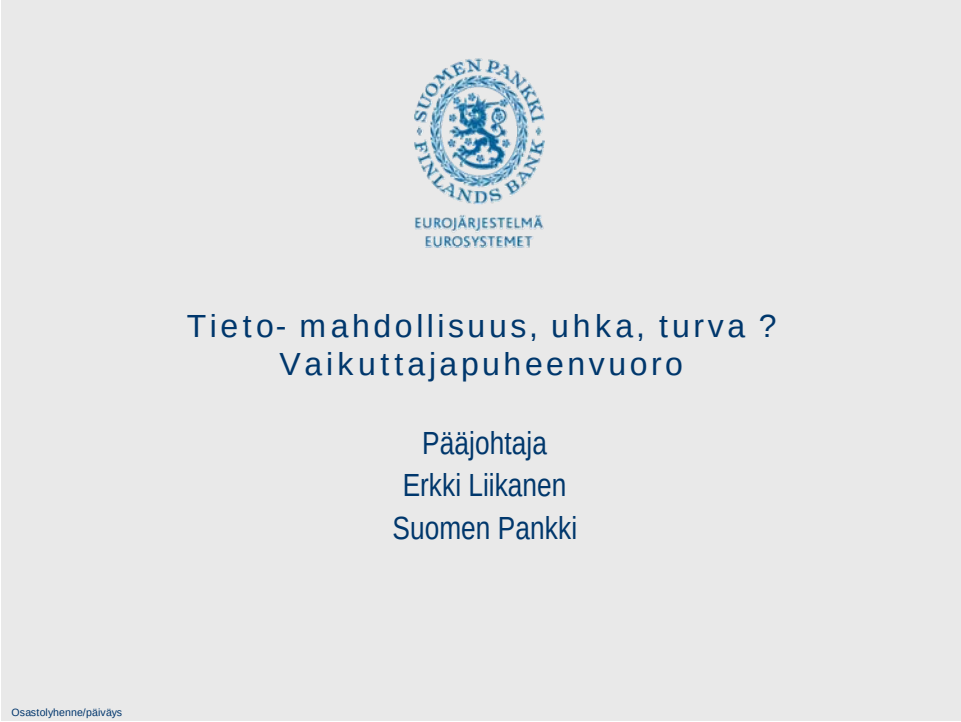
7.2.2006 Marina Congress Center

Pääjohtaja Erkki Liikanen



Tiedosta ja viestinnästä on tullut keskeinen tekijä talouden ja yhteiskunnan kehittymisessä. Jotta voisimme ymmärtää paremmin tietoverkkoja ja niihin liittyvää turvallisuutta, on paikallaan katsoa, miten tähän on tultu.

Tietoverkkojen kehitys ja ennen kaikkea Internetin ja World Wide Webin yleistyminen ovat olleet vallankumouksellinen edistysaskel tietojärjestelmien hyväksikäytössä.

Kauan automaattinen tietojenkäsittely hoidettiin suurilla keskuskoneilla tai minitietokoneilla. Turvallisuus tuli hoidetuksi fyysisillä turvaamismekanismeilla, koska keskusyksiköt, päätteet ja muut oheislaitteet muodostivat yhtenäisiä, mutta yksittäisiä kokonaisuuksia.

Avointen viestintäverkkojen läpimurto muutti kaiken. Erilliset ja jopa eri valmistajien rakentamat tietokoneet voitiin liittää toisiin. Syntyi valloittava uusi visio; kaikki voitiin liittää toisiinsa, vapaasti ja ilman rajoituksia. Tietokoneverkkojen ensimmäinen alue olivat yliopistot ja tutkimuslaitokset sekä eräät suuret yritykset.

Toimistojen henkilökohtaiset tietokoneet, PC:t ja niiden muodostamat lähiverkot yleistyivät räjähdysmäisesti 1980-luvulla. Ja sitten 1990-luvun alussa yleistynyt www-tekniikka toi internet-verkon yleiseen tietoisuuteen. Tietojen jakaminen järjestelmien kesken loi perustan täysin uudentasoiseen tuottavuuden nostamiseen. Tietokantoja voitiin jakaa, informaatiokustannukset laskivat rajusti. Yritykset ja yhteisöt siirtyivät verkkomaailmaan. Yhä kriittisemmät toiminnot tulivat verkoista riippuviksi.

