Liikenne- ja viestintäministeriö

LUONNOSVERSIO 9.12.2016

Suomen tietoturvallisuus-strategia

maailman luotetuinta digitaalista liiketoimintaa

Julkaisuja X/2016

LUONNOSVERSIO 9.12.2016

Liikenne- ja viestintäministeriön

visio
Hyvinvointia ja kilpailukykyä hyvillä yhteyksillä

toiminta-ajatus
Liikenne- ja viestintäministeriö edistää väestön hyvinvointia ja elinkeinoelämän kilpailukykyä. Huolehdimme toimivista, turvallisista ja edullisista yhteyksistä.

arvot
Rohkeus
Oikeudenmukaisuus
Yhteistyö

Liikenne- ja viestintäministeriö

Julkaisun päivämäärä x.x.2016 **LUONNOSVERSIO 9.12.2016**	
Julkaisun nimi **Suomen tietoturvallisuusstrategia – maailman luotetuinta digitaalista liiketoimintaa**	
Tekijät Liikenne- ja viestintäministeriö	
Toimeksiantaja ja asettamispäivämäärä Valtioneuvoston toimintasuunnitelma strategisten kärkihankkeiden ja reformien toimeenpanemiseksi 28.9.2015	
Julkaisusarjan nimi ja numero **Liikenne- ja viestintäministeriön julkaisuja xx/2016**	ISSN (verkkojulkaisu) 1795-4045 ISBN (verkkojulkaisu) URN HARE-numero
Asiasanat Digitalisaatio, digitaalinen liiketoiminta, tietoturvallisuus, tietosuoja, tieto- ja viestintäjärjestelmät, riskienhallinta, yksityisyyden suoja, viestinnän luottamuksellisuus,	
Yhteyshenkilö Olli-Pekka Rantala, Timo Kievari	
Muut tiedot Strategian valmistelua tukemaan asetettiin 28.9.2015 tietoturvallisen liiketoiminnan kehittämisrhmä. Ryhmä kokoontui 5 kertaa ja järjesti kuulemistilaisuuden strategian luonnoksesta.	

Tiivistelmä

Suomella on hyvät edellytykset tulla tunnetuksi osaavana, menestyvänä ja luotettavana maana, jossa on turvallista tarttua digitalisaation mukanaan tuomiin mahdollisuuksiin. Digitaalisen tiedon hyödyntämiseen perustuvia palveluita kehittämällä ja tarjoamalla voidaan luoda ja kiihdyttää talouskasvua. Menestymisemme on riippuvaista siitä, että kehitämme, omaksumme ja kokeilemme uudenlaisia liiketoiminnan ja ansainnan malleja. Tämä edellyttää, että uusiin palveluihin, liiketoimintamalleihin ja markkinatoimijoihin voidaan luottaa.

Vahva ote tietoturvallisuuden osaamisen ja markkinoiden kehittämisestä parantaa mahdollisuuksiamme vaikuttaa rooliimme ja asemaamme nopeasti muuttuvassa maailmanjärjestyksessä. Tämän digitaalisen itsenäisyyden turvaaminen on välttämätöntä, jotta Suomesta on edellytyksiä ponnistaa kansainvälisille markkinoille ja jotta Suomi voisi toimia turvallisen ja luotettavan kyberympäristön sillanrakentajana.

Kansallisen tietoturvastrategian visiona on se, että maailman luotetuin digitalinen liiketoiminta tulee Suomesta. Strategian tavoitteina on, että: 1) lainsäädännöstä aiheutuu Suomessa harjoitettavaan digitaaliseen liiketoimintaan mahdollisimman pieni maariski; 2) EU:n sisämarkkina toimii luotettavasti; 3) kansainvälisissä standardeissa arvostetaan suomalaista laatua ja markkinoilla on saatavilla digitaalisia hyödykkeitä, joiden tietoturva on sisäänrakennettua; 4) tietoturvaa ja siihen liittyvää osaamista tutkitaan, mitataan, seurataan ja kehitetään; 5) viranomaiset auttavat yhteisöjä tietoturvan parantamisessa ja pidättäytyvät rajoittamasta epäsuhtaisesti kansalaisten ja yritysten tietoturvaa tai yksityisyyttä.

Tavoitteiden toteutumista tukevat keskeiset toimenpiteet on kuvattu strategiassa. Lisäksi tavoitteiden ja toimenpiteiden tarve on perusteltu strategian perusteluosassa.

Kommunikations-
ministeriet

	Publikationsdatum **UTKAST VERSION 9.12.2015**
Publikation	
Författare	
Tillsatt av och datum	
Publikationsseriens namn och nummer **Kommunikationsministeriets publikationer xx/2014**	ISSN (webbpublikation) 1795-4045 ISBN (webbpublikation) URN HARE-nummer
Ämnesord	
Kontaktperson	Rapportens språk
Övriga uppgifter	
Sammandrag	

Ministry of Transport and Communications

	Date **DRAFT VERSION December 9th 2015**
Title of publication	
Author(s)	
Commissioned by, date	
Publication series and number **Publications of the Ministry of Transport and Communications xx/2014**	ISSN (online) 1795-4045 ISBN (online) URN Reference number
Keywords	
Contact person	Language of the report
Other information	
Abstract	

LUONNOSVERSIO 9.12.2015

Sisällysluettelo

1. JOHDANTO

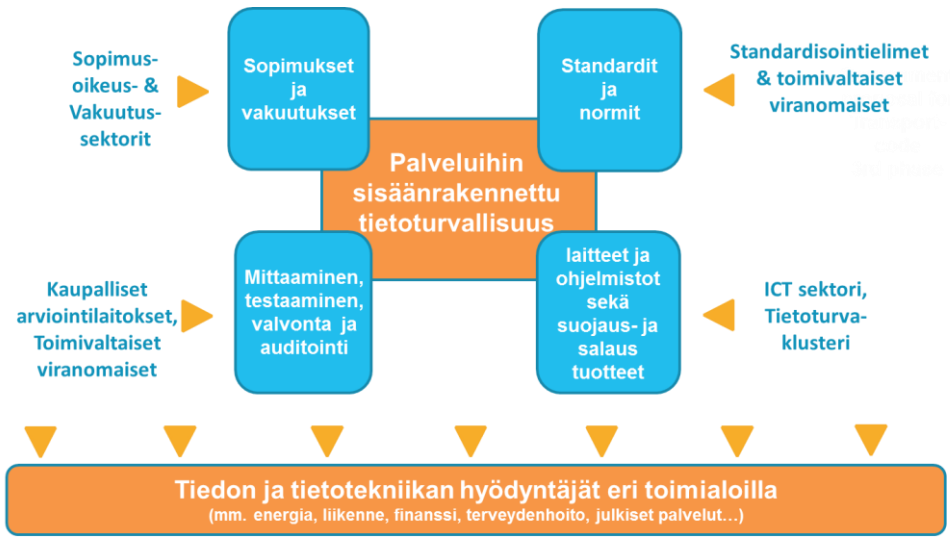
Pääministeri Juha Sipilän hallituksen kärkihankkeena Suomeen rakennetaan digitaalisen liiketoiminnan kasvuympäristö. Yhtenä kärkihankkeen keskeisenä toimenpiteenä valmistellaan ja toimeenpannaan luottamusta internetiin sekä digitaalisiin toimintatapoihin lisäävä kansallinen tietoturvastrategia.

Kärkihankkeiden toimeenpanosuunnitelmassa on kirjattu keskeiset tavoitteet ja lähtökohdat strategiatyölle. Kansallinen tietoturvastrategia painottuu kilpailukyvyn ja vientiedellytysten varmistamiseen, EU:n digitaalisten sisämarkkinoiden kehittämiseen sekä yksityisyyden suojan ja muiden perusoikeuksien turvaamiseen. Strategia tähtää muutokseen, jonka tuloksena tietoturva on sisäänrakennettu erilaisiin järjestelmiin, päätelaitteisiin ja palveluihin. Strategialla puututaan luottamusta heikentäviin ilmiöihin, kuten tietoturvaloukkauksiin ja laajamittaisiin yksityisyyden suojan loukkauksiin verkoissa.

Strategian osana toteutetaan parhaillaan neuvoteltavan EU:n verkko- ja tietoturvadirektiivin edellyttämät lainsäädäntömuutokset. Samalla arvioidaan kansallisen sääntelyn vaikutukset kansalaisten ja yritysten mahdollisuuksiin hyödyntää tietotekniikan mahdollistamia palveluja sekä liiketoimintamalleja turvallisesti ja tiedonkäsittelyyn liittyvät riskit halliten.

Strategialla pyritään lisäämään kaupallisten tiedon salaus- ja suojausmenetelmien tarjontaa ja käyttöä sisämarkkinoilla. Strategian toimeenpanolla kehitetään myös päätelaitteiden, käyttöjärjestelmien, selainten, hakukoneiden, viestintäsovellusten, pilvipalveluiden ja muiden keskeisten tieto- ja viestintäteknisten hyödykkeiden tietoturvaominaisuuksia. Strategisin toimenpitein parannetaan myös digitaalisten hyödykkeiden tietoturvaominaisuuksien yhteentoimivuutta, läpinäkyvyyttä sekä todennettavuutta. Samalla vahvistetaan kyvykkyyttä havaita ja selvittää tietoturvapoikkeamia sekä arvioidaan, millä keinoilla Suomeen saataisiin parhaiten ankkuroitumaan yritystemme kannalta kriittistä tietoturvaosaamista sekä tietoturvapalveluita tarjoavia yrityksiä.

EU:n verkko- ja tietoturvadirektiiviehdotuksen mukaisesti kunkin jäsenvaltion tulee laatia kansallinen strategia, jossa määritellään puitteet, visio, tavoitteet ja painopisteet verkko- ja tietoturvallisuudesta kansallisella tasolla. Parhaillaan loppusuoralla neuvoteltavan direktiiviehdotuksen vaatimukset huomioidaan strategiassa ja sen toimeenpanossa.



2. STRATEGIAN VISIO

Suomella on hyvät edellytykset tulla tunnetuksi osaavana, menestyvänä ja luotettavana maana, jossa on turvallista tarttua digitalisaation mukanaan tuomiin mahdollisuuksiin. Digitaalisen tiedon hyödyntämiseen perustuvia palveluita kehittämällä ja tarjoamalla voidaan luoda ja kiihdyttää talouskasvua. Menestyksemme on riippuvaista siitä, että kehitämme, omaksumme ja kokeilemme uudenlaisia liiketoiminnan ja ansainnan malleja. Valmius luopua vanhoista tehottomista rakenteista ja uskallus omaksua uusia toiminnan tapoja on merkittävällä tavalla riippuvaista siitä, että uusiin palveluihin, liiketoimintamalleihin ja markkinatoimijoihin voidaan luottaa.

Vahva ote tietoturvallisuuden osaamisen ja markkinoiden kehittämisestä parantaa mahdollisuuksiamme vaikuttaa rooliimme ja asemaamme nopeasti muuttuvassa maailmanjärjestyksessä. Tämän digitaalisen itsenäisyyden turvaaminen on välttämätöntä, jotta Suomesta on edellytyksiä ponnistaa kansainvälisille markkinoille ja jotta Suomi voisi toimia turvallisen ja luotettavan kyberympäristön sillanrakentajana.

Kansallisen tietoturvastrategian visiona on se, että:

> ***”Maailman luotetuin digitaalinen liiketoiminta tulee Suomesta.”***

3. STRATEGIAN TAVOITTEET JA NIITÄ EDISTÄVÄT TOIMENPITEET

Strategian visiossa kuvattu tavoitetila voidaan saavuttaa parantamalla tietoturvallisuutta ja siitä riippuvaisen liiketoiminnan luotettavuutta johdonmukaisesti useilla erilaisilla keinoilla. Tietoturvallisuutta ja digitaalisten toimintamallien luotettavuutta voidaan edistää erityisesti lainsäädännön, sopimusten, teknologian ja liiketoimintamallien tasoilla tehtävillä ratkaisuilla.

Strategian tavoitteina on, että:

1) lainsäädännöstä aiheutuu Suomessa harjoitettavaan digitaaliseen liiketoimintaan mahdollisimman pieni maariski;

2) EU:n digitaalinen sisämarkkina toimii luotettavammin;

3) Suomalaiset yritykset hyötyvät kansainvälisistä standardeista ja markkinoilla on saatavilla digitaalisia hyödykkeitä, joiden tietoturva on sisäänrakennettua;

4) tietoturvaa ja siihen liittyvää osaamista tutkitaan, mitataan, seurataan ja kehitetään;

5) viranomaiset auttavat yhteisöjä tietoturvan parantamisessa ja pidättäytyvät rajoittamasta epäsuhtaisesti kansalaisten ja yritysten tietoturvaa tai yksityisyyttä.

Jokainen tavoite ja sen täyttymistä tukevat keskeiset toimenpiteet on selostettu tarkemmin jäljempänä olevissa luvuissa. Strategisten tavoitteiden ja toimenpiteiden tarvetta on perusteltu strategian liitteenä olevassa perusteluosassa.

3.1 Lainsäädännöstä aiheutuu Suomessa harjoitettavaan digitaaliseen liiketoimintaan mahdollisimman pieni maariski

Lainsäädäntö luo edellytykset siihen, että Suomessa harjoitettavaan liiketoimintaan kohdistuu mahdollisimman pieni maariski. Suomi on houkutteleva kohde datan käsittelyyn ja hyödyntämiseen perustuville investoinneille. Suomi erottuu edukseen luotettavana sijoittautumispaikkana digitaalisuutta hyödyntäville yrittäjille.

TOIMENPITEET:

- Tiedon käsittelyyn ja tietoturvaan liittyvän lainsäädännön valmistelun ja säädösten sujuvoittamisen yhteydessä arvioidaan erityisesti säädösten vaikutukset liiketoiminnan harjoittamiselle Suomessa
- Verkko- ja tietoturvadirektiivin voimaansaattamisen yhteydessä turvataan yritysten mahdollisuudet sovittaa tietoturvariskien hallintaan liittyvät uudet velvoitteet osaksi muiden liiketoiminnan riskiensä hallintaa
- Maariskit pyritään minimoimaan valmisteltaessa EU:n tietosuoja-asetuksen edellyttämiä muutoksia kansallisen sääntelyn
- Huolehditaan, että viestinnän välittäjän vastuuta koskevaa sääntelyä kehitetään EU:ssa teknologia- ja toimijaneutraalisti (vastuu yksityisyyden suojasta ja tietoturvasta viestejä välitettäessä)
- Kyberturvallisuuden kehittämistyössä ja viranomaisten tiedonhankintavaltuuksia uudistettaessa turvataan kaikin keinoin käyttäjien oikeuksien, kuten yksityisyyden suojan ja luottamuksellisen viestin suojan säilyminen sähköisissä palveluissa ja verkkoympäristössä
- Selvitetään kysyntää sellaisille tietoturvapalveluille, joiden tarjonnassa tai käytössä voidaan soveltaa yksinomaan Suomen tai EU:n lainsäädäntöä. Arvioidaan miten tällaista palveluntarjontaa on tarvittaessa mahdollista ankkuroida Suomeen, esimerkiksi valtionomistuksen keinoin

3.2 EU:n digitaalinen sisämarkkina toimii luotettavammin

Suomi pyrkii pienentämään maariskejä EU:n sisällä ja kansainvälisessä yhteisössä, jotta tiedon vapaa liikkuvuus voitaisiin turvata kansalaisten perusoikeuksia ja yritysten oikeushyviä vaarantamatta. Suomi tavoittelee EU:ssa ja kansainvälisessä yhteistyössä yhteisen lähestymistavan löytämistä sille, missä tarkoituksessa ja missä laajuudessa valtio voi rajoittaa toisessa valtiossa olevan henkilön yksityisyyttä tai tietoturvaa. Suomi huomioi kansainvälisiä sopimuksia laatiessaan erityisesti sopimusten vaikutukset tietoturvahyödykkeitä tuottaville ja niitä hyödyntäville suomalaisille yrityksille.

TOIMENPITEET:

- Suomi huomioi tietoturvastrategian tavoitteet Euroopan komission digitaalisten sisämarkkinoiden strategian sekä EU:n kyberturvallisuusstrategian toimeenpanossa
- Suomi vaikuttaa aktiivisesti tietoturvastrategian tavoitteiden huomioimiseksi Euroopan Unionin verkko- ja tietoturvaviraston (ENISA) toiminnassa
- Suomi huomioi tietoturvastrategian tavoitteet OECD:n ministerikokouksessa Cancunissa 2016 annettavan julistuksen valmistelussa
- Tietoturvastrategian tavoitteet huomioidaan kyberturvallisuuden ulkopoliittisia ulottuvuuksia yhteen sovittavassa työssä sekä laadittaessa Suomea sitovia kansainvälisiä sopimuksia
- Suomen vaikuttaa aktiivisesti tietoturvastrategian tavoitteiden huomioimiseksi EU:n komissioon kauppaneuvotteluissa sekä ns. Safe Harbour-päätöstä mahdollisesti uudistettaessa

3.3 Suomalaiset yritykset hyötyvät kansainvälisistä standardeista ja markkinoilla on saatavilla digitaalