

ETÄKÄYTTÖ YLIOPISTOISSA

Suositus 4.2.2004

Sami Koskinen
Paavo Moilanen
Tuomo Myllynen
Kari Välimäki

SISÄLLYSLUETTELO

JOHDANTO	1
DOKUMENTIN TARKOITUS	1
MÄÄRITELMÄT JA RAJAUKSET.....	1
KÄYTTÄJÄHALLINTO.....	2
KÄYTTÖOIKEUDET	2
VALVONTA.....	3
ETÄYHTEYS JA ETÄKÄYTTÖ	4
SISÄVERKON LAAJENTAMINEN	5
LANGATTOMAT YHTEYDET	6
ETÄYHTEYKSIEN SUOJAUS.....	7
KUSTANNUKSET	7
ETÄTOIMIPISTEET JA YHTEISTYÖKUMPPANIT	8
ETÄPALVELUT	9
ETÄKÄSITELTÄVÄ MATERIAALI.....	10
TIETOTURVA	11
OHJEISTAMINEN	12

JOHDANTO

Tietokoneiden ja sähköisten palvelujen käyttö on yliopistoissa rakennettu alkujaan yliopiston omissa tiloissa tapahtuvaa käyttöä ajatellen. Tietoliikenteen kehittyminen on tarjonnut mahdollisuuden laajentaa käyttöä myös yliopiston ulkopuolelle. Tämä on hoidettu yliopistoissa eri tavoin ja palveluita on voitu rajoittaa tai ehdollistaa jollakin tavalla. Käytön laajentuessa yliopiston hallintavallan ulkopuolelle syntyy tilanteita, joissa tarvitaan ohjeita, sopimuksia, sitoutumista ja varmistamista suojatulle käytölle.

Dokumentin tarkoitus

Tämä dokumentti määrittelee yleisellä tasolla niitä seikkoja, joita on huomioitava tarjottaessa yliopiston tietoteknisiä palveluja yliopiston varsinaisen sisäverkon ulkopuolelle. Tavoitteena on riittävä määrittely täydellisen sijasta. Jokaisen yliopiston on itse tehtävä tarvittavat päätökset toteutuksesta ja sen laajuudesta.

Määritelmät ja rajaukset

Etäyhteydellä tarkoitetaan yhteyttä, joka muodostetaan yliopiston ulkopuolelta jollakin teknisellä menetelmällä ja tietoliikennelaitteilla ja ohjelmistoilla käyttäjän päätelaitteen ja yliopiston tietoliikenneverkon välille. Etäyhteys mahdollistaa **etäkäytön** eli esimerkiksi kotoa tai matkalta voidaan käyttää joitakin yliopiston tietoteknisiä palveluja. Näitä **etäpalveluja** voivat olla esimerkiksi www-käyttö, sähköposti tai pääsy omaan kotihakemistoon.

Etätyö on työsuhteeseen perustuvaa työsopimuksen alaista toimintaa ja se rajataan tämän tarkastelun ulkopuolelle. Työaika-, palkka- ja muut korvauskysymykset liittyvät työsopimukseen tai erillisiin työntekijän ja työnantajan välisiin sopimuksiin eikä näitä kysymyk-

Lyhyesti

- Etäyhteydellä tarkoitetaan tietoliikenneyhteyttä viraston sisäverkon ulkopuolelta.
- Etäkäytöllä tarkoitetaan tietoteknisten palvelujen käyttöä etäyhteyden avulla.
- Etätyöllä tarkoitetaan muualta kuin viraston vakituisessa toimipisteessä suoritettavaa työtä.
- Virkatöiden täydennystehtäviä ovat [omaehtoisella päätöksellä] etäyhteyden kautta hoidettavat, normaalisti virkapaikalla tehtävät työt.

siäkään tarkastella tässä raportissa. Mikäli etätyöhön liittyy yliopiston tietotekniikka-palvelujen käyttöä, on etätyöstä sopimisen yhteydessä sovittava myös etäkäytöstä ja sen toteutustavoista. Työpaikan ulkopuolella tehtävät virkatöiden täydennystehtävät ovat omaehtoista työtä työpaikan ulkopuolella ja siinä voidaan tarvita etäyhteyksiä.

KÄYTTÄJÄHALLINTO

Tietotekniikassa käyttäjähallinnon tehtävänä on myöntää ja valvoa käyttöoikeuksia ja -lupia ja pitää niihin liittyviä tietoja jatkuvasti ajan tasalla. Käyttöoikeuksien ja eri-laisten käyttölupien myöntäminen saattaa kuulua monelle eri taholle, koska tietoja hallitaan kunkin sovellusalueen omissa sovelluksissa, rekistereissä tai tietokannoissa. Käyttöoikeus voi olla myös henkilön työtehtäviin sidottu. Käyttäjähallinto voi olla jaettu siten, että tietotekniikkakeskus hoitaa käyttöoikeuksien teknisen kirjaamisen jonkun muun rekisterinpitäjän tai palvelun tarjoajan tekemän valtuutuksen perusteella. Näiden vastuullisten osapuolien välillä pitää toimia joustava tietojen vaihto kumpaankin suuntaan reaaliaikaisen ylläpidon takaamiseksi.

Tulevaisuudessa yliopistojen väliset rajat hämärtyvät. Tavoitteena on, että yhdestä yliopistosta saamallaan tunnuksella käyttäjä voisi käyttää myös jonkun toisen yliopiston hallinnoimia järjestelmiä hankkimatta uutta tunnusta toisesta yliopistosta. Joustavuutta tavoiteltaessa voi syntyä myös tilanteita, joissa käyttäjälle annetaan liian monia tai liian laajoja palveluja vieraan yliopiston tietojärjestelmiin. Tästä syystä on tärkeää, että yliopistojen välillä on yhdenmukainen ja samojen suositusten mukaisesti toimiva käyttäjähallinto.

Käyttöoikeudet

Käyttö- ja pääsyoikeudet perustuvat käyttäjän asemaan ja roolin yliopistossa. Perusrooleja on kaksi: opiskelijan rooli ja yliopiston henkilökuntaan kuuluvan jäsenen rooli. Henkilökunnalla on

Päätettävää

- Kuka saa käyttää etäyhteyksiä ja millä ehdoin.
- Kenen tehtävä on myöntää etäkäyttöoikeus.
- Miten käyttöoikeutta haetaan.
- Miten pitkään käyttöoikeus on voimassa.
- Mitä etäyhteyden yli saa tehdä.
- Miten käyttöä valvotaan.
- Missä tapauksessa käyttöoikeus peruutetaan.

lisäksi työ- ja luottamustehtäviin liittyvän vastuun määrittelemiä muita rooleja. Opiskelijoiden muut roolit voidaan johtaa opintosuunnasta, opinto-oikeudesta, aineyhdistelmistä jne. Tietoteknisen ylläpito henkilöstön työtehtävien määrittelemät käyttäjätunnuksiin, pääsynhallintaan ja käytön valvontaan liittyvät roolit laajoine valtuuksineen on huomioitava erityisesti. Vastaavia erityisrooleja voi tulla myös ulkopuolisille yhteistyökumppaneille heidän ylläpitäessään jotain yliopiston järjestelmää tai tuottaessaan jotain palveluja.

Henkilöiden mahdolliset kaksoisroolit saattavat muodostaa ongelmia. Henkilö voi olla töissä yliopistossa ja samalla jonkun toisen organisaation työntekijä tai osakas. Usein myös opiskelijat toimivat yliopiston palkkaamina työntekijöinä. Kaksoisroolit ovat käyttäjähallinnolle hankalia, mutta niiden aiheuttamat ongelmat on pyrittävä minimoimaan varautumalla tilanteeseen ennakolta.

Valvonta

Yliopiston erilaiset tietotekniset palvelut pidetään tarjolla eri tavoin kontrolloituina. Palvelut voivat olla avoimia (anonyymeja), heikon tunnistuksen vaativia tai vahvan tunnistuksen suojaamia. Palvelujen käyttöä voidaan rajata. Esimerkiksi käyttö voi olla sallittua vain tiettyinä kellonaikoina ja viikonpäivinä tai vain nimetyiltä päätelaitteilta. Rajaukset tietojen käyttötarkoituksesta, salassapidosta tai tietojen luovuttamisesta on kirjattava tietojärjestelmä- ja rekisteriselosteiden lisäksi myös käyttäjäkohtaisiin sopimuksiin.

