osa WWW-palvelinohjelmistoista on hyvin haavoittuvia ja WWW-sivustojen asiattomaan muuttamiseen on olemassa useita valmisohjelmia. Suurin uhka tiedotuspalvelimille on yleensä väärin tai puutteellisen asennusvalintojen tai uusien, vielä paikkaamattomista ohjelmien haavoittuvuuksista johtuva ilkeävaltainen murtautuminen ja sivujen muuttaminen. Tämän lisäksi voidaan murrettua WWW-palvelinta käyttää uusiin tietomurtoihin tai palvelinta käyttää muuten luvatta muuhun tarkoitukseen. Vaarana on myös että WWW-palvelin ei pysty palvelemaan käyttäjiä, jos palvelunestohyökkäys (DoS, Denial of Service) tai hajautettu palvelunestohyökkäys (DDoS, Distributed Denial of Service) varaa kaikki palvelun tarjoamat resurssit.

Viranomaisen tiedotuspalvelussa tiedon oikeellisuus eli sisällöllinen ja tekninen eheys on ensiarvoisen tärkeää. Vaikka tahalliset sivujen muutokset voivat olla helposti havaittavissa, teknisen muuttumattomuuden varmistamiseen kannattaa käyttää aikaisemmin mainittuja eheyden valvontaan tarkoitettuja ohjelmistoja.

Tietojen käytettävyyden on osa tietoturvallisuutta. Tietojen luotettavuutta lisää tieto- ja asiointipalvelujen tarjoaminen käyttäen standardien mukaisesti toteutettua WWW-käyttöliittymää (HTML-standardeja sekä siihen liittyviä mm. CSS, DOM, XML, ECMAScript ym. standardeja¹⁴). Palvelun ominaisuuksilla ei pidä ohjata käyttäjää käyttämään

¹⁴ Näistä vastaa suurelta osin WWW-consortium eli W3C, <http://www.w3.org/>. Suomessa standardointityötä tekee Tietoyhteiskunnan kehittämiskeskus ry, <http://www.tieke.fi/standardointi.nsf>

tietoturvallisuudeltaan heikoiksi tunnettuja selaimia tai niiden versioita. Selainkohtaisia ominaisuuksia HTML-kielestä ei tule käyttää. Palveluiden tulee tarvittaessa olla käytettävissä myös tekstipohjaisilla selaimilla tai olla sovitettuja useamman tyyppisille päätelaitteille.

Tiedon eheys Internet-palveluissa varmistetaan palvelinten suunnitelmallisella ylläpidolla. Koska kyseessä on organisaation ulkoisen kuvan kannalta varsin näkyvä asia, on sekä tietojen sisällöllinen että tekninen ylläpito- ja siirtomenettely suunniteltava ja toteutettava huolellisesti. Tarvittaessa niin, että toiminnassa on riittävä työnjako sekä perustehtävien että hyväksymisen ja valvonnan osalta.

Tiedotuspalvelimen tietosisällön varmistus mahdollisen eheysongelman varalta voidaan toteuttaa osittain kytkemällä se osaksi tietojen ylläpitomenettelyä niin, että tiedot säilytetään ja ylläpidetään sisäverkossa olevalla turvalla palvelimella, jonka kautta julkaistavat tiedot siirretään julkiseen palvelimeen. Vertailemalla näiden kahden palvelimen tietosisältöä (esimerkiksi ohjelmallisesti) voidaan tarvittaessa varmistua tiedotuksen oikeellisuudesta. Palvelimen julkisten tietojen päivitys voidaan hoitaa esim. automaattikopiona sisäisestä koneesta. Kaikki etäkäyttöön tarkoitetut sisällönmuokausohjelmat tulee poistaa varsinaiselta WWW-palvelimelta, koska niiden säilyttäminen verkkopalvelimella on tietoturvariski.

Eräs julkisen palvelun huolellisen sisällön ylläpidon peruseräpäätteitä on, ettei palvelimelle sijoiteta mitään sellaista, mikä ei ole tarkoitettu julkaistavaksi, edes palvelimen sellaiseen osaan, mistä tieto ei normaalitilassa ole kaikkien luettavissa. On muistettava, että WWW-palvelimen datahakemiston kaikki tiedostot voivat olla haettavissa (tämä kannattaa kuitenkin käytettävissä olevin teknisin keinoin mahdollisimman pitkälle estää), vaikka niitä ei olisikaan linkitetty tietyille WWW-sivuille. Tiedostonimien arvaaminen on usein helppoa. Samoin tietoa ei pidä siirtää palvelimelle ennen virallista julkaisupäivää.

Joidenkin palvelujen osalta on ehkä tarpeen ottaa kantaa tietopalvelimen toimintatarpeeseen myös poikkeusoloissa. Erityisesti, jos palvelimella on turvallisuuden kannalta tärkeää tietoa.

Tietopalveluiden palvelinohjelmistoissa on yleensä ominaisuuksia, joiden avulla voidaan toteuttaa "kevyt" käyttäjien tunnistus ja todennus käyttäjätunnuksen ja salasanan avulla (ns. basic authentication) tai rajoittaa käyttöä yhteydenottajan verkko-osoitteen perusteella. Näiden käyttöä ei suositella, koska tietopalveluiden käyttämisen yhteydessä ei yleensä ole tarpeen tunnistaa käyttäjää ja tietopalvelinohjelmistojen salasanamenettely on yleensä tietoturvallisuudeltaan heikko. Mikäli "kevyttä" tunnistusta kuitenkin perustellusti tarvitaan, sen toteutuksessa on otettava huomioon, että palvelinohjelmistoihin sisältyvä salasanan base64-koodaus ei ole salausta vaan helposti muutettavissa selväkieliseksi eli salasana on suojattava muulla tavoin, esim. käytettävä yhteyden salaamiseen SSL:ää. Lisäksi käyttäjätietojen kerääminen edellyttää aina

henkilötietolain¹⁵ noudattamista mm. informointivelvoitteen (rekisteriseloste), käytön suunnitelmallisuuden (esim. henkilötietojen käyttötarkoituksen määrittely) ja tietojen suojaamisen osalta. Kevyissä tunnistusmenetelmissä valmiina olevien käyttäjätunnus- ja salasana-tietojen turvallinen säilytys vaatii myös yleensä erityishuomiota (salaus, säilytyspaikka ja sen suojaus). Myös tiedotuspalvelimeen voi olla aiheellista toteuttaa mahdollisuus varmistaa palvelimen oikeellisuus SSL-varmenteella, jolloin käyttäjä voi tarkistaa asioivansa oikean palvelimen kanssa.

WWW-järjestelmässä on yleisessä käytössä lähinnä SSL-tekniikkaan perustuva salaus ja tätä kannattaa hyödyntää aina, kun se on mahdollista ja vähintäänkin silloin, jos ollaan tekemisissä tietokantatietojen kanssa. Mikäli asioija pääsee muuttamaan tietoja, tulee vaatia vahvempaa tunnistamista ja todentamista lähinnä julkisen avaimen järjestelmään perustuvilla ratkaisuilla.

Tietopalvelin tulee erottaa omaksi tähän tarkoitukseen varatuksi laitteistoksi, jolle käytetään palveluntarjoajan hotellipalvelua. WWW-palvelimen tietoturvasuojaa voidaan lisätä sijoittamalla palvelin suojattuun verkkoon. Jos WWW-palvelin sijoitetaan ulkoiselle eteisverkkoalueelle, kuten kuvassa 10, tulee reitittimen/palomuurin estää muu kuin HTTP- ja HTTPS-liikenne WWW-palvelimelle. Vaihtoehtoisesti voidaan palomuuriratkaisussa tehdä oma suojattu aliverkko, jolloin palomuurisäännöstö estää ylimääräisen tietoliikenteen WWW-palvelimelle. Julkista WWW-palvelinta ei pidä koskaan sijoittaa organisaation sisäverkkoon.

WWW-palvelimet tuottavat haettavan tiedon usein ns. sisällöntuottamisohjelmistojen avulla (esim. CGI, ASP, PHP). Näiden ohjelmistojen käyttöönoton ja asennuksen yhteydessä tulee huomioida turvallisen ohjelmoinnin periaatteet sekä sisällöntuottamisohjelmistojen tyypilliset tietoturvaominaisuudet:

- liittymät ja ohjelmakutsut muihin ohjelmistoihin
- tarkistetaan, että kaikki valmiskomponentit, joita käytetään WWW-palvelussa eivät sisällä virheitä tai ylimääräisiä ohjelmaosia.
- estetään kaikki palvelimen SSI-komennot (Server Side Include), joiden avulla saadaan käyttöön sivuille lisättävät ulkoiset ohjelmat.
- kaikkien ohjelmien toiminta tulee testata erillisessä testikoneessa ennen tuotantoon asennusta
- tietoturvaohjelmille altistumista voidaan testata työkaluilla
- asennetaan ohjelmat niin, että koodin suoritus tapahtuu mahdollisimman vähin oikeuksin ja huomioidaan tämä mm. ohjelmistokoodin sijoittelulla hakemistorakenteeseen

¹⁵ Henkilötietolaki (523/1999)

- vältetään WWW-sivustojen asentamista oletushakemistoihin ja oletustiedoilla
- määritellään HTML-sivujen merkkijärjestelmä yksityiskohtaisesti
- ohjelmalle annettavat syötteet pitää tarkistaa ja virheelliset syötteet tulee hylätä.

Sivujen toteutuksessa ei suositella käytettäväksi toiminteita, joita voidaan pitää käyttäjän/asiakkaan kannalta riskinä, koska silloin voidaan ohjata näitä hyväksymään tietoturvallisuuden kannalta riskialttiita tekniikoita. Myöskään muita kuin tilapäisiä evästeitä ei suositella käytettäväksi palveluissa muuhun tarkoitukseen kuin palveluistunnon vuorovaikutus- tai tapahtuman tilan hallintaan.

WWW-palvelinohjelmistojen kohdalla on lisäksi kiinnitettävä huomiota seuraaviin asioihin.

- Useimmilla palvelinohjelmistoilla on pääsy kaikkiin tai useimpiin palvelinkoneen tiedostoihin ja näiden tiedostojen suoja on palvelinohjelmiston oikeiden asetusvalintojen varassa. Tämän takia palvelinohjelmisto on asennettava näyttämään tiedostoja vain rajatulta levyalueelta.
- Erityistä huomiota on kiinnitettävä hakemistoviittauksiin, kuten Unixin symbolisiin linkkeihin. Yksinkertainenkin virhe näiden asetuksessa saattaa avata koko palvelimen tiedostojärjestelmän ulkomaailmalle¹⁶.

Tietojen hakupalvelut käyttävät ns. hakurobotteja WWW-tiedon indeksien ja hakemistojen luomiseen. Hakurobottien toiminnasta ja mahdollisuuksista vaikuttaa siihen, mitä tietoa palveluista hakukoneiden kautta löytyy on syytä olla tietoinen ja käyttää näitä mahdollisuuksia hyväksi (esim. robots.txt-tiedosto). Osa hakuroboteista kerää myös sähköpostiosoitteita ei-toivotun kaupallisen viestinnän tarpeisiin.