Ensin tuli hieno visio kaiken vapaudesta ja helppoudesta. Mutta sitten havahduttiin; turvallisuusriskit kasvoivat voimakkaasti. Verkkoturvallisuus nousi suureksi kysymykseksi. Vapaan liitettävyyden ideologia ei mahdollistanut liiketoimintakriittisten käyttökohteiden varustamista verkotetuilla järjestelmillä. Tietokonevirukset olivat ensimmäisiä esimerkkejä järjestelmien haavoittuvuudesta.

Kuva 1: Verkko- ja tietoturva – ensimmäinen osa verkkoturvallisuus

Tieto- ja viestintäjärjestelmien turvallisuudesta on tullut päättäjille keskeinen haaste. Politiikkavastausten löytäminen on kuitenkin tullut entistä haastavammaksi. Viestintäpalveluja eivät enää tarjoa valtion omistamat monopolit, vaan useat yksityiset operaattorit ja palveluntarjoajat keskenään kilpaillen, ei vain kotimaassa vaan yhä enemmän Euroopan tai maailmanlaajuisesti. Verkot lähentyvät toisiaan: ne pystyvät tukemaan samoja palveluja, niitä liitetään yhä enemmän yhteen ja ne käyttävät osin samaa infrastruktuuria.

Kuva 1: Verkko- ja tietoturva – toinen osa verkkorikollisuus, kolmas osa hakkerointi

Verkkorikollisuus syntyi. Hakkerointi nousi huolenaiheiden kärkeen. Verkkorikollisuuden erilaiset ilmentymät ovat kuitenkin kehittyneet koko ajan samassa tahdissa, kun tietoverkoissa käsiteltävien taloudellisten tai yleisten intressien koko on kasvanut.

Pitkään verkkorikollisuus oli suurelta osin näppärien nörttien leikkiä, "kiusantekoa" vailla taloudellisia tavoitteita. Tilanne on muuttunut ja taloudellinen rikollisuus verkkojen kautta on lisääntynyt. Olemme saaneet lukea asiantuntijoiden kertomuksia järjestäytyneen rikollisuuden ja tietotekniikka-asiantuntijoiden yhteistyöstä. Ja olemme lukeneet, kuinka kotikoneita on kaapattu roskapostin levityskeskuksiksi.

Kuva 1: Verkko- ja tietoturva – neljäs osa yksityisyyden suoja

Verkkojen suuri tuottavuuskontribuutio liittyy siihen, että tietoja, myös henkilötietoja voidaan tallettaa ja käsitellä verkkoympäristössä. Se on helppoa ja taloudellista.

Mutta samalla ovat lisääntyneet riskit yksityisyydensuojan suhteen. On välttämätöntä suojata kansalaiset ja heidän henkilökohtaiset tietonsa. Laajat tietokannat ja tehokkaat tiedon hakuvälineet mahdollistavat hyvinkin tarkan henkilöiden profiloinnin.
Ellei käyttäjien tietoja ja yksityisyyttä kyetä suojaamaan, ihmiset tulevat säikyiksi eivätkä tietoyhteiskunnan suuret taloudelliset ja yhteiskunnalliset mahdollisuudet voi realisoitua.

Kuva 1: Verkko- ja tietoturva – viides osa identiteetti varkaus

Identiteettivarkaus on tietoverkoissa tarjottaviin palveluihin liittyvä vakava uhka. Identiteettivarkaus tarkoittaa henkilötietojen hankkimista ja väärinkäyttämistä siten, että niiden avulla tehdään sitoumuksia, esimerkiksi avataan tilejä tai tehdään ostoksia verkkokaupassa. Yhdysvalloissa ja Iso-Britanniassa tilastoidaan vuosittain miljoonia tämäntyyppisiä rikoksia ja ilmiö uhkaa luottamusta verkkopalveluiden käyttöön.