Palveluihin pääsyä ja palveluiden käyttöä valvotaan. Pääsyn valvontaan käytetään perinteisen käyttäjätunnus-salasanaparin lisäksi tai sijasta tarvittaessa vahvan tunnistuksen tarjoavia välineitä, kuten toimikortteja. Tunnistuksen jälkeen käyttäjän pääsy- ja käyttöoikeudet määräytyvät hänen kulloisenkin roolinsa perusteella.

Kirjautumista ja kirjautumisyrityksiä sekä kaikkea käyttöä valvotaan keräämällä lokitietoja käyttäjistä, yhteyksistä, laitteista, toiminnoista ja tapahtuma-ajoista. Lokitietoja tulee kerätä riittävällä tarkkuudella, jotta niiden perusteella voidaan tarvittaessa selvittää toimintavirheet ja mahdolliset väärinkäytökset.

Käytön valvonnan ja lokitietojen keruun pitää aina olla hyvin perusteltua ja käyttäjän tulee olla tietoinen valvonnasta. Käytännössä tämä tarkoittaa valvottavien seikkojen esittelemistä henkilöstölle tai jollekin yhteistoimintaelimelle ja kirjaamista perustelluineen käyttö sopimukseen ja palvelukuvauksiin. Jokainen käyttäjäksi ryhtyvä allekirjoittaa käyttö sopimuksen, jolla hyväksyy lokitietojen keruun. Yliopistojen tietoteknisten palveluiden yhteiskäytön vuoksi käyttö sopimuksia tulee myös päivittää siten, että niissä myönnettyyn käyttö oikeuteen liittyvien lokitietojen keruu on oikeutettua kaikissa käyttäjälle samalla sopimuksella oikeutetuissa käyttö paikoissa ja palveluissa.

ETÄYHTEYS JA ETÄKÄYTTÖ

Etäyhteys rakennetaan siten, että sitä voidaan pitää käyttötarkoitukseensa riittävän turvallisena. Yksinkertaisimmassa tapauksessa kaikki yhteydet ovat samalla tavalla määritellyjä ja riittävän turvallisia kaikkeen käyttöön. Tällöin yhteydet rakennetaan sen mukaan, millaista suojaustasoa enimmillään tarvitaan, vaikka yhteys muihin tarpeisiin nähden on jopa ylisuojattu.

Käyttöpolitiikassa on harkittava, mitä käyttöä ja toimintoja etäyhteydellä sallitaan hoidettavaksi ja millä ehdoilla. Yleensä etäyhteydellä hoidetaan vain sellaisia tehtäviä, joiden hoitaminen ei aiheuta tarpeettomia tietoturvariskejä. Kaikkein riskialttiimpia toimintoja ei etäyhteyden välityksellä tule sallia. Yleisesti olisikin tarpeen jakaa toiminnot ryhmiin tai turvaluokkiin, joille kullekin määritellään, voiko etäyhteyttä yleensä käyttää ja jos voi niin miten toteutettuna.

Vastuu etäyhteydestä ja etäkäytöstä muodostuu kolmijakoiseksi:

1. teknisesti luotettavasta tietoliikenneyhteydestä vastaa tietoliikenneyhteyden tarjoaja
2. käyttöoikeuden myöntäjä tai palvelun tarjoaja vastaa käyttöoikeuksien myöntämisestä ja käytön valvonnasta
3. käyttäjä on vastuussa käytöstä ja saamiensa ohjeiden noudattamisesta.

Etäkäytön yhteyspalvelun tarjoaja määrittelee vaihtoehdot: takaisinsoitolla varustettu modeemi- tai ISDN-ratkaisu puhelinverkossa, kiinteästi kytketty datayhteys, yliopis-

ton verkkoon päätetty ADSL-yhteys, Internetin kautta muodostettu VPN-yhteys ja joissakin tapauksissa yhteys Internetin kautta ilman VPN:ää. Kulloinkin etäkäyttöön soveltuvan ratkaisun valinta riippuu järjestelmien tietosisällöstä ja käyttäjäkunnasta sekä käyttötavasta. Järjestelmien jako turvaluokkiin selkeyttää oikean etäkäyttötavan määrittämistä.