Myös yleisimmissä palvelinkäyttöjärjestelmissä on valmiina tai saatavilla palvelinohjelmistoista riippumattomia yhteyksien rajoitustoimintoja (kuten Unixin TCP-wrapper). Näitä kannattaa käyttää tarpeen mukaan, erityisesti ulko- tai eteisverkossa toimiviin palvelimiin voidaan valita rajoitusasetuksiin organisaation käytössä olevat verkko-osoitteet, jolloin asetusvirhe palomuurissakaan ei päästä hyökkääjää palvelimelle.

Palvelun tarjoajan tulee myös miettiä, mitä lokitietoja palvelimesta kerätään ja kuinka niiden asiallinen käsittely hoidetaan (kts. kohta 3.2.1.4).

¹⁶ Esimerkiksi `cd html-data; ln -s / juuri; lynx http://localhost/juuri/`

- Asiointijärjestelmässä tarvittavat vuorovaikutteiset ominaisuudet ja mahdollisuudet selvittää mahdolliset ongelmatilanteet muita kanavia käyttäen. Esimerkiksi muutosmahdollisuudesta: Kuinka asiakas voi muuttaa syöttämiään tietoja, jos hän on havainnut virheen, mutta on jo ehtinyt lähettää tiedot?
- Pystytäänkö järjestelmällä hoitamaan koko asiointiprosessi, joka muodostuu esimerkiksi seuraavista toiminnoista: asian vireillepano, ilmoittaminen, tiedoksisaanti, valtuutus ja kuittaus.
- Kaikki asiointitapahtumat tulee arkistoida (esim. tarvittaessa alkuperäinen sähköisesti allekirjoitettu viesti) ja diarisoida. Asioinnin kirjaamotointi riippuu asioinnin teknisestä toteutuksesta¹⁹.

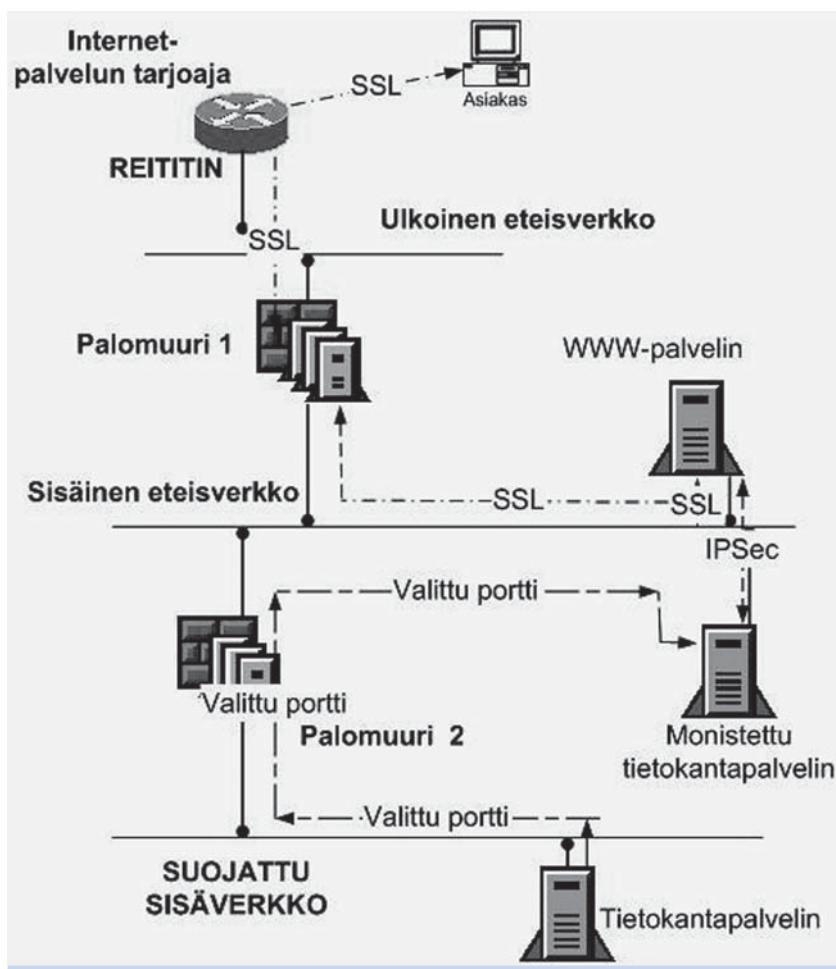
Asiointijärjestelmä koostuu usein edustapalvelimesta (WWW-palvelin) ja tietokantapalvelimesta sekä näiden välisestä yhteydestä, jossa tiedon kulku tulee suojata koko ketjun osalta. Ensimmäinen suojauskeino on sijoittaa tietokantapalvelin sisäiseen eteisverkkoon, kuten kuvassa 11. Usein tietoturvaa lisätään pitämällä varsinaisesta tietokantapalvelimesta kopiota sisäisessä eteisverkossa ja siirtämällä datat säännöllisesti yhdensuuntaisesti varsinaisesta tietokannasta kopiotietokantaan. Lisäksi tietoturvaa voidaan parantaa monistetun tietokantapalvelimen suojaamisella niin, että vain WWW-palvelimelta on oikeus tehdä suorittavia tarkoin rajattuja toimenpiteitä tietokantapalvelimelle.

Asioija ottaa yhteyden asiointipalvelimeen, josta suoritetaan tarvittavat tiedon haut tietokantapalvelimelta. Muu kuin käsiteltävänä oleva salaisena pidettävä data ei saa sijaita asiointipalvelimessa tai sen on oltava salattuna, jotta vahinko tietomurron yhteydessä jäisi mahdollisimman pieneksi.

- Asiointi vaatii tietojensa luonteen takia usein suojatut yhteydet asiointipalvelimelle, jotka useimmissa tapauksissa toteutetaan käyttäen SSL-protokollaa. SSL-suojaa yhteyden asioijan ja asiointipalvelimen välillä, mutta ei sinänsä suorita asiakkaan tunnistusta. Tunnistamiseen tulee käyttää esimerkiksi henkilökorttiratkaisua.
- Uudelleen tunnistautumista voidaan vaatia tietoturvan lisäämiseksi. Tällä varmistetaan, että kerran kirjautunut asioija on sama asioija, joka aloitti yhteyden.

¹⁹ Arkistointilaitoksen antamia ohjeita liittyen sähköiseen kirjaamotointiin löytyy osoitteesta narc.fi.

Kuva 11. Esimerkki tietokantapalvelimen sijoittamisesta asiointia varten



Salausmekanismeihin liittyy aina avaintenhallintaa, josta tulee huolehtia palveluja tarjottaessa. Esimerkiksi, kuinka järjestetään voimassa olevien avainten tarkastus. Samoin varmenteita käytettäessä tulee huolehtia siitä, että järjestelmässä ja käytettävissä varmennepalveluissa on riittävät toiminnot varmenteiden tarkistamiseen, kelpuuttamiseen, vanhentumiseen ja peruuttamiseen²⁰. Latautuvien toiminteiden käyttöä ei suositella.

²⁰ Laki sähköisestä allekirjoituksesta (14/2003) edellyttää näitä ominaisuuksia laatuvarmenteilta.

Asiointijärjestelmässä on myös tarvittaessa ratkaistava menetelmä, kuinka asioijan antamat tiedot viedään asiointijärjestelmään tai tietokantaan. Jos tietoja ei tarvitse välittömästi päivittää, voidaan tehdä erillisiä päivitysajoja tietokantaan syötetyistä tiedoista, jotka tulee viedä heti talteen turvalliseen paikkaan ja muualle kuin asiointijärjestelmään. Kun päivitykset tulee tehdä välittömästi, ei kuvassa esitettyä kopiotietokantaa voi olla. Tällöin yhteys otetaan suoraan varsinaiseen tietokantaan. On huomattava, että suora tietokantayhteys on monesta syystä riskialttein vaihtoehto.

Jos julkisissa asiointipalveluissa tarvitaan Javaa, JavaScriptejä tai PHP:tä (Hypertext Preprocessor), tulee niiden ohjelmoinnissa ja asentamisessa huomioida niiden tietoturvaheikkoudet. Palveluita ei myöskään tule rakentaa käyttäen ActiveX:ää.

Mikäli riittävää suojaustasoa ei voida saavuttaa, ei asiointipalvelua voida toteuttaa avoimessa tietoverkossa.

3.5 Internetin käyttö organisaatioiden väliseen ja sisäiseen tiedonsiirtoon

Internetiä käytetään yhä enemmän organisaatioiden väliseen tiedonsiirtoon, koska Internet-tekniikat ja yhteiskunnan tiedonvälitystavat ovat muuttuneet käytettävimmiksi ja yhdenmukaisemmiksi.

Internetiä voidaan käyttää esimerkiksi yhdistämään organisaation eri toimipisteiden verkkoja tai järjestää eri organisaatioiden välinen tietojen välittäminen joko automatisoituna sovelluksesta - sovellukseen siirtona tai ns. eräsiirtona. Mahdollista on myös, että organisaatio käyttää ulkoistettua järjestelmää Internet-verkon kautta ostaen sen palveluna ulkopuoliselta (ASP). Kaikissa näissä tapauksissa on tarpeen mukaan huolehdittava sekä tiedonsiirron salauksesta että käyttäjien tai tiedon alkuperän riittäväs-tä todentamisesta.

Organisaation tietoturvamennettelyissä tulee huomioida erikseen tietoturva vaatimukset, joita edellytetään, jos organisaatioiden sisäistä sekä organisaatioiden välistä tiedonsiirtoa tapahtuu Internetin välityksellä. Tiedonsiirto voi olla sähköposti-, EDI-, puhe²¹- tai videoneuvotteluliikennettä sekä tietojärjestelmien etäylläpitoon liittyvää tietoliikennettä. Riippumatta tiedonsiirtotavasta luottamuksellista tietoa ei saa välittää salaamattomana Internetin yli sekä käyttäjien ja kohteiden (esimerkiksi dokumentit, palvelinlaitteet, etätyöskentelylaitteet) tunnistamiseen ja todentamiseen tulee kiinnittää erityistä huomioita

²¹ VoIP eli Voice over IP

Organisaation sisäisessä ja välisessä tietojen siirrossa Internetin välityksellä tulee huomioida, millaista tiedonsiirtoa organisaation toiminnan kannalta tarvitaan ja kuinka tiedonsiirto tapahtuu turvallisesti. Esimerkiksi tietojärjestelmien etäylläpito edellyttää aina vahvaa salausta ja tunnistusta²².

Jos välitetään säännöllisesti tietoja Internetin yli kahden kohteen välillä, niin tulee harvita yksityisen virtuaaliverkon käyttöönottoa tietoliikenneyhteyden turvaamiseksi. Yksityistä virtuaaliverkkoa suositellaan myös käytettäväksi extranet- ja etäyhteyksien suojaamiseksi.

Yksityinen virtuaaliverkko (VPN) yhdistää saman organisaation kaksi toimipistettä salatulla tietoliikenneyhteydellä, joka on osa verkon suojarajapintaa. Tietoliikenteen suojaukseen kannattaa käyttää ns. tunnelointitoimintoa, jolloin yksittäisten koneiden verkko-osoitteet eivät näy mahdolliselle tarkkailijalle.

Organisaatioiden välinen organisaatioiden välinen tiedonsiirto (EDI-tietoliikenne) tulee suojata, koska suojaamaton organisaatioiden välinen tiedonsiirto on yhtä altis esimerkiksi tietojen tarkkailulle kuin suojaamaton sähköpostiliikenne. EDI-tietoliikennettä voidaan suojata EDIFACT-standardissa esitetyillä tietoturvarakenteilla ja suojausmekanismeilla²³. Organisaatioiden välisessä tiedonsiirrossa suositellaan siirtymistä XML-standardin mukaiseen (eXtensible Markup Language) tiedonvälitykseen²⁴.