Turvallisuuden vähimmäistason varmistamiseksi on sekä kansallisella että EU:n tasolla annettu suuri määrä oikeussäännöksiä televiestinnän sääntelykehyksen ja tietosuojalainsäädännön puitteissa. Näitä säännöksiä on sovellettava tehokkaasti nopeasti muuttuvassa ympäristössä.

Säännösten haaste on, että teknologiat ja myös niiden väärinkäyttö etenevät nopeasti. Siksi lainsäätäjällä ja viranomaisilla riittää haastetta.
Samalla on tärkeää, että yritykset kehittävät koko ajan ratkaisuja turvallisuusongelmien voittamiseksi. Molempien tulisikin kulkea käsi kädessä, regulaation ja teknologisten innovaatioiden.

Turvallisuudesta on tullut markkinoilla ostettava ja myytävä kauppatavara ja osapuolten välisten sopimusten osa. Taloustieteilijät sanovat, että hintamekanismi tasapainottaa turvallisuuden tuottamisen kustannukset ja erityiset turvallisuustarpeet.

Monet turvallisuusriskit ovat kuitenkin yhä ratkaisematta tai ratkaisujen tulo markkinoille on hidasta – merkittävän markkina-aseman saavuttaneet toimijat ovat jarruttaneet kilpailevien ratkaisumallien yleistä hyödyntämistä. Näitä puutteita koskevin erityisin

poliittisin toimin voidaan vahvistaa markkinaprosessia ja samalla parantaa sääntely-järjestelmän toimivuutta. Tällaisten toimien on oltava osa eurooppalaista lähestymistapaa sisämarkkinoiden varmistamiseksi, yhteisistä ratkaisuista hyötymiseksi ja jotta voitaisiin toimia tehokkaasti maailmanlaajuisella tasolla.

Kuva 2 – Eurooppalainen tietoyhteiskunta kehitys

Eurooppalainen tietoyhteiskuntakehitys on edennyt eEurope2002- ja eEurope2005-ohjelmissa. Tietoturvallisuuden alueella ensimmäinen merkittävä linjanveto esitettiin komission tiedonannossa heinäkuussa vuonna 2001. Se ei silloin saanut juurikaan huomiota. Mutta syyskuu 2001 muutti kaiken. Verkkoturvallisuus nousi huolten kärki-joukkoon.

Tämän jälkeen komissio esittikin Euroopan verkko- ja tietoturvaviraston (ENISA) perustamista. Suomalaisina voimme olla ylpeitä siitä, että olemme saaneet merkittäviä tehtäviä virastoon liittyen, onhan sen johtokunnan puheenjohtajana suomalainen Kristiina Pietikäinen.

Olen hyvin iloinen, että seuraajani Viviane Reding on esittänyt jatko-ohjelman i2010, jossa on edelleen turvallisuudella keskeinen merkitys. Ohjelma nostaa merkittävinä haasteina esiin yhteentoimivuuden, turvallisuuden ja luotettavuuden, identiteetin hallinnan, oikeuksien hallinnan ja helppokäyttöisyyden.

Tietoturvallisuuskeskustelu on siirtymässä teknisestä turvallisuudesta yleisen luottamuksen saavuttamiseen digitaalisessa maailmassa. Eurooppalaisen tietoyhteiskunnan haasteissa vuoden 2005 jälkeen nostetaan esiin **luottamus ja luotettavuus**: tietoverkkojen on oltava sekä turvallisia että luotettavia.