Käyttäjähallinto liittyy aina eri järjestelmien tai palvelun etäkäyttöön myöntämällä ja poistamalla käyttöoikeuksia ja niihin kuuluvia toimintoja. Käyttäjähallinto valvoo myös käyttäjiä ja tapahtumia ja sekin hyötyisi toimintojen ja järjestelmien turvaluokituksesta.

Käyttäjän tulee noudattaa saamiaan ohjeita ja hänelle jää myös velvollisuus ilmoittaa käyttäjähallinnolle kaikesta havaitsemastaan epätavallisesta tapahtumasta yhteyttä tai järjestelmää käytettäessä. Käytöstä on tarpeen tehdä käyttäjän ja yliopiston välille kirjallinen sopimus käytön tarkoituksesta ja vastuunjaosta ja mitä järjestelmää tai palvelua se koskee sekä miten yhteys teknisesti pitää muodostaa ja kenen ulkopuolisten tietoliikenneyhteyksien tarjoajien palveluja suositellaan käytettäväksi.

Sisäverkon laajentaminen

Perinteisesti on yliopiston ulkopuolelta luotu etäyhteydet puhelinverkkoon liitetyllä yliopiston omalla soittosarjapalvelulla. Puhelinyhteyksiin voi liittyä soittajan puhelinnumeron tarkistaminen ja yhteys muodostuu vasta takaisinsoitolla. Perinteisen modeemin tilalla voi olla myös ISDN-yhteys (Integrated Services Digital Network), mutta selvästi nopeammat laajakaistayhteydet ovat yleistymässä. Nämä ADSL-yhteydet voidaan päättää yliopiston omaan verkkoon, jolloin yhteyden liikenne on yliopiston omassa hallinnassa.

Soittosarjapalvelu voidaan myös ulkoistaa. Käyttäjien tunnistamiseen ja todentamiseen käytetystä menettelystä on tällöin sovittava yliopiston ja teleoperaattorin kesken ja huolehdittava, että palvelun ja yliopiston välinen liikenne on suojattua. Tämä yhteysmuoto on muistettava huomioida toimintojen etäkäytön kategorisoinnissa.

Puhelinverkkoyhteydet samoin kuin laajakaistayhteydet ovat salaamattomia. Yliopis-

ton oma soittosarjapalvelu yliopiston omissa tiloissa voi olla turvallisempi kuin yliopiston verkkoon päätetyt laajakaistayhteydet ja ne taas voivat olla turvallisempia kuin ulkoisen soittosarjapalvelun käyttäminen jos soittosarjan liikennettä ei salata.

Sisäverkon laajentaminen voi olla tarpeen myös jonnekin ennalta määrittelemättömään paikkaan kuten matkoilla lentoasemat, hotellihuoneet, konferenssitilat tai vierailut yliopistoihin, tutkimuslaitoksiin tai yrityksiin. Etäkäytettävän palvelun sisältö voi olla sellaista, että yhteys pitää olla luotettava ja siirtyvän aineiston on pysyttävä salassa. Puhelinyhteys yliopiston soittosarjapalveluun on perinteinen tapa, mutta puutteena on heikko luottamuksellisuus ja suuret käyttökustannukset. Parempi vaihtoehto on salaava VPN-yhteys.

Langattomat yhteydet

Yhteys yliopiston verkkoon voidaan muodostaa myös langattomalla tekniikalla. Langattomalla osalla verkko ei ole kuitenkaan enää rajautunut huoneeseen eikä rakennukseen ja sitä voidaan käyttää kuuluvuusalueella myös käytävillä ja aula- sekä ulkotiloissa jopa yllättävän laajalla alueella. Tästä syystä kaikki langattomat yhteydet, myös yliopiston sisällä, ovat yhteyksiä yliopistoverkon ulkopuolelta. Langattomat verkot (WLAN) tulee erottaa omaan virtuaaliverkkoonsa (VLAN) yliopiston muusta verkosta ja sallia niistä pääsy varsinaiseen sisäverkkoon vain riittävän turvallisella tavalla.

Sen lisäksi, että yhteys tietoliikenneverkkoon on langaton, voi langattomia yhteyksiä olla myös erilaisten laitteiden välillä (näppäimistö, hiiri, tulostin jne) usealla eri tekniikalla (radioyhteys, infrapuna, Bluetooth). Tietovuotoja voi tapahtua näiden laitteiden välisessä tiedonsiirrossa koska sivulliset voivat seurata sitä kuten varsinaista verkkoliikennettäkin. Tietoturvariskien välttämiseksi tarvitaan selkeä ohjeistus tarvittavista suojaustoimenpiteistä ja siitä, mikä käyttö langattomalla yhteydellä sallitaan ja mitä ei. Siitäkin on sovittava, mistä langatonta yhteyttä saa tai ei saa käyttää. Vaikeasti suojattavia paikkoja ovat julkiset tilat kuten lentoasemat, konferenssi- ja messualueet sekä ravintolat ja kahvilat.

Langattomuus on ulkopuolisille kiinnostava mahdollisuus. Erilainen väärinkäyttö ku-

ten laittomien ohjelmakopioiden, videoiden, kuvien tai roskapostin lähettäminen voi heille onnistua ilman seuraamuksia.

Etäyhteyksien suojaus

Tietoliikenneyhteyksien on oltava suojattuja etäyhteyksiä käytettäessä, mutta sisäisissäkin yhteyksissä salattua liikennöintitapaa kannattaa käyttää jos sellainen vaihtoehto on tarjolla ja sen käyttö on mahdollista. Palomuureilla voidaan estää turvattomien liikennöintitapojen käyttö.

Yliopiston omaa verkkoa voidaan laajentaa ja suojata myös siten, että käyttäjän työaseman ja palvelimen välille muodostetaan suojattu putki, jota pitkin tiedot liikkuvat (VPN Virtual Private Network) suojassa ulkopuolisilta. Tällaiset salaavat VPN-yhteydet päätetään tavallisesti palomuriin tai erilliseen VPN-keskittimeen, joka voi olla myös VPN-ominaisuuksilla varustettu reititin.

Eri yritysten VPN ratkaisut eivät ole samanlaisia eivätkä keskenään välttämättä yhteensopivia. Osa toteutuksista ei ole salaavia ja salauksien tasoissakin on eroja. VPN yhteyksiä rakennettaessa on syytä pitäytyä ratkaisuissa, jotka noudattavat IPSEC suosituksia. Erityisesti mobiilikäyttäjille tarkoitetuissa palveluissa kannattaa pysyä yhden valmistajan tuotteissa, sillä yhteensopivudessa on valmistajakohtaisia eroja.

Käyttäjän työasemaan VPN-yhteyden muodostamiseksi tarvittavat ohjelmat ja niiden asennusohjeet on tarjottava luotettavalla ja yksinkertaisella tavalla. Tarjolla pidetään käytössä olevia versioita ohjelmista ja versioiden vaihtuessa huolehditaan siitä, että vanha versio päivittyy automaattisesti tai päivittämistarpeesta tiedotetaan. Epäluotettavalla versiolla etäyhteyden muodostus kielletään ja käyttö tulee estää jos se on mahdollista.

Kustannukset

Etäkäytöstä sovittaessa nousee säännöllisesti esiin kysymys kustannusten jaosta. On luonnollista, että henkilö, joka kokee tekevänsä työnantajalleen työtä varsinaisen työajan ulkopuolella, usein muualla kuin varsinaisella työpaikalla, odottaa työnantajan

tulevan jollakin tavalla vastaan työn suorittamiseen liittyvissä kustannuksissa. Kustannuskohteita ovat laite-, ohjelmisto- ja tietoliikennekustannukset sekä mahdolliset työtila- ja asennuskustannukset.