Jos organisaatio korvaa perinteisen puhelinvaihteen (PBX) IP-puhelinliikennetarkkailulla (VoIP, Voice over IP), viraston tulee huomioida ratkaisun suunnittelussa seuraavat asiat:

- IP-vaihdepalvelin on palvelin, joka on yhtä haavoittuva kuin mikä muu tahansa komponentti organisaation verkossa.
- IP-vaihdepalvelin on suojaamattomana altis viruksille, palvelunestohyökkäyksille ja tunkeutumisille.
- IP-vaihdepalvelin tulisi sijoittaa erilleen muusta lähiverkosta omaan toimialueeseen (domain). Puheliikenne tulisi eristää virtuaalisilla lähiverkkoratkaisulla (VLAN) ja mahdollisuuksien mukana puheliikennettä tulisi salata.

²² Lisää menettelyohjeita etätyöskentelyn tietoturvallisuuteen on ohjeessa VAHTI 3/2002.

²³ Lisätietoja EDI-standardista (ISO 9735) löytyy muun muassa WWW-osoitteesta www.iso.org.

²⁴ Lisätietoja XML-standardista löytyy dokumentista "Valtion tietotekniikan rajapintasuosituksia (27/2001)".

Jos organisaatiolla on tarvetta käyttää videoneuvottelujärjestelmiä, tulee järjestelmän suunnittelussa ja käytössä huomioida, että videoneuvottelujärjestelmät ovat suojaamattomana haavoittuvia viruksille, palvelunestohyökkäyksille ja salakuuntelulle.

Videoneuvottelujärjestelmien suojaamiseksi löytyy kaupallisia ohjelmistoja, joiden käyttöä tulee harkita. Videoneuvottelun suojaamisen tarve tulee suunnitella sen mukaan, kuinka luottamuksellisia asioita videoneuvottelussa käsitellään.

Organisaation sisäisen ja organisaatioiden välisen tiedonsiirron suojaamisessa tulee yllä olevien ohjeiden lisäksi huomioida muut tässä ohjeessa jo aikaisemmin esitetyt toimintaohjeita turvalliselle Internetin käytölle.

3.6 Sähköposti ja muut viestintäsovellukset

Sähköposti on pääasiassa henkilökohtaiseen sähköiseen viestintään tarkoitettu ohjelmisto. Organisaation toiminnan kannalta suurimmat sähköpostiohjelmiston käytön ongelmat liittyvät sen käyttötarkoitukseen. Sähköpostin käyttötarkoituksia voivat olla:

- yksityinen viestintä
- sisäinen viestintä
- organisaatioiden välinen hallinnollinen yhteydenpito ja tiedonsiirto
- asiakkailta tuleva viestintä, joka sisältää organisaation perustoimintaan liittyviä, käsittelyvelvollisuuden piirissä olevia asioita.

Jälkimmäiset ovat asioita, jotka viraston on hoidettava. Toisaalta työntekijän yksityinen ja henkilökohtainen viestintä on jo perustuslain säännöksillä luottamuksellisuuden osalta suojattu.

Koska yllä mainituista sähköpostin eri käyttötavoista voi seurata käytännön ristiriitoja, on sähköpostin käyttötarkoitus organisaation toiminnan kannalta syytä määritellä ja toteuttaa sähköpostin käyttöön liittyvät suojaukset sekä käyttöpolitiikka ja käyttäjien ohjeistus sen mukaisesti²⁵.

Jos sähköpostia käytetään valtionhallinnon organisaatioiden salassa pidettävien tietojen siirtoon tai asiakkaan asiointiin²⁶, täytyy käytettävässä sähköpostijärjestelmässä olla sähköinen allekirjoitus- ja salausratkaisu. Niiden osalta on otettava huomioon sekä yhteentoimivuus yleisten salaus- ja PKI-standardien kanssa että käytettävi-

²⁵ Lisätietoja sähköpostista löytyy ohjeesta Valtionhallinnon sähköposti ja lokitietojen käsittelyohje, VAHTI 5/2001

²⁶ Esimerkiksi Internet-asiointipalveluja täydentävänä kanavana

en varmennepalveluiden kanssa. Lisäksi niissä asioissa, joita em. standardit eivät määrittele, kuten eri sähköpostiohjelmien toiminnoissa voi olla eroja. Nämä erot on huomioitava, testattava ja tarvittaessa ilmoitettava yhteentoimivuuteen liittyvät seikat asiointiosoitteiden julkaisun yhteydessä.

Sähköpostiviesti koostuu otsake- ja runko-osioista. Otsakeosioon tulee kentiä viestin lähettämisaikakohdasta, lähettäjä, vastaanottaja/t, jakelupolku, aihe ja muuta määräämuotoista tietoa. Tiedot järjestetään sähköpostistandardin²⁷ määrittelemään muotoon lähetystä/vastaanottoa varten. Itse sähköpostijärjestelmän toiminta perustuu kolmeen erilliseen osaan:

- Sähköpostin käyttöliittymä
- Sähköpostin välitysohjelmisto
- Paikallinen jakeluohjelmisto

Käyttäjän lähettäessä sähköpostia viesti muokataan käyttöliittymän toimesta muotoon, jossa välitysohjelmisto ottaa viestin vastaan. Jos viesti välityspalvelimella jaetaan vain samaa palvelinta käyttäville, hoitaa paikallinen jakeluohjelmisto viestin jakamisen oikeille vastaanottajille. Kun viesti välitetään eteenpäin toiselle välitysagentille, tunnustetaan vastaanottava palvelin ja mahdollistetaan yhteys.

Nämä kolme sähköpostikomponenttia välittävät postin eri sähköpostiprotokollilla:

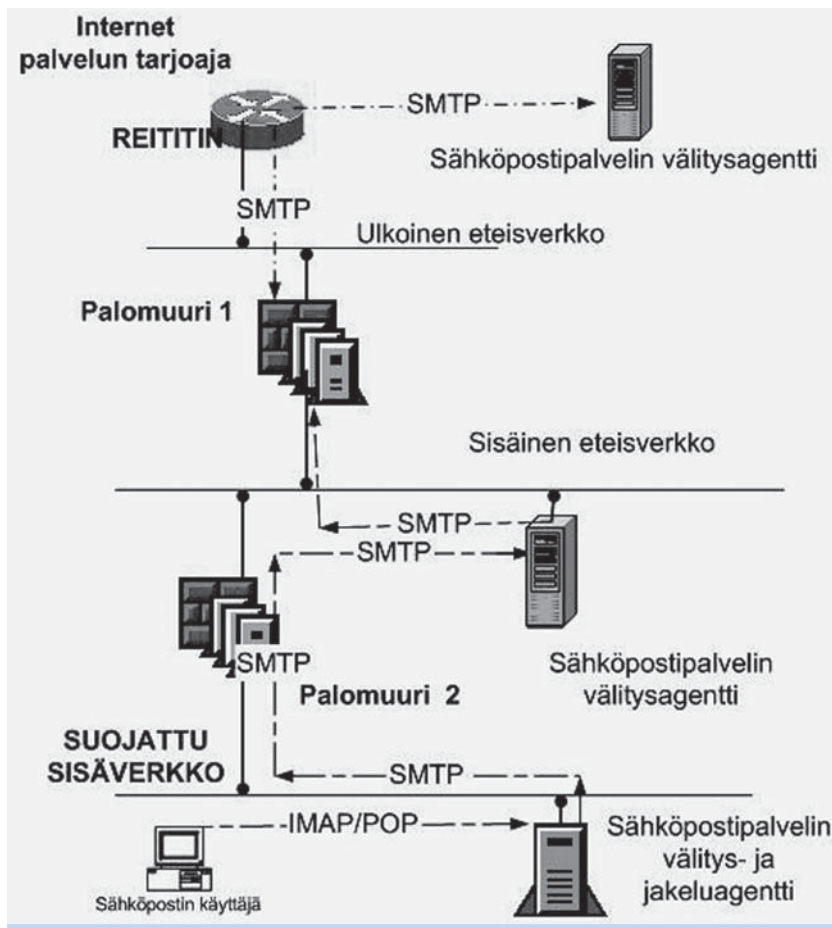
- lukuprotokolla huolehtii sähköpostin kulusta sähköpostipalvelimesta tyypillisesti muussa koneessa toimivalle käyttöliittymälle ja
- sähköpostin välitysprotokolla siirtää viestin verkossa välityspalvelimille.

Nykyisessä ympäristössä sähköpostin lukuprotokollia ovat POP ja IMAP, välitysprotokollana toimii SMTP. Myös HTTP-protokollaa käytetään sähköpostin lukemiseen joissakin palveluissa.

Käytettäessä WWW-selainta sähköpostin käsittelyyn tulee yhteydet tehdä aina SSL/TLS/SSH-protokollalla. Tämä takaa sähköpostin turvallisuuden selaimen ja sähköpostipalvelimen välillä, mutta ei suoja liikennettä sähköpostijärjestelmän eri palvelimien välillä eikä liikennettä muihin sähköpostijärjestelmiin.

²⁷ Erityisesti RFC 2822

Kuva 12. Esimerkki sähköpostiviestien välittämisessä palomuurilla suojatun yhteyden läpi



Sähköpostipalvelinten sijoittelussa pitää ottaa huomioon esimerkiksi tarve suojata organisaation sisäinen sähköpostiliikenne siten, että sisäinen liikenne ei ole enemmän altis ulkoisille uhkille kuin muutkaan sisäisen verkon järjestelmät. Tämä tarkoittaa sisäisen liikenteen sähköpostipalvelimen sijoittamista sisäiseen verkkoon ja ohjaamalla ulkoinen liikenne eteisverkkoon sijoitetun sähköpostiyhdyskäytävän kautta. Jälkimmäinen asennetaan samoilla huolellisilla periaatteilla kuin muut julkiseen Internetiin yhteydessä olevat palvelimet. Ulkoisen ja sisäisen sähköpostin ero pitää ohjeistaa myös käyttäjille ja huomioitava ero mm. sähköpostiviestin edelleen lähettämistä rajoittavana tekijänä.

3.6.1 Sähköpostin luottamuksellisuus ja salaus

Turvallisuusmielessä sähköpostin lukuprotokollat ovat perinteisesti olleet ongelmallisia, sillä ne välittävät sähköpostilaatikon avaamiseen tarvittavan salasanan selväkielisenä verkossa. Kuitenkin tähän on viime aikoina kehitystyössä kiinnitetty huomiota ja protokollista on kehitetty versiot, jotka mahdollistavat suojatun käytön. Esimerkiksi POP3 ja IMAP4 mahdollistavat SSL/SSH-salauksen käytön.