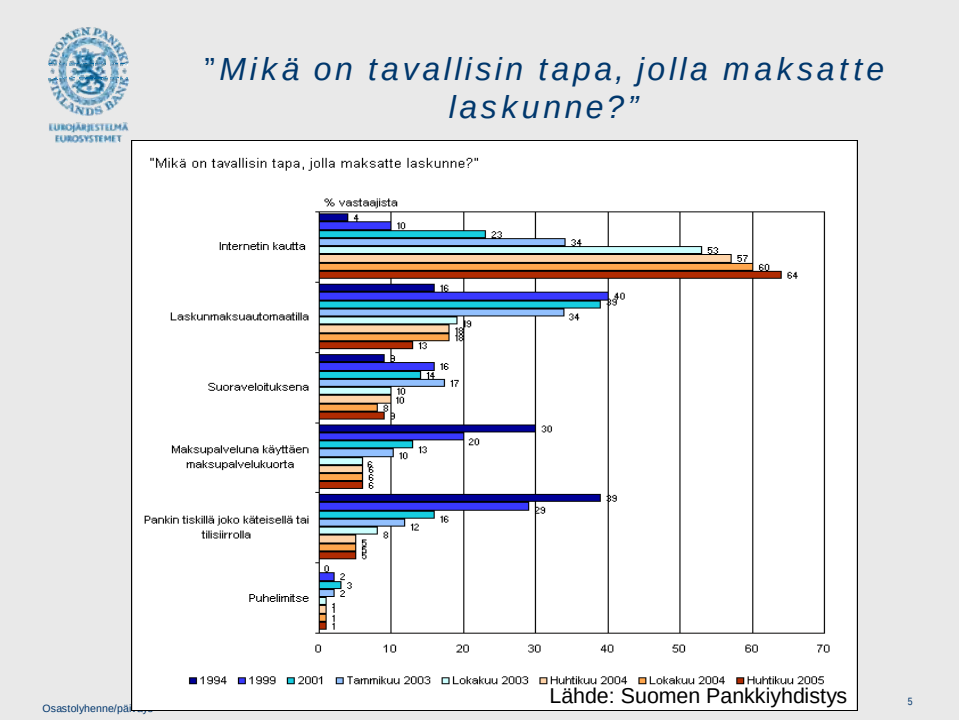
Kuluttajat edellyttävät yksityisyyden suojan turvaamista sekä laittomien kaupankäynti-tapojen ja laittoman sisällön torjuntaa.

Ja nykyelämän infrastruktuurit rakentuvat suuressa määrin tieto- ja viestintäteknologian varaan ja ovat riippuvaisia toisistaan, joten toimintahäiriöillä voi olla vakavia seurauksia.

Eurooppalainen kehitys on tuonut mukanaan myös tietoturvatekijöitä, joiden vaikutus aiheuttaa ristiriitaa. Keskustelu sähköisen viestinnän tunnistamistietojen tallentamis-velvoitteesta on varmasti tuttu myös tälle yleisölle. Velvoitteen taustalla on terrorismin torjunta. Käytännössähän tämä tarkoittaa sitä, että teleoperaattoreiden on tallennettava puheluihin ja sähköpostiviestintään liittyvät tiedot määräajaksi (6-24kk). Tämä on koettu uhaksi yksityisyydelle samalla, kun se aiheuttaa merkittävät kustannukset operaattoreille. Aiheeseen liittyen on käynnistetty Suomessakin selvitys kustannusjaosta.

Suomi on ollut aktiivisessa roolissa tietoturvallisuusasioissa. Vuonna 2003 Valtioeuvosto hyväksyi kansallinen tietoturvallisuusstrategian, joka on saanut huomiota. Parasta aikaa on käynnissä vastaavan eurooppalaisen strategian laatimistyö, jossa Suomi on ollut aloit-teellinen. Tulevalla EU-puheenjohtajuus kaudella tietoturvallisuusasioihin kiinnitetään erityishuomioita.

Kuva 3:"Mikä on tavallisin tapa, jolla maksatte laskunne?"



Pankkijärjestelmä on verkkopalvelujen aktiivisimpia käyttäjiä. Näin verkkomaailman mahdollisuudet ja uhkat ovat pankkimaailmassa läsnä joka päivä.