Työnantajan tulisi tarjota riittävät työvälineet turvalliseen etäkäyttöön. On suositeltavaa listata etäkäytön eri käyttötapaukset ja määrittää eri käyttötapauksissa tarvittavat välineet kunkin käyttötilanteen vaatiman vähimmäisturvatason saavuttamiseksi. Joissakin tilanteissa riittää, että järjestelmää käytetään työntekijän itse hankkiman tietoliikenneyhteyden kautta työntekijän omalla tietokoneella, mutta eräissä tilanteissa on syytä harkita työnantajan määrittämiä, ylläpitämiä ja kustantamia yhteyksiä ja tietokoneita. Sähköpostin lukeminen voi esimerkiksi olla sallittua työntekijän itse valitsemasta paikasta työnantajan vaikuttamatta mitenkään käytettävään tietoliikenneyhteyteen tai tietokoneeseen, jota käytetään. Sen sijaan kriittisten järjestelmien, kuten esimerkiksi tietoliikenteen aktiivilaitteiden tai käyttäjähallinnan ylläpito tai jopa käsittely muualta kuin työpaikalta voi olla syytä rajata tapahtuvaksi ainoastaan työnantajan täysin kustantamilta ja ylläpitämiltä tietoliikenneyhteyksiltä ja tietokoneilta. Eräissä järjestelmissä, kuten esimerkiksi lokipalvelussa, etäkäyttö on syytä kieltää.

Mikäli työnantaja maksaa tai tarjoaa esimerkiksi tietoliikenneyhteyksiä työntekijälle, tästä voi syntyä työntekijälle verotettavaa tuloa. Jos kustannettujen työvälineiden käyttö liittyy työtehtäviin, mutta niitä käytetään myös yksityiskäyttöön, on työntekijän itse selvítettävä verottajan kanssa mahdolliset veroseuraamukset.

Etätoimipisteet ja yhteistyökumppanit

Jotta etätoimipisteessä olisi käytettävissä yhtäläiset palvelut kuin yliopistolla, sisäverkkoa laajennetaan niihin käyttötarpeen edellyttämällä tavalla. Eri toimipisteisiin harkitaan tapausittain luotettavin ja tarkoituksenmukaisin laajentamistapa. Tietoliikennetapaukset eri toimipisteissä voivat olla erilaisia.

Yhteistyökumppaneille voidaan tarvittaessa myöntää etäkäyttöoikeus vastaavalla tavalla kuin yliopiston omalle henkilökunnalle. Tällöinkin on huolehdittava siitä, että etäyhteyden ylitse pääsee käyttämään vain kumppanin roolin mukaisia palveluja ja

vain niitä. VPN-tekniikka on yksi tapa suojata yliopiston ja yhteistyökumppaneiden verkkojen välillä tehtävä luottamuksellinen tiedonsiirto internetin yli.

ETÄPALVELUT

Yliopiston tarjoamat etäpalvelut on jaettavissa sisäisiin, vain yliopiston henkilökunnalle ja opiskelijoille tarkoitettuihin palveluihin ja toisaalta julkisiin, kaikille kiinnostuneille avoimiin palveluihin. Sisäiset palvelut edellyttävät käyttäjän tunnistamista tai niiden käytölle on jokin muu rajoittava ehto palvelun laadusta riippuen. Pääsääntöisesti etäpalveluja tarjotaan virkatöiden täydennystehtävien ja opiskeluun liittyvien tehtävien hoitoon, mutta myös tutkimus ja tieteellinen yhteistyö käyttävät monia etäpalveluja maailmanlaajuisesti. Eri yhteistyökumppaneille tarjottavista palveluista on sovittava aina tapauskohtaisesti.

Palvelujen luokittelu

- Julkiset palvelut ovat tarjolla kaikkialle maailmaan.
- Etäkäytettävät palvelut edellyttävät käyttäjän tunnistamista ja tietoturvallista yhteyttä.
- Etäylläpito on tietoteknisistä palveluista vastaaville henkilöille tarjottu mahdollisuus tehdä kiireellisiä ylläpitotöitä erityisen turvallisen etäyhteyden kautta.
- Sisäisten palvelujen käyttö on rajattu yliopiston sisäverkkoon, eikä niitä voi käyttää etäyhteyden kautta.

Etäpalvelut tarvitsevat luokituksen, josta voidaan johtaa sitten etäkäytön toteutustavat kullekin luokalle. Etäpalvelut tarjotaan käyttäjille siten, että palvelun tietosisältö pysyy palvelulle asetetulla turvatasolla, mutta käytöstä ei kuitenkaan tehdä käyttäjälle liian monimutkaista. Yleisimmät palveluja välittävät liikennöintikäytännöt (protokollat) tukevat salausta, eikä salauksen käyttäminen lisää merkittävästi kuormitusta nykyisillä laitteilla eli mitään erityistä etua ei saada salaamattoman yhteyden käytöstä.

Salaus voi olla myös epäilyttävä jos valmistaja ei avoimesti jaa tietoja toteutuksestaan. Epäluotettava salaus voi vaarantaa paitsi tietosisällön myös järjestelmien käyttöturvallisuuden vuotamalla käyttöoikeuksia sivullisille.

Salauksen tulisi käyttää hyväkseen varmenteita. Varmenteita voidaan lisäksi käyttää myös järjestelmien sekä käyttäjien vahvaan tunnistamiseen. Varmenteilta tulee vaatia

julkisesti saataville niihin liittyvä varmennepolitiikka CP (Certificate Policy) tai varmennekäytäntö CPS (Certification Practice Statement). Näiden avulla voidaan muodostaa käsitys varmenteen myöntäneen tahon luotettavuudesta.

Sisäisiä palveluja voivat olla esimerkiksi yliopiston kirjaston tarjoamat tietokannat, informaatiopalvelu ja muut tietolähteet, sähköposti, opiskelijarekisteri sekä kurssi- ja tentti-ilmoittautumisjärjestelmät. Käyttäjän tunnistaminen ja todentaminen tulisi aina tapahtua siten, että tapahtumaan liittyvän tiedon eheydestä ja luottamuksellisuudesta voidaan olla varmoja. Palvelun saatavuus voidaan rajata myös siten, että se on tarjolla vain yliopiston verkosta ei sen ulkopuolelta.

Yleisenä suosituksena on, että tarjolla on vain sellaisia sisäisiä ja julkisia palveluja, jotka on rekisteröity yliopistolle annettujen ohjeiden mukaisesti. Palveluista tulee olla tiedossa palvelun tarjoaja, tarkoitus, käyttäjäkunta ja ylläpito.

ETÄKÄSITELTÄVÄ MATERIAALI

Kaikki tärkeä tietoaineisto säilytetään ensisijaisesti yliopiston palvelimilla. Säilytyksestä on sovittava, missä aineistoa säilytetään, tarvittaessa palvelin- ja hakemistokohteisesti. Säilytysmuodoista on myös hyvä sopia. Käyttäjän omalla laitteistolla ei pitäisi säilyttää yliopiston tietoaineistoja eikä varsinkaan millään kannettavalla päätelaitteella. Mitään virallista aineistoa ei saa olla ainoana kopiona käyttäjän työasemassa tai käyttäjän tietovälineillä. Kun aineistoa säilytetään yliopiston palvelimilla, voidaan varmuuskopioinnista huolehtia järkevästi.

Tietoaineiston käsitteleminen käyttäjän työasemassa voi muodostaa uhan tietojen päätyemisestä asiattomiin käsiin. Kun työasemassa käsitellään tietoja, syntyy paikalliselle levyasemalle työkopioita ja välitalennuksia tai eri tasoisia vedoksia. Tiedostojen poistaminen ei tuhoa tietoja levyiltä vaikka ne eivät enää olekaan käyttäjän nähtävissä. Kannettavien laitteiden yleistymisen, niiden pieni koko ja mukana kuljettaminen on tehnyt niistä suosittuja kohteita varkaille. Koneen mukana katuvat myös tiedot. Käsiteltävän aineiston tulostaminen paperille ja aineiston jollain tietovälineellä olevat versiot ovat myös uhka tietovuodolle. Tulosteiden oikea hävittäminen ja tietovälinei-

den huolellinen käsittely on tärkeää ja sekin kannattaa ohjeistaa.

Etäkäsittelytietoa on luotava luokitus, jossa määritellään kunkin luokan osalta säännöt käsittelylle ja säilytykselle sekä aineiston tuhoamiselle. Luokitus voi olla sama kuin etäkäytettävillä palveluilla. Luottamuksellista tietoa saa käsitellä ainoastaan järjestelmissä, joissa käytetään vahvaa salausta sekä tunnistuksessa että tietoa talletuksessa. Salaustavasta on syytä sopia yliopiston kanssa etukäteen, erityisesti jos salausta on tiedostokohtaista.

Yliopistojen on syytä määrittää hyväksyttävät tiedostojen sekä tietojärjestelmien salaustavat. Samalla on otettava kantaa siihen, onko joissakin tapauksissa syytä käyttää sellaista salausta, jonka yliopisto voi tarpeen vaatiessa purkaa eräänlaisella yleisavaimella. Tällöin salausta on kuitenkin hiukan arveluttava, jos on yleisavain, niin salausta on luultavasti purettavissa myös jollakin muulla tavalla.

TIETOTURVA

Valtiovarainministeriön asettaman Valtionhallinnon tietoturvasuojien johtoryhmä VAHTI on laatinut turvallisuusohjeita etäkäytölle. Tietoturvasuojien ohjeistoa löytyy osoitteesta www.vm.fi/vahti/ ja erityisesti sieltä kannattaa lukea työaseman käyttäjälle tarkoitettu ohje ”Valtionhallinnon etäyhteyden tietoturvasuojien ohje VAHTI 3/3002” ja sitä täydentävä etäyhteyksien rakennusarkkitehtuuria tietoturvan kannalta kuvaava dokumentti ”Turvallinen etäkäyttö turvattomista verkoista VAHTI 2/2003”.

Etäkäyttäjän on itse huolehdittava, ettei etäpisteestä ole ulkopuolisille pääsyä yliopiston järjestelmiin suoraan eikä välillisesti.

Laitteessa, jolla käytetään yliopiston palveluja kytkemällä se osaksi yliopiston sisäverkkoa, on oltava itse yhteyden mahdollistavien ohjelmien lisäksi ainakin

- ajantasainen yliopiston hyväksymä virustorjuntaohjelma, joka päivittyy automaattisesti ja jonka virustietokanta päivittyy myös automaattisesti
- palomuri, joka sulkee etäyhteyttä käytettäessä liikenteen muualta ja muualle kuin yliopiston verkkoon

- mikäli käsitellään ei-julkiseksi luokiteltua tietoaineistoa, tulee koneessa käyttää hakemistojen ja tiedostojen salausohjelmistoa. (VM on pyytänyt ohjelmistoista tarjoukset ja Hansel on tehnyt niistä yhteenvedon, valintaa tai suositusta ei vielä valtiorhallintoon ole annettu).

Yliopisto määrittelee mitkä ohjelmistot ja miten käytettynä toteuttavat riittävän tietoturvan. Yliopisto voi estää etäyhteyden käytön ilman asianmukaisia suojauksia.

OHJEISTAMINEN

Etäkäyttö perustuu monessa asiassa sopimukseen ja luottamukseen. Sopimuksia tarvitaan etäkäytöstä (laitteet, ohjelmat, tietoliikenneyhteydet, asennukset, velvollisuudet, käyttötarkoitus), salassapidosta (aineistot, salasanat ja suojausmenetelmät) ja kustannusten jaosta sekä työajan ja palkkion laskemisesta. Useita ohjeita on laadittava ja olisi tärkeää yhtenäistää niitä ja siksi yliopistojen välinen yhteistyö on tarpeen.

Ohjeiden ja sopimusten aiheita.

- Etäkäyttölupa - kenelle, hakeminen, myöntäminen, velvoitteet
- Etäkäytettävien palveluiden vastuut
- Etäkäyttöratkaisut – laitteet, ohjelmat, asennukset, käyttäjätuki
- Etäkäyttösopimus Liite 1
- Salassapitositoumus - myös ulkopuolisia varten Liite 2