Verkossa on myös useita lähinnä yksityiskäyttöön tarkoitettuja sähköpostipalvelimia, joissa sähköpostin luku tapahtuu suoraan WWW-selaimen avulla, eli sähköpostin käyttöliittymä on selain eikä erityinen sähköpostin lukuohjelma²⁸. Valtionhallinnon organisaation toiminnan kannalta ilmaisen sähköpostin käyttö ei ole sähköpostiviestien käsittelyyn liittyvien vastuukysymysten takia mahdollista. Niiden yksityiskäyttöä organisaation WWW-liittymän kautta ei kuitenkaan tarvitse kieltää, koska esim. sähköpostin yksityiskäyttö voidaan kanavoida ulkopuolisiin WWW-sähköposteihin, mikä organisaation toiminnan kannalta voi ehkäistä viestintäsalaisuuden hallintaongelmia pois virallisesta sähköpostista. Jos tällaisten palveluiden käyttö henkilökunnalle sallitaan, on syytä huolehtia viestintäsalaisuudesta mm. välimuistipalvelimissa ja kieltää kaiken organisaation postin jälleenlähetys näihin palvelimiin.

Sähköpostin lukuprotokollan salaus ratkaisee vain viestin suojauksen oman postipalvelimen ja lukuohjelman välillä. Tämän välin ulkopuolella viesti liikkuu selväkielisenä eri postipalvelimien välillä, ellei sitä ole erikseen postin lukuohjelmassa salattu tai salattu alemmilla tietoliikennetasoilla. Postin salaukseen kahden eri käyttäjän välillä on kaksi päävaihtoehtoa: PGP tai S/MIME. Salausjärjestelmät eivät valitettavasti ole tällä hetkellä yhteensopivia, eli PGP-käyttäjä ei voi lukea S/MIME-postia ja päinvastoin.

S/MIME (Secure/Multipurpose Internet Mail Exchange) on suositeltavin standardi sähköpostin salaukseen. Tästä standardista on syytä käyttää versiota, jonka salaus on riittävän vahva. S/MIME hyödyntää X.509-varmenteita sekä luottamusmallia. S/MIME v3 etuja ovat muun muassa seuraavat:

- Soveltuu isoille käyttäjämäärille ja organisaatioille.
- Kattava tuki eri sähköpostiohjelmistoille (muun muassa Tiimiposti ja Microsoft Outlook) ja selainohjelmille.
- Avaintenhallinnointi on jouhevampaa
- Käyttäjän kannalta se on läpinäkyvä.

²⁸ Tällaisia palveluita on Suomessa (esim. jippii.fi, luukku.com, suomi24.fi) ja ulkomailla (esim. Hotmail, Yahoo)

Toisaalta taas S/MIMEn käyttöönotto vaatii sen, että jokaiselle käyttäjälle on luotava oma X.509v3-sertifikaatti.

PGP asennetaan erillisenä ohjelmalla (PGP, GPG tai OpenPGP) ja sen luottamusmalli toimii vapaamuotoisella verkostoperiaatteella. PGP ei ole sellaisenaan yhteensopiva virallisten varmennepalveluiden kanssa eikä sen avulla ole toteutettu virallista, lakiperusteisiin hallinnollisiin vastuisiin perustuvaa julkisen avaimen arkkitehtuuria.

Sähköposti tulisi pääsääntöisesti säilyttää sähköpostipalvelimella eikä käyttäjän henkilökohtaisessa työasemassa. Kopioita voi toki pitää työasemassa, esimerkiksi kannettavassa tietokoneessa. Näin siksi, että palvelimelle voidaan järjestää säännöllinen varmuuskopiointi ja työaseman kiintolevyn hajoaminen ei kadota sähköposteja. Tämä toimintamalli on sisäänrakennettu WWW- tai IMAP-pohjaisiin järjestelmiin. POP-sähköposti voidaan yleensä erikseen asentaa jättämään viestit palvelimelle.

Sähköpostilaatikoiden käyttöoikeudet on viestintäsalaisuuden takia suositeltavaa toteuttaa siten, että tavallisilla ylläpitovaltuuksilla ei ole lukuoikeutta henkilökohtaisiin sähköpostilaatikoihin. Mikäli lukuvaltuuksia poikkeuksellisesti ja perustellusti tarvitaan, tilapäisten oikeuksien käyttöönotto voidaan toteuttaa hallinnollisesti (esimiehen/ tilaajan tms. valvojan lupa) ja teknisesti (oikeuksien muutoksista seuraava automaattinen lokimerkintä) valvotulla menettelyllä.

3.6.2 Sähköpostin palveluosoitteista

Mikäli asiointimahdollisuus sähköpostitse päätetään luoda, kansalaisten viranomaiselle lähettämä sähköpostiliikenne tulee ohjata ensisijaisesti palveluosoitteisiin, esim. info@organisaatio.fi tai kirjaamo@organisaatio.fi. Tämä mahdollistaa asiointin kirjauksen, kuormituksen jakamisen ja tehtävien joustavan hoidon esimerkiksi tehtävien vaihtuessa tai lomien aikana. Lisäksi menettely ehkäisee mahdollisia ongelmatilanteita viestintäsalaisuuden suhteen. Viranomaisen palveluosoitteisiin tuleva sähköposti suositellaan kuittaamaan.

Työntekijän nimelle lähetettyyn sähköpostiin on suhtauduttava viestintäsalaisuuden huomioiden. Työntekijän saadessa organisaation virallista postia omalla nimellään, on hänen tarvittaessa lähetettävä se asianomaiseen palveluosoitteeseen.

HAITTAOHJELMAT JA SÄHKÖPOSTIN LIITETIEDOSTOT

Erilaisten haittaohjelmien yleinen leviämistapa on nykyään sähköpostin liitetiedostot. Tämän vuoksi kaikki sisään tulevat ja ulos lähtevät sähköpostiviestit tulisi tarkastaa virusten ja muiden haittaohjelmien varalta. Sähköpostin tarkastus voidaan järjestää joko palomuurijärjestelmän tai sähköpostipalvelimen yhteyteen, mikäli sähköpostiviestit eivät ole salattuja esimerkiksi PGP- tai S/MIME-ratkaisuilla. Salattujen viestien virus-

torjunnasta tulee huolehtia salauksen purkavalla laitteella, mielellään ei kuitenkaan omalla työasemalla. Varmuuden vuoksi sähköpostiohjelmista tulee myös kytkeä ne ominaisuudet pois, jotka aiheuttavat liitetiedoston tai HTML-muotoisen sähköpostin sisältämien toimintojen automaattisen suorittamisen. Myös ulospäin lähtevä sähköposti tulisi ohjata tarkastuksen kautta, tällä estetään esim. ulkoa tuotujen levykkeiden, CD- tai DVD-levyjen sisältämien virusten leviäminen muualle sähköpostin kautta.

Haittaohjelmavaaran vuoksi on sähköpostiohjelmiston asentamisessa otettava kantaa myös siihen, minkä tyyppisiä liitetiedostoja päästetään sisäiseen verkkoon²⁹. Monet tiedostotyyppit ovat suoritettavia ohjelmia tai komentojonotiedostoja, jotka voivat olla haittaohjelmia mutta eivät muodoltaan hallintotoiminnassa käsiteltäviä asiakirjoja. Esimerkkipolitiikkana voi olla, että makro- tai komentojonovirusvaaran vuoksi dokumentit otetaan vastaan vain PDF- tai RTF-muodossa³⁰, ja yli 4 megatavun liitetiedostoja ei välitetä. Jos liitetiedostoja suodatetaan pois, poistetusta liitteestä tulee lähettää automaattiviesti tai muu tieto sähköpostiviestin vastaanottajalle.

3.6.3 Ei-toivottu kaupallinen viestintä

'Ei-toivottua' kaupallista viestintää (roskaposti, spam, unsolicited commercial e-mail, UCE) on markkinointi- tai vastaavassa tarkoituksessa suurelle joukolle (esim. useita miljoonia) sähköpostin käyttäjiä yleensä oikean näköisestä, mutta käytännössä toimimattomasta, sähköpostiosoitteesta lähetetyt sähköpostiviestit³¹. Tyypillistä on myös se, että roskapostin lähettäjän osoite on väärennetyt. Roskaposteihin ei pidä vastata eikä myöskään pidä käyttää roskapostien tarjoamia keinoja päästä pois jakelulistalta. Näiden toimenpiteiden todellinen tarkoitus on varmistaa osoitteiden toimivuus.

Jokainen ylläpitäjä voi estää roskapostin välittämisen asentamalla sähköpostin välityspalvelimen niin, että se ei välitä eteenpäin ulkopuolelta lähetettyä roskapostia. Sähköpostipalvelimelle voidaan myös asentaa roskapostisuodatus. Tällöin sähköpostipalvelin suodattaa ja poistaa automaattisesti sähköpostiviestit, jotka sisältävät suodatuksessa määritellyjä kriteereitä. Tässä menetelmässä on selkeitä riskejä siihen, että suodatussäännöt vahingossa poistavat jotakin asiallista sähköpostia. Esimerkiksi kaikille avoimissa asiointipalveluissa tätä ei voi käyttää.

²⁹ Lisätietoja poistettavista liitteistä <http://support.microsoft.com/default.aspx?scid=kb;EN-US;262631> tai <http://nsa2.www.conxion.com/support/guides/sd-7.pdf>

³⁰ Uusimmissa PDF- ja RTF-muodoissa on esiintynyt makroja, mutta ne ovat suojatumpia kuin esimerkiksi DOC-muotoiset dokumentit. Ongelmia voi olla myös eri organisaatioiden tavoissa hyväksyä dokumentteja.

³¹ Sähköisen viestinnän tietosuojalakesityksen mukaan suoramarkkinointi on sallittua jos se kohdistuu käyttäjiin jotka ovat antaneet nimenomaisen suostumuksen ennalta. Yhteisöillä on oikeus kieltää suoramarkkinointi.

3.6.4 Muista viestintäsovelluksista

Sähköpostin lisäksi Internet-käyttöön on olemassa reaaliaikaisia viestintäsovelluksia, joiden käyttöön liittyy sähköpostiin verrattuna uusia tietoturvauhkia. Pikaviestisovellusten (Instant Messaging, IM) toiminta perustuu kahden tai useamman tietokoneen suoraan kommunikointiin keskenään, jolloin tietokoneet muodostavat keskenään ns. vertaisverkon (peer to peer, P2P). Näillä sovelluksilla käyttäjät pystyvät kommunikoimaan suoraan ilman suuria aikaviiveitä toistensa kanssa sekä ottamaan vastaan tiedostoja tai jakamaan niitä toisten käyttäjien kanssa. Niihin liittyy usein tekijänoikeuksia loukkaavia käyttötapoja ja ne ovat merkittäviä haittaohjelmien välittäjiä. Tämän lisäksi ulkopuolinen voi harhauttaa käyttäjää tätä kautta avaamaan tietämättään pääsyn tietokoneisiin ja tietojärjestelmiin. Näiden sovellusten käyttäminen organisaation laitteistoilla tulee kieltää käyttäjien ohjeistuksessa ja tarvittaessa palomuu- ja ohjelmistoasennusten yhteydessä estää.

Organisaation on hyvä ottaa kantaa myös asiakaspalvelin-mallilla toimivan IRC-kommunikaatiosovelluksen (Internet Relay Chat) tai Internetin yli tapahtuvien videoneuvottelujen 'web conferencing' käyttöön. Ne voivat olla käyttökelpoisia kommunikointimuotoja sisäverkossa, mutta osallistuminen organisaation ulkopuolisiin keskustelufoorumeihin ei ole yleensä viranomaisen toimintamuoto eikä videoneuvotteluja tule tehdä suojaamattoman verkon yli. Näiden lisäksi erilaisten etäkäyttöohjelmien ja IP-puhelujen (Voice over IP) tietoturvariskit ja suojausmekanismit tulee arvioida ennen käyttöönottoa.

LIITE 1

Henkilökunnan Internet-käytön tietoturvaohjeen malli

Tämä ohjemalli kuvaa asioita, joihin tulee ottaa kantaa henkilöstön Internet-käytön ohjetta laadittaessa. Henkilöstön Internet-käytön ohjeen tulee sisältää toimintaohjeita sekä Internetin että sähköpostin käyttöön liittyen. Yleiskäyttöistä ohjemallia ei voida laatia, koska Internet-verkon käyttötavat vaihtelevat organisaatiokohtaisesti ja konkreettiset tietoturvatilat riippuvat osittain:

- siitä, mitä palveluita käyttäjille sallitaan ja miten tekninen suojaus on toteutettu,
- käyttäjien teknisestä tietämyksestä ja osaamisesta,
- organisaation tehtävistä (Internet työvälineenä) ja
- muusta tietoturva- ja tietotekniikkaohjeistuksesta.

Tietoturvaohjeistuksen lisäksi on syytä ottaa kantaa sovellusten käyttöpolitiikkoihin, viestinnän muotoseikkoihin ja teknisiin yksityiskohtiin. Esimerkiksi useiden sovellusten käyttöön liittyy riskejä, joita aiheutuu käyttäjien virheistä ja osittain käytettävien sovellusten ominaisuuksista (sähköpostien jakelulistat ja väärään osoitteeseen lähettämisen riski). Näistä tulee mahdollisuuksien ja tarpeiden mukaan varoittaa sovelluskohtaisissa ohjeissa. Kaikkien tietoturva-asioiden eriyttäminen omiin tietoturvaohjeisiin ei välttämättä ole suotavaa.

Tietoturvallisuutta voidaan vain marginaalisesti parantaa opastamalla käyttäjiä tunnistamaan riskejä sisältäviä teknisiä erikoisuuksia. Yleensä vahvat ja ajantasaiset tekniset suojaukset, oikeat tietotekniset perustiedot sekä normaalit varovaisuussäännöt tuottavat paremman tuloksen.

TAUSTAA

Internet-verkon käytöstä aiheutuu organisaation tietojen käsittelylle erilaisia uhkia. Tietohallinnon tavoitteena on hallinnoida Internet-yhteyksiä ja -käyttöä siten, että tietoturvallisuushkat on mahdollisimman pitkälle teknisin keinoin ennalta ehkäisty. Tämä ei kuitenkaan ole täysin mahdollista, koska Internet-uhkat ja tekniikka kehittyvät jatkuvasti. Tekniset keinot eivät estä kaikkia uhkia, joten osa riskeihin varautumisesta jää peruskäyttäjien vastuulle.

YLEISTÄ

Internet-verkko on laaja "virtuaaliympäristö", jossa pätevät lähtökohtaisesti normaalit yhteiskunnan ja työympäristön säännöt. Työnantajalla ei ole velvollisuutta eikä mahdollisuutta Internet-yhteyden avaamisen yhteydessä edeltä käsin tyhjentävästi joko kieltää tai sallia kaikkia kyseenalaisia tai väärinkäytösmahdollisuuden sisältäviä sovelluksia tai käyttötapoja. Tästä syystä käyttäjällä itsellään on vastuu noudattaa organisaation tietoturvaohjeistusta, jotta Internetissä käytettävien palveluiden käyttö ei aiheuta tietojen käsittelylle ja toiminnalle ylimääräisiä tietoturvariskejä.

Työnantaja ei seuraa ja valvo Internet-käyttöä aktiivisesti henkilötasolla. Internet-yhteyksien ylläpitäjällä on velvollisuus valvoa yhteyden tietoturvallisuutta. Tietoturvallisuuden valvomiseksi verkon käytöstä jää jälkiä (ns. lokitiedot), joista saadaan tarvittaessa jälkikäteen selvitettyä verkon käyttöön liittyviä tapahtumia. Valvonnassa seurattavat tapahtumat ovat teknisiä. Mutta jos virhe-, järjestelmien suorituskyky- tms. tapahtumien syy on henkilötasolla, voidaan myös verkon tapahtumia joutua selvittämään käyttäjä tunnistaen. Lokitietojen käyttö henkilökuntaan päin on täysin avointa. Mikäli teknisiä Internet-käyttöön liittyviä henkilötason ongelmia ilmenee, siitä ilmoitetaan asianomaiselle mahdollisimman pian.

Tässä ohjemallissa kuvataan toimenpiteitä ja käytösääntöjä, joilla peruskäyttäjän tasolla voidaan hallita Internet-verkon käyttöön liittyviä tietoturvariskejä.

INTERNET-YHTEYKSIEN KÄYTTÖTARKOITUS

Internet-yhteys on tarkoitettu työtehtävien hoitamiseen. Sallitut käyttötarkoitukset ovat:

- informaation hankkiminen työtehtävien suorittamiseksi
- ammatillisen sivistyksen kehittäminen
- ammattiyhdistystoiminta
- sallittua yksityiskäyttöä ovat
 - pankkiasiointi
 - satunnainen viestintä, ilmoitukset tms. jotka ovat esim. kiireellisiä ja työläitä hoitaa muulla tavoin

Verkon palveluiden ja sovellusten käyttäminen ei saa olla ristiriidassa organisaation viestinnän, toiminnan tarkoituksen tai tietoturvallisuuden kanssa.

RAJOITUKSET

- työnantajan luottokortin käyttö maksuvälineenä Internetissä on kielletty muulloin kuin perustelluissa poikkeustapauksissa

YHTEYSTAPA

Kaikki organisaation verkosta tapahtuva Internet-käyttö kulkee palomuurin kautta. Laitteiden tai ohjelmien asentaminen muun kuin tietohallinnon toimesta ja ohjauksessa on kielletty.

KIELLETTYT TAI RAJOITETUT SOVELLUKSET JA PALVELUT

Seuraavien sovellusten käyttö niiden sisältämien erityisen korkeiden tietoturvariskien tai muun haitan takia suositellaan kiellettäväksi.

- Pikaviestisovellukset (Instant Messaging)
 - AOL ja MSN Instant Messenger sekä vastaavat
- Musiikki- ja videotiedostojen lataamiseen tarkoitettavat sovellukset
 - Napster ja KaZaA sekä vastaavat
- Nettiradio
- Automaattiset näytönsäästäjät, jotka kuluttavat työaseman resursseja omaan toimintaansa
 - SETI@home (Search for Extra Terrestrial Intelligence)
- Keskusteluryhmät kuten IRC ja erilaiset chat-ryhmät
- Uutisryhmä-palveluihin (News Groups) saavat osallistua ainoastaan erikseen nimetyt henkilöt.
- kaikki käyttötarkoitukseltaan haitalliset, hyvän tavan vastaiset tai työtehtävien kanssa ristiriidassa olevat palvelut (esim. salauksen purku jo lain nojalla)

KÄYTTÖÖN LIITTYVÄT MUUT RAJOITUKSET

- tarvittaessa organisaatio määrittelee käyttöajat ja -paikat

KÄYTTÖSÄÄNNÖT

Tekijänoikeussäännöt on huomioitava myös Internetistä peräisin olevan aineiston suhteen. Samoin on suhtauduttava varauksin kaikenlaisen aineiston luotettavuuteen ja oikeellisuuteen. Internetissä kuka tahansa voi julkaista mitä tahansa. Kuten muuallakin, kannattaa lähtökohtaisesti pitää luotettavana vain ennestään tunnettuja lähteitä. Teknisenä varmistuksena voidaan selaimen kautta selvittää palvelimen ylläpitäjän SSL-varmenne.

Internetiä käytettäessä on toimittava niin, että haittaohjelmien pääsy sisäiseen verkkoon estetään mahdollisimman pitkälle ennalta. Tunnetut ja luotettavat verkkopalvelut eivät pääsääntöisesti sisällä haittaohjelmia. Epämääräisiä ja käyttötarkoitukseltaan työtehtävien suorittamiseen liittymättömiä sivustoja pitää mm. haittaohjelmavaaran takia välttää ja varoa.

Organisaation hankintoihin ja muihin tukitoimintoihin tarjolla olevia asiointipalveluita voidaan käyttää vasta, kun on päätetty palvelun käytön turvallisuus työnantajaorganisaation kannalta. Näitä palveluita voivat sen jälkeen käyttää nimetyt/ valtuutetut henkilöt ja/tai erikseen annettujen ohjeiden mukaisesti.

Seuraavilla toimenpiteillä voidaan Internet-uhkia hallita peruskäyttäjätasolla:

- Sisäisten tietojärjestelmien ja -verkkojen käyttöön tarkoitettua henkilökohtaista käyttäjätunnusta ja salasanaa ei käytetä Internetissä oleviin palveluihin rekisteröitymiseen koska se voi tätä kautta paljastua ulkopuoliselle
- Myös työnantajan sähköpostiosoitteen luovuttamisessa esim. Internet-palveluihin rekisteröidytessä kannattaa olla varovainen. Osoite voi tätä kautta kulkeutua ns. ei-toivottuun kaupalliseen viestintään käytetyille (spam) postituslistoille.
- Internet-selaimen tietoturva-asetuksia ei saa heikentää ilman tietohallinnon lupaa¹.
- Ohjelmien lataaminen ja asentaminen Internetistä muun kuin tietohallinnon toimesta on kielletty.

1 Selaimen ominaisuuksien (ks. varsinaisen ohjeen kohta "selaimet") käyttäjähallintaa voidaan tarvittaessa ohjeistaa

Työntekijä vastaa sähköpostin käytöstä, sähköpostilaatikon sisällöstä ja sisällön ylläpidosta. Tällöin työntekijän tulee ottaa huomioon seuraavat seikat:

- Työsähköpostia on käytettävä kuin mitä tahansa työvälinettä työtehtävien hoitamiseen.
- Ilman sähköistä allekirjoitusta sähköpostiviestin näyttöarvo ilman monimutkaisia teknisiä selvityksiä on rajallinen (esim. taloudellisen tapahtuman todisteena).
- Sähköpostiviesti on dokumentti, josta voi olla kopioita monessa paikassa (mm. varmuuskopiot, sähköpostipalvelimet, työasemat) jota voidaan riittävän perusteen ilmetessä käyttää yhtenä todistusaineistona.
- Sähköpostia suojaa viestintäsalaisuus, mutta se ei sellaisenaan takaa tietojen salassapitoa. Salassa pidettävien tietojen lähettäminen salammattomassa Internet-sähköpostissa on kielletty.
- Sähköpostiviestien automaattinen edelleen lähetys sisäisestä ja/tai suojatusta sähköpostiympäristöstä suojattomaan (Internet) on kielletty. Tapauskohmainen edelleen lähetys sallittu vain tilannekohtaisen harkinnan perusteella.
 - Sähköpostin liitetiedostoja lähetettäessä tulee huomioida seuraavat asiat:
 - Liitetiedostot ovat yleisimpiä virusten ja muiden haittaohjelmistojen leviämistäpoja.
 - Haittaohjelmien torjunta suodattaa lähetettävistä ja tulevista sähköposteista seuraavat tiedostotyyppit.
 - Seuraavat virustorjunnan läpi päästämät tiedostotyyppit voivat sisältää viruksia².
- Tuntemattomalta lähettäjältä saadun, epätavallisesti otsikoidun tai muuten oudon sähköpostiviestin liitetiedostoa avattaessa tulee noudattaa varovaisuutta. Jos avaat sinulle lähetetyn liitetiedoston, tallenna se aina ensin työasemasi kiintolevylle. Ota tarvittaessa yhteyttä tekniseen tukeen. Myös tietokonevirusvaroitukset voivat olla haitantekomielessä tehtyjä. Niihin ei kannata reagoida selvittämättä varoituksen aiheellisuutta esim. tekniseltä tuelta. "Spam" eli roskapostiviesteihin ei pidä vastata.
- Ketjukirjeiden lähettäminen työnantajan laitteista sähköpostitse on kielletty. Ketjukirjeet ovat haittaohjelmien levittäjiä ja kuormittavat turhaan tietotekniikkaresursseja. Lisäksi Rahankeräys L 2 § 3 mom. kieltää rahankeräysketjukirjeet.

2 Ks. Lisätietoja <http://support.microsoft.com/default.aspx?scid=kb;EN-US;262631>

LISÄKSI PALVELU- JA SOVELLUSKOHTAISET OHJEET TARVITTAESSA

Esimerkiksi sähköpostin asiointikäyttö tai ASP-palveluiden käyttö edellyttää käytön organisointia, tukitoimintojen järjestämistä sekä tarvittavien tietoturvaominaisuuksien toteuttamista. Nämä pitää tarvittavilta osin myös ohjeistaa.

Tähän ohjeeseen liittyvissä kysymyksissä ja mahdollisissa ongelmatilanteissa ota yhteyttä tietohallintoon.

YHTEYSTIEDOT:

Yksikkö:

Henkilö:

Puhelinnumero:

Sähköpostiosoite:

LIITE 2: Palvelimen asennusohje

I SÄHKÖPOSTIPALVELIN

Sähköpostipalvelimen ylimääräisten palvelujen karsiminen

NRO	TIETOTURVATOIMINNE
1	Asenna järjestelmä, sille varattuun laitteeseen
2	Asenna vain tarvittavat palvelut
3	Asenna kaikki soveltuvat päivitys- ja korjausajot
4	Poista kokonaan tai käytöstä kaikki tarpeettomat palvelut, kuten WWW-mail, FTP tai etähallinnointi
5	Poista kaikki toimittajan dokumentaatio palvelimelta
6	Aja soveltuva turvallisuusasennus (Hardening script) järjestelmälle
7	Muuta palveluilmoituksia niin, ettei järjestelmän sovellus-, käyttöjärjestelmä- tai versiotietoja näytetä
8	Poista kaikki turhat sähköpostikomennot, kuten VRFY ja EXPN

Käyttöjärjestelmän konfigurointi ja sähköpostipalvelimen pääsynvalvonta

NRO	TIETOTURVATOIMINNE
9	Rajoita sähköpostisovelluksen pääsyä tietokoneen resursseihin. Tee sille oma tiedostoalueensa, jossa se voi vain toimia
10	Mahdollista pääsoikeuksien vahvempi tarkastelu, mikäli niitä tarvitaan
11	Konfiguroi sähköpostipalvelu toimimaan omalla käyttäjätunnuksellaan ja rajoita sen oikeudet minimiin
12	Tarkista, että sähköpostipalvelua ei ajeta pääkäyttäjän tunnuksin (root, admin)
13	Konfiguroi sähköpostipalvelimen lokitiedot niin, että palvelu voi kirjoittaa lokia, muttei lukea sitä
14	Konfiguroi palvelin niin, että väliaikaistiedostot saavat riittävät, mutta rajoitetut oikeudet toiminnalleen
15	Konfiguroi palvelimen käyttöjärjestelmä niin, että kaikki sovelluksen tarvitsemat väliaikaistiedostot ovat sähköpostipalvelun omistamia
16	Varmista, että sähköpostipalvelu ei voi kirjoittaa tiedostoja kuin sille varatulle alueelle
17	Konfiguroi sähköpostipalvelu toimimaan chroot:na Linux- ja Unix-järjestelmissä
18	Konfiguroi käyttäjien sähköpostilaatikat eri levyille ja levypartitiolle, kuin käyttöjärjestelmä ja sähköpostisovellus
19	Rajoita sallittujen liitetiedostojen kokoa
20	Tarkista, että lokitiedostolle on varattu riittävästi tilaa

Liitetiedostot ja sisällöntarkistus

NRO	TIETOTURVATOIMINNE
21	Asenna keskitetty virustorjuntajärjestelmä (sähköpostin välityspalvelimelle, palomuriin tai sähköpostipalvelimelle)
22	Asenna virustorjunta kaikille työasemille
23	Päivitä virustorjuntapalvelinten tietokannat säännöllisesti ja riittävän usein
24	Kouluta käyttäjät ymmärtämään virusten aiheuttamat ongelmat ja kuinka minimoida ongelmien aiheuttamat häiriöt
25	Informoi käyttäjiä, jos virustorjunta on pettänyt
26	Konfiguroi sisällönsuodatus niin, että se poistaa epäilyttävät viestit
27	Konfiguroi sisällönsuodatus niin, että se poistaa roskapostiviestit
28	Luo sisällönsuodatuspolitiikka
29	Konfiguroi palvelin niin, että se ei hyväksy sähköposteja palvelimilta, jotka ovat ns.mustallalistalla
30	Konfiguroi palvelin poistamaan tietyistä osoitteista tulevat sähköpostit tarvittaessa
31	Konfiguroi sähköposti vaatimaan autentikointi jälleenlähetettävälle posteille
32	Konfiguroi palvelin käyttämään salattua autentikointia
33	Konfiguroi palvelin tukemaan vain SSL/TLS suojattuja web-yhteyksiä ja vain jos ne ovat aivan välttämättömiä

III SÄHKÖPOSTIN KÄYTTÖLIITTYMÄN ASENNUS

Sähköpostin käyttöliittymän päivitys- ja korjausajot

NRO	TIETOTURVATOIMINNE
1	Päivitä sähköpostin käyttöliittymästä turvallisin versio
2	Aja kaikki tarvittavat turvalliset korjausajot
3	Aja kaikki korjausajot selaimen, mikäli postipalvelua käytetään selaimen kautta

Sähköpostin käyttöliittymän turvallisuus

NRO	TIETOTURVATOIMINNE
4	Poista automaattinen viestien esikatselu
5	Poista seuraavan viestin automaattinen aukeminen
6	Poista, jos mahdollista, aktiivisten toimintojen prosessointi
7	Mahdollista vahva tunnistus ja todennus
8	Poista mahdollisuus tallentaa käyttäjätunnus ja salasana
9	Mahdollista sisällön salaaminen, esimerkiksi PGP:llä tai S/MIME:llä
10	Konfiguroi käyttäjä tallentamaan saapuneet viestit salattuina
11	Mahdollista vain luotetut ja tarvittavat plug-in-toiminnot
12	Jos web-palvelua tarvitaan, konfiguroi se käyttämään SSL/TLS-yhteyttä ja 128-merkin mittaista avainta
13	Opetä käyttäjille mahdollisista tietoturvauhista, joita web-käytössä ovat mahdollisia

Microsoft Outlookin konfiguroinnissa huomioitavaa

NRO	TIETOTURVATOIMINNE
14	Poista ActiveX toiminnot (kirjatut ja kirjaamattomat)
15	Poista Java-oikeudet
16	Poista mahdollisuus ladata ohjelmia IFRAME:ssa
17	Poista aktiivi skriptaus
18	Poista Java-applettien skriptaus

Eudoran konfiguroinnissa huomioitavaa

NRO	TIETOTURVATOIMINNE
19	Poista 'sallitaan toiminnot HTML-sisällössä'
20	Poista Microsoft näyttäjä
21	Poista MAPI

Netscapen konfiguroinnissa huomioitavaa

NRO	TIETOTURVATOIMINNE
22	Poista Javan mahdollistaminen
23	Poista Javascript sähköpostissa ja uutispalveluissa
24	Poista lähetä sähköposti osoite anonyymissä FTP-salasana
25	Poista Microsoft ActiveX

IV WINDOWS-PALVELIMENTARKISTUSLISTA**Päivitykset ja korjausajot**

NRO	TIETOTURVATOIMINNE
1	Viimeisimmät turvalliset päivitykset
2	Viimeisimmät turvalliset korjaukset

Auditointi- pääsyoikeuspolitiikat

NRO	TIETOTURVATOIMINNE
3	Salasanojen pituudet ja voimassaoloajat
4	Salasanojen hyväksymiskriteerit ja historiointi
5	Sovellusten tapahtumalokien käsittely
6	Kirjautumisten tapahtumalokien käsittely
7	Järjestelmän tapahtumalokien käsittely

Tietoturva-asetusten valinta

NRO	TIETOTURVATOIMINNE
8	Operointioikeuksien antaminen
9	Järjestelmän alasajoparametrien valinta

10	Virtuaalimuistien tyhjentäminen alajasossa
11	Allekirjoitusten käsittely
12	Edellisten istuntojen muistaminen ja niistä ilmoittaminen
13	Salasanojen vaihtopakon asentaminen
14	Yleistunnusten uudelleen nimeäminen ja käyttöoikeuksien poistaminen
15	Domain-yhteyksien salaaminen
16	Rekisteriasetukset
17	Poista lähetä sähköposti osoite anonyymissä FTP-salasana

Käyttäjät, tiedostot ja levyjärjestelyt

NRO	TIETOTURVATOIMINNE, KÄSITTELE KÄYTTÄJIEN OIKEUDET
33	Käyttäjä- ja pääkäyttäjäoikeudet
34	Domainiin liittäminen
35	Varmistukset
36	Kellonajat
37	Verkon käyttäjien oikeudet järjestelmään
38	Luottamussuhteiden luonti
39	Lokaalit käyttöoikeudet
40	Alasajot ja niiden parametointi
NRO	TIETOTURVATOIMINNE, KÄSITTELE TIEDOSTO- JA REKISTERIOIKEUDET
41	Tiedosto-oikeuksien asettaminen
42	Rekisterioikeuksien asettaminen
NRO	TIETOTURVATOIMINNE, MUUT JÄRJESTELMÄ VAATIMUKSET
43	NTFS-levyjärjestelyt
Lisä 1	Lisätietoja esimerkiksi osoitteesta www.cissecurity.org

LIITE 3: Verkon seuranta- ja hallintatyökalut

I JÄRJESTELMÄ		
NRO	TYÖKALU	TYÖKALUN KUVAUS
1	watcher, klaxon, List Open Files (Isol), showid, loginlog	Järjestelmän resurssien käytön tutkimiseen, ylimääräiset palvelut, sisäänkirjautumiset, odottamattomat alasajot tai epätavallinen tietoliikenne
2	snort, Advanced security audit trail for Unix (asax), swatch, logsurfer, tklogger	Aktiiviset tunkeutumisen havainnointijärjestelmät, aktiivinen lokitietojen valvonta tai käyttöoikeusloukkausten seuranta
II VERKKO		
NRO	TYÖKALU	TYÖKALUN KUVAUS
3	tcp wrapper, tcpdump, argus, arpmon, arpmwatch, snort, courney, gabriel, logdaemon, rfingerd, clog, pidentd, enchanged portmap, ethereal	Verkkoliikenneyhteyksien valvonta ja tutkiminen, epäonnistuneet yhteysyritykset, luvattomat verkkoskannaukset, järjestelmälliset porttiskannaukset palomuuriasetusten vastainen liikenne tai epätavallinen tiedostojen siirto
4	ifstatus, Check Promiscuous Mode(cpm)	Verkkokortin valikoimattoman tilan (promiscuous mode) tutkiminen
5	nmap, fremont, strobe, Internet Security Scanner (ISS), System Administrator's Tool for Analyzing Networks (satan), Security Administrator's Integrated Network Tool (saint), Security Auditor's Research Assistant (sara), Nessus, Retina, Network Security Gard, MacPork	Uusien odottamattomien palvelujen havaitseminen ja tarvittavien palvelujen olemassaolo
III KÄYTTÄJÄ		
NRO	TYÖKALU	TYÖKALUN KUVAUS
6	Computer Oracle and Password System (cops), tiger, checkXusers, chkacct	Käyttöoikeuksien konfigurointien tarkistamiseen, kuten todennus- ja valtuustiedot
7	noshall, ttywatcher, logdaemon	Käyttäjien toimintojen, esim onnistuneet, epäonnistuneet ja epätavalliset sisäänkirjautumisten, tutkiminen ja valvonta
8	ttpsdserver	Tool-talk tietokantapalvelu CDE:tä käytettäessä

IV TIETOJEN JA OHJELMISTOJEN EHEYDEN VARMISTAMINEN		
NRO	TYÖKALU	TYÖKALUN KUVAUS
9	cops, tiger, secure-sun-check	Käyttöjärjestelmän ja lisäohjelmien turva-aukkojen tutkiminen
10	Tripwire, L5, hobgoblin, Reserch Institute for Advanced Computer Science (RIACS Auditing Package)	Hakemistojen sisällön ja suojausten muutosten muutosten havaitseminen
11	trojan.pl	Troijan Hevosten skannaus
V JÄRJESTELMÄN YKSITYISKOHTAINEN TUTKIMINE		
NRO	TYÖKALU	TYÖKALUN KUVAUS
12	top, Special Process Status (sps), Show Process Accounting Records (spar) , log surfer, logcheck	Lokittietojen läpikäynti ja tiivistäminen epätavallisen toiminnan havaitsemiseksi
13	chlastlog, chkwtmp, loginlog, trimlog	Lokittietojen eheyden tutkiminen mahdollisten peukalointien toimesta
14	The Coroner's Toolkit (TCT)	Oikeustutkimuksien apuohjelma

Lisää verkon seuranta- ja hallintatyökaluja esimerkiksi osoitteessa <http://www.isecom.org/projects/operationaltools.htm>.

LIITE 4: Internet-protokollien suojaaminen

I INTERNET-PROTOKOLLAT JA NIIDEN SUOJAAMINEN

PALVELU	TCP	UDP	LISÄSELVITYS
SSH	22		Secure Shell on sovellustason VPN
FTP	20/21		File Transfer Protocol, voidaan suojata ssh:n sftp:llä
SMTP	25		Simple Mail Tranfer Protocol, voidaan suojata käyttäen TLS:ää ja sähköpostiviestit suojataan käyttäen S/MIME, PGP tai PEM standardeja.
DNS	53	53	Suojataan DNSSEC-protokollaa käyttäen
RPC	135	135	Suojataan Secure RPC:tä käyttäen
POP3	110	110	Käyttämällä (TLS/SSL) suojattua yhteyttä porttiin 995
IMAP4	220	220	Suosittelaa (TLS/SSL) suojattua yhteyttä imaps porttiin 993
HTTP	80		HyperText Transfer Protocol
LDAP	389	389	Lightweight Directory Access Protocol
HTTPs	443		SecureHTTP (SSL)
RTSP	554		Real Time Streaming Protocol
NNTPs	563		Secure NNTP news (SSL)
LDAPs	636	636	Secure LDAP (LDAP suojattu TLS/SSL:illä)
SOCKS	1080		Internet Proxy
Lotus Notes	1352		
Citrix ICA	1494, dyn>= 1023	1604, dyn>= 1023	Remote Application Access
H.323 Host Call	1720	1720	
PPTP	1723		VPN PPTP käyttää myös GRE-protokollaa
PGPfone		4747	Secure Phone

Salausmekanismeja

PROTOKOLLA			LISÄSELVITYS
IPSec			Pakettitason salaus
SSH	22	22	SSH-yhteydellä voidaan suojata paljon muitakin yhteyksiä, kuten kuin Telnet ja FTP
SSL			Istuntotason suojaus, jota käytetty monen protokollan suojaamiseen
PGP			Pretty Good Privacy Suojattu sähköposti
S/MIME			Suojattu sähköposti

Secure RPC			Etäproseduurikutsujen suojaaminen
SET			Luotettava elektroninen maksaminen
Cybercash			Elektroninen maksaminen

IP-TASON SUOJAAMINEN

Perustuu yleensä IPsec

PALVELU	IPV4	IPV6	LISÄSELVITYS
*	Turvaton	Tietoturva huomioitu	http://www.iana.org/assignments/port-numbers

LIITE 5: Lyhenteitä ja käsitteitä

Active Server Pages	ASP. Tekniikka dynaamisen sisällön tuottamiseen. Perustuu Microsoftin kehittämien komentokielen käyttämiseen.
Address Resolution Protocol	ARP. Protokolla, jolla IP-osoite muunnetaan fyysiseksi osoitteeksi.
Application Service Provision	ASP. Sovellusvuokraus.
base64	Menetelmä binääritiedon muuntamiseksi ASCII- muotoon ja päinvastoin.
Berkeley Internet Name Domain	BIND. Yleisin nimipalveluohjelmisto.
Border Gateway Protocol	BGP. Reitittimien käyttämä protokolla reititystietojen vaihtamiseen.
Cascading Style Sheets	CSS. W3C:n määrittelemä tyylikieli, jolla voidaan erottaa HTML- dokumenttien esitystapa (ulkoasu) niiden rakenteesta. CSS-tiedostoilla voidaan luoda yhtenäinen tyyliasu sivustoille.
Certification Authority	CA. Varmentaja, varmenteita myöntävä organisaatio esim. Väestorekisterikeskus.
Common Desktop Environment	CDE. UNIX-käyttöjärjestelmän graafinen käyttöliittymä-standardi.
Common Gateway Interface	CGI. Tiedonsiirtoliitäntä WWW-palvelimen ja CGI-ohjelman välillä. Jälkimmäinen voi olla millä tahansa ohjelmointikielellä toteutettu.
Cookie	Eväste. Eväste on WWW-sivun tai muun ohjelmiston automaattisesti asiakaslaitteelle asentama ohjelma, jonka avulla kyetään seuraamaan ja arvioimaan laitteella tapahtuvaa Internet-käyttöä, käytetyn laitteen teknisiä ominaisuuksia ja asennettuja ohjelmistoja.
Denial Of Service	DoS. Palvelunestohyökkäys, jolla tukkeutetaan verkko hyödyttömällä palvelupyynnöillä.
Distributed Denial Of Service	DDos. Palvelunestohyökkäys, joka toteutetaan useammalta lähettäjälaitteelta.
Document Object Model	DOM. HTML/XML-sivun oliomalli.
Domain Name Service	DNS. Nimipalvelu muuntaa IP-osoitteet verkkonimiksi ja päinvastoin.
Dynamic Host Configuration Protocol	DHCP. Protokolla, jolla annetaan laitteille vaihtuvat verkko-osoitteet.

ECMAScript	European Computer Manufacturer's Association:in määrittelemä standardi JavaScript-kielestä.
EDI for Administration, Commerce and Transport	EDIFACT. ISO:n määrittelemä tiedon siirron standardi.
Eheydenhallintaohjelma	Ohjelma, joka laskee ja vertaa aineistosta laskettuja tiivisteitä tiedon muuttumisen havaitsemiseksi.
Eteisverkko	DeMilitarized Zone (DMZ). Eteisverkko on osittain suojattu, sisäisestä verkosta eristetty verkkoalue, johon sijoitetaan Internet-verkkoon tarjottavia tai sitä hyödyntäviä palveluita.. Ulkoiseen eteisverkkoon organisaatio sijoittaa yleensä julkiseen käyttöön tarkoitettuja palvelimia, kuten WWW-palvelimen.
eXtensible Markup Language	XML. Määrittely rakenteisen tiedon ja tiedon siirron kuvausten siirtoon organisaatioiden ja sovellusten välillä.
File Transfer Protocol	FTP. Protokolla tiedostojen siirtoon laitteelta toiselle TCP/IP-käytäntöä hyödyntämällä.
Finnish Communication And Internet Exchange ry (FICIX ry)	Suomen Internet-liikenteen solmupisteet omistava yhteisö.
General Packet Radio System	GPRS. Langattoman tiedon siirron standardi.
Grid-computing	Suoritinresurssien virtuaalinen keskittäminen.
Haittaohjelma	Vahingollinen, joko itsenäisesti leviävä tai tiedostoihin liitetty ohjelma jonka tarkoituksena on aiheuttaa eri tasoista haittaa.
HyperText Markup Language	HTML. Sivunkuvauskieli.
HyperText Preprocessor	PHP. WWW-palvelujen ohjelmointikieli.
HyperText Transfer Protocol	HTTP. WWW:n perus-sovellusprotokolla, jolla WWW-palvelimet ja selaimet kommunikoivat keskenään.
Intrusion Detection System	IDS. Tunkeutumisen havainnointijärjestelmä, joka tarkastelee laitteen tai tietoliikenteen toiminnan poikkeamia.
International Standard Organization	ISO. Vuonna 1946 perustettu kansainvälinen standardointijärjestö, jonka nimi ei ole akronyymi, vaan kreikkankielinen sana joka tarkoittaa yhdenvertaisuutta.
International Telecommunication Union	(ITU-T) Aiemmin CCITT. Kansainvälinen telealan ja tietoliikenteen ohjausorganisaatio.
Internet Assigned Numbers Authority	IANA. IP-protokollien parametrejä koordinoiva yhteisö.
Internet Control Message Protocol	ICMP. Tietoliikenteen hallintaprotokolla.

Internet Engineering Task Force	IETF. Internet-tietoliikenteen tärkein standardointielin.
Internet Message Access Protocol	IMAP. Protokolla sähköpostiviestien hakuun sähköpostipalvelimelta.
Internet Protocol	IP. Määrittelee pakettien muodon ja osoitekaavan.
Internet Relay Chat	IRC. Keskustelu(ryhmä)sovellus.
IP-vaihdepalvelin	“Voice over IP”-verkoissa käytetty puhelinvaihd palvelin.
IPSec	Standardikokoelma IP-tason suojattuun tiedonsiirtoon.
IPv4	Internet-protokollan versio 4.
IPv6	Internet-protokollan versio 6.
Joukkolähetys	Multicast. Viestin lähettäminen kerralla useampaan osoitteeseen.
Julkinen avain	Public Key. Epäsymmetrisen salauksessa käytettävän avainparin julkinen osa.
Kaikuviesti	Broadcast. Sanoma, joka lähetetään kaikille verkon laitteille.
Kertakirjautumisjärjestelmä	SSO. Single Sign On. Tunnistamistapa , jossa käyttäjä tunnustetaan istunnon aikana vain kerran.
Langaton lähiverkko	WLAN. Wireless Local Area Network. Korkean taajuuden radioaaltoja hyödyntävä langaton verkkotekniikka.
Layer 2 Tunneling Protocol	L2TP. PPP-protokollan laajennus, joka mahdollistaa VPN-yhteyden.
Mail Exchange	MX. Nimipalvelun sähköpostitietue, jolla löydetään aluenimen sähköposteja käsittelevä palvelin.
Media Access Control	MAC. Laiteosoite, joilla verkkoon liitetyt laitteet tunnustetaan.
Message Digest #5	MD5. Yksisuuntainen tiivistefunktio.
Multipurpose Internet Mail Extension	MIME. Menetelmä, jolla muussa kuin ASCII-muodossa oleva tieto voidaan muuntaa ASCII-muotoon sen Internetissä siirtämistä varten.
Network Address Translation	NAT. Menetelmä, jota käytettäessä voidaan lähiverkossa käyttää Internetissä näkymättömiä verkko-osoitteita.
Open Shortest Path First	OSPF. Reititysprotokolla, joka laskee parhaan reitityspolun autonomisen järjestelmän solmujen välillä.

Open Systems Interconnection Architecture OSI.	ISO-standardiin perustuva arkkitehtuuri. Seitsemään protokollakerrokseen perustuva tiedonsiirtoverkkojen kehysmalli.
Personal Identification Number	PIN. Tunnusluku
Pikaviestisovellus	IM, Instant Messaging. Vertaisverkkoihin perustuva, kahdenväliseen, tosiaikaiseen toimintaan perustuva viestintä- tai tiedonsiirtojärjestelmä.
Point-to-Point Tunneling Protocol	PPTP. Microsoftin kehittämä VPN-tekniikka, joka toimii linkkitason tunnelointiprotokollana.
Post Office Protocol	POP. Protokolla sähköpostiviestien hakuun sähköpostipalvelimelta.
Pretty Good Privacy	PGP. Nimi standardille ja salausohjelmalle, jolla voidaan suojata sähköpostiviestejä ja tiedostoja. Perustuu julkisen avaimen järjestelmään.
Primaaripalvelin	Primary Server, jolta ensisijaisesti haetaan esim. nimitietoja.
Private Branch Exchange	PBX. Yksityisen, yhteisön, yrityksen tai näiden yhdistelmien käyttämä yhteinen analoginen puhelinvaihejärjestelmä, jota usein hallinnoi kolmas osapuoli.
Proxy-palvelin	Selaimen ja WWW-palvelimen välissä oleva palvelin joka voi suorituksen nopeuttamiseksi toteuttaa palvelupyynnöt säilyttämällä sivuja muistissaan. Voi myös suodattaa liikennettä.
Public Key Infrastructure	PKI. Julkisen avaimen järjestelmä.
Pääsynvalvontalista	ACL, Access Control List. Pääsynvalvontaan liittyvä palvelu, jossa pidetään yllä tietoa pääsyoikeuksista.
Real-Time Transport Protocol	RTP. Reaaliaikaiseen tiedon siirtoon (video, ääni) tarkoitettu protokolla.
Request for Comments	RFC. IETF-standardin esiaste.
Reverse Address Resolution Protocol	RARP. ARP:n käänteinen toiminto.
Rootkit	Tietoturtojen yhteydessä käytettävä ohjelmisto, joka pyrkii peittämään murtautumislajit.
Routing Information Protocol	RIP. Protokolla, jolla reitittimet vaihtavat tietoja reititystauluista.
Salainen avain	Secret Key. Symmetrisessä salauksessa käytettävä avain.

Secure Hash Algorithm-1	SHA-1. Yksisuuntainen tiivistelaskentafunktio, jolla lasketaan datasta yksisuuntainen HASH-luku, jonka avulla pystytään varmistamaan tiedon eheydestä.
Secure HTTP	SSL:n ohella toinen WWW:n salausprotokollista.
Secure Shell	SSH. Salauksen ja vahvan todennuksen sisältävä etäkäyttöprotokolla.
Secure Socket Layer	SSL. WWW:n yleisin salausprotokolla.
Sekundaaripalvelin	Secondary Server, joka palvelee tiedon haussa toissijaisena palvelimena ja vasta, kun primaaripalvelin ei vastaa.
Server Side Include	SSI. HTML-”kommentti”, jonka kautta voidaan myös kutsua suoritettavia ohjelmia.
Simple Mail Transfer Protocol	SMTP. Protokolla sähköpostiviestien siirtämiseen palvelinten välillä.
Simple Network Management Protocol	SNMP. Joukko verkonhallintaprotokollia.
Sisällöntuottamishjelmisto	Ohjelmistot, joilla tuotetaan tietoja WWW-palvelimelle esim. ASP, CGI tai PHP.
S/MIME	RSA-salauksella suojattu MIME.
Spam	Massapostituksena lähetetty sähköinen kaupallinen viestintä.
Sulkulista	CRL. Certificate Revocation List, varmentajan julkaisema lista niistä varmenteista, jotka on mitätöity (suljettu) niiden voimassaolo aikana.
Sähköinen henkilökortti	Poliisin myöntämä henkilökortti ja matkustusasiakirja, jonka sirulla on Väestörekisterikeskuksen myöntämä kansalaisvarmenne.
Tiiviste	Hash-value, Message Digest. Tiivistelaskentafunktiolla tiedoista muodostettu kiinteämittainen tiiviste.
Transmission Control Protocol	TCP. Protokolla, joka muodostaa tiedonsiirtoyhteyden ja huolehtii mm. pakettien järjestyksestä.
Troijan Hevonen	Hyötyohjelmaksi naamioitu haittaohjelma.
Trusted third Party	TTP. Luotettu kolmas osapuoli, varmentaja.
Uniform Resource Locator	URL. Sähköisen asiakirjan tai muun kohteen osoite Internetissä
User Datagram Protocol	UDP. Pääasiassa broadcast-viesteihin käytetty protokolla.

Vakoiluohjelma	Spyware. Troijan Hevoseen verrattava ohjelma, jolla yleensä kerätään tietoa markkinointitarkoituksiin.
Verkonkuunteluohjelma	Ohjelma, jolla voidaan salakuunnella verkon liikennettä.
Vertaisverkko	Peer to Peer. Työasemien välinen suora tietoliikenne.
Virtual Local Area Network	VLAN. Eri verkkosegmenttien ohjelmallinen yhdistäminen samaksi loogiseksi lähiverkoksi.
Voice over IP	VoIP. Tekniikka, jolla IP-verkoissa voidaan siirtää puheluja.
World Wide Web	WWW. Internet hypermediaverkostona.
Yksityinen avain	Private Key. Epäsymmetrisen salauksessa käytettävän avainparin yksityinen avain.
Yksityinen virtuaaliverkko	VPN. Virtual Private Network. Avoimen verkon kautta salaustekniikalla suojatuin yhteyksin luotu looginen sisäverkko.
X.509	Varmennestandardiehdotus.

LIITE 6: Lähteitä

VAHTI:n suositukset ja VM:n ohjeet (<http://www.vm.fi/vahti>):

- Valtionhallinnon etätyön tietoturvallisuusohje, VAHTI 3/2002 (VM 30/01/2002)
- Toimet tietoturvaloukkaustilanteissa, VAHTI 7/2001 (VM 44/01/2001)
- Valtionhallinnon sähköpostien ja lokitietojen käsittelyohje, VAHTI 5/2001 (VM 34/01/2001)
- Sähköisten palveluiden ja asiointin tietoturvallisuuden yleisohje, VAHTI 4/2001 (VM 32/01/2001)
- Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus, VAHTI 3/2001 (VM 30/01/2001)
- Valtionhallinnon tietojärjestelmäkehityksen tietoturvallisuussuositus, VAHTI 3/2000 (VM 30/01/2001)

Lait, asetukset ja periaatepäätökset:

- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Laki sähköisestä asiointista viranomaistoiminnassa (13/2003)
- Laki sähköisistä allekirjoituksista (14/2003)
- Henkilökorttilaki (829/1999)
- Laki Viestintähallinnosta (625/2001)
- Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999)
- Laki yksityisyyden suojasta työelämässä (477/2001)
- Henkilötietolaki (523/1999)
- Laki sähköisistä allekirjoituksista (14/2003)
- Sähköisen viestinnän tietosuojalakiesitys

Muita lähteitä:

- Valtionvarainministeriö: Valtion tietotekniikan rajapintasuosituksia (27/2001)
- Kerttula, Esa: Tietoverkkojen tietoturva, Edita, 1999
- Hakkerin käsikirja, Maximum Security, Edita 2002
- Tietoturvasertifikaatti-CISSP, Edita 2002
- Yksityisyyttä suojaavat palvelut verkkoviestinnässä, LVM 2002
- Raimo Koski, Tomi Kajala, Linux, Red Hat Linux 7, EDITA 2001
- Allen, Julia H.: Verkkotietoturvan hallinta – CERT, Edita, 2002
- William R. Cheswick, Steven M. Bellovin, Firewalls and Internet Security
- Karanjit Siyan, Internet Firewalls and Network Security, NRP 1995
- W. Richard Stevens, TCP/IP Illustrated, Volume 1, The Protocols
- Steven Splaine, Stefan P. Jaskiel, The Web Testing Handbook STQE 2001
- Wack et al: Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41 (www.nist.gov/)
- Tracy et al: Guidelines on Electronic Mail Security, NIST Special Publication 800-45 (www.nist.gov/)

LIITE 7: Valtiovarainministeriön ja VAHTIn tietoturvallisuusohjeistoa

- Valtion tietohallinnon Internet-tietoturvallisuusohje, VAHTI 1/2003
- Arkaluonteisten kansainvälisten aineistojen käsittelyohje, VAHTI 4/2002
- Etätyön tietoturvaohje, VAHTI 3/2002
- Tunnistamisperiaatteet valtionhallinnon verkkopalveluissa, VM 2002
- Tietoteknisten laittilojen turvallisuussuositus, VAHTI 1/2002
- Tietotekniikan turvallisuus ja toiminnan varmistaminen, VM ja PTS, 2002
- Toimet tietoturvaloukkaustilanteissa, VAHTI 7/2001
- Tietotekniikkahankintojen tietoturvaluustarkistuslista, VAHTI 6/2001
- Sähköpostin ja lokitietojen käsittely, VAHTI 5/2001
- Sähköisten palveluiden ja asiointin tietoturvallisuuden yleisohje, VAHTI 4/2001
- Salauskäytäntöjä koskeva valtionhallinnon tietoturvaluussuositus, VAHTI 3/2001
- Valtionhallinnon lähiverkkojen tietoturvaluussuositus, VAHTI 2/2001
- Valtion viranomaisen tietoturvaluustyön yleisohje, VAHTI 1/2001
- Tietokoneviruksilta ja muilta haittaohjelmistoilta suojautumisen yleisohje, VAHTI 4/2000
- Tietojärjestelmäkehityksen tietoturvaluussuositus, VAHTI 3/2000
- Valtion tietoaineistojen käsittelyn tietoturvaohje, VAHTI 2/2000
- Tarpeettomien tietoaineistojen hävittämisohje, VM 19.4.2000
- Valtionhallinnon tietoturvaluuskäsitteistö, VAHTI 1/2000
- Tietojärjestelmäselosteen laadintasuositus, VM 17.2.2000
- Salassa pidettävien tietojen ja asiakirjojen turvaluokittelu- ja merkintäohje
- Tietohallintotoimintojen ulkoistamisen tietoturvaluussuositus, VAHTI 2/1999
- Suositus toimitilaturvaluudesta, VM 31.12.1998
- Tietoturvaluuden tulosohtaus ja kehittämisvälineet, VAHTI 2/1997