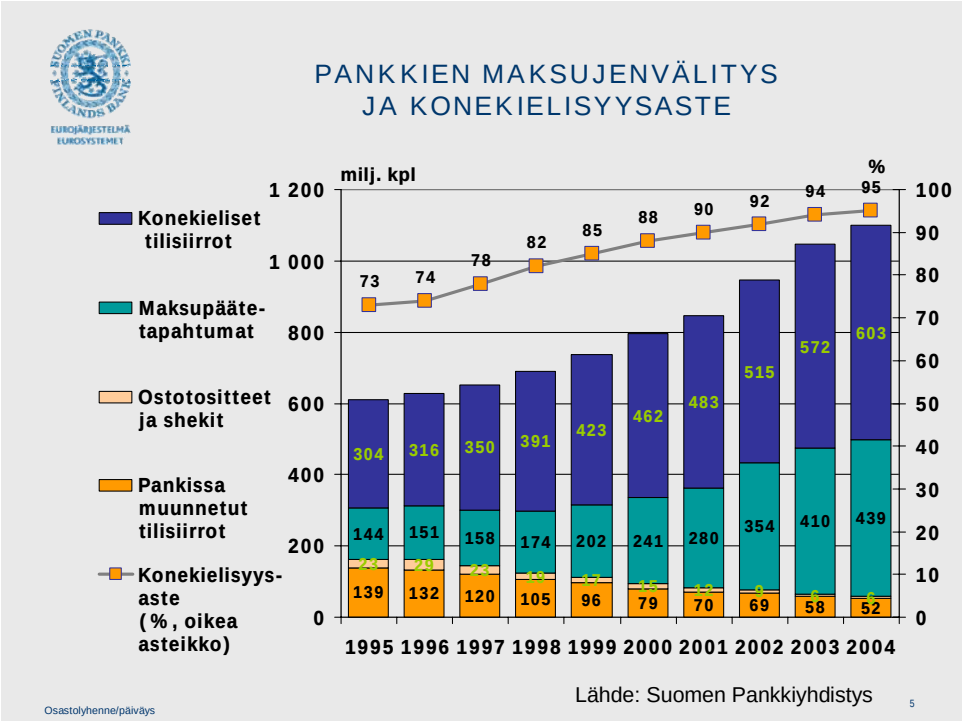
Suomalaiset taas ovat maailmanlaajuisestikin kärkijoukossa sähköisten pankkipalvelui-den ja korttimaksamisen alueilla. Kuvassa esitetty kyselytutkimukseen perustuva vertailu

osoittaa, että 64 % vastaajista on ilmoittanut Internetin tavallisimmaksi laskujen maksamistavaksi.

Mainitsin edellä identiteettivarkaudet vakavana haasteena verkko- ja tietoturvallisuudelle. Pankit ovat tämän ongelman ytimessä. Phising eli tietojenkalastelu liittyy identiteettivarkauksiin. Saimme viime joulukuussa nähdä, miten yhden pankin asiakkailta yritettiin kerätä tunnistautumistietoja väärennetyllä sähköpostiviestillä.

Korttimaksamisen alueella on luotettava tunnistaminen etenemässä keskeisten luottokorttiyhtiöiden (Eurocard, Mastercard, Visa = EMV) standardoiman sirukorttitekniikkaan perustuvan EMV-järjestelmän myötä. EMV:n käyttöönotto vaikuttaa sekä kortteihin, maksupäätteisiin, pankkiautomaatteihin että taustajärjestelmiin. EMV:n tavoitteena on korttiväärennösten estäminen, väärinkäytösten vähentäminen, maksutapahtuman nopeuttaminen ja kansainvälisen yhteiskäytön turvaaminen.

Kuva 4: Pankkien maksujenvälitys ja konekielisyysaste

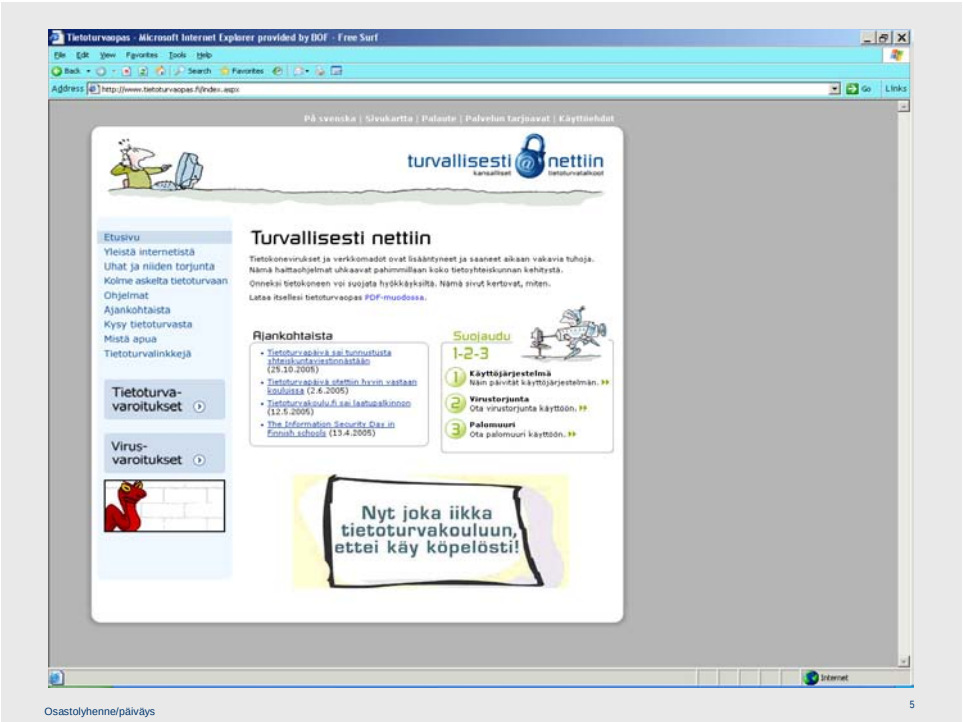


Rahoitustoimiala on hyvä esimerkki alueesta, jolla tieto- ja viestintätekniikka on mahdollistanut ja mahdollistaa edelleen uudentyyppisten palveluiden, jakelukanavien, toimintamallien ja jopa pankkien syntymisen. Kuvassa on esitetty maksujenvälityksen kehittymistä 1990-luvun puolivälistä eteenpäin ja voimme havaita, että konekielisyysaste lähestyy 100 %:a.

Rahoitustoimiala on mitä suurimmassa määrin riippuvainen toimivista tietojärjestelmistä ja -verkoista. Alan kriisiharjoituksissa on havaittu, että palveluiden tuottaminen manuaalisin järjestelyin on hyvin rajoitettua. Ajantasaiset tilitiedot ja toimiva maksunvälitys ovat edellytyksiä pankkipalveluiden tuottamiselle.

Uhkatekijöinä korostuvat tietojärjestelmiin ja sähkön saatavuuteen kohdistuvat häiriöt. Viime aikoina tapahtuneet luonnonkatastrofit ovat nostaneet yhteiskunnan kriittisen infrastruktuurin varmistamisen keskeiseksi turvallisuusasiaksi. Osana tätä työtä on varmistaa myös rahoitusmarkkinoiden toimivuus. Näköpiirissä on ratkaisuja, joissa järjestelmät konsolidoituvat aiempaa tehokkaammiksi kokonaisuuksiksi. Monesti uusiin palveluihin liittyy epäilyksiä niiden luotettavuudesta ja turvallisuudesta. Kehitettäessä uusia ratkaisuja, turvallisuus on keskeinen mahdollistaja.

Kuva 6: Kansallinen tietoturvapäivä



Tänään 7.2.2006 vietetään kolmatta kansallista tietoturvapäivää. Digitaalinen maailma ja tietoverkot ovat tulleet merkittäväksi osaksi sekä työtä että vapaa-aikaa. Se on helpottanut elämää.

Olemme kuitenkin saaneet lukea maailmanlopun ennustajien - niitä on teknologian piirissä kuten muuallakin - varoittelua siitä, että internet on tulossa tiensä loppuun ja digitaalinen maailma on romahtamispisteessä. Näin ei ole.

Mutta suotuisa kehitys edellyttää tietoturvallisuuden tiedostamista myös yksilötasolla. Liikkuvat työpisteet, kommunikaattorit ja muut kämmentietokoneet ovat irrottaneet meidät tietotekniikka-ammattilaisten jatkuvasta ohjauksesta. Kotikoneiden osalta huomaamme usein olevamme "omillamme".

Siksi on muistettava, että myös käyttäjällä on oma vastuunsa. On tärkeä tuntea tietoturvallisuuden aakkoset. Omalla käyttäytymisellä voi riskejä merkittävästi vähentää. Riskien maailmassa ei pidä mennä paniikkiin, vaan pysyä valppaana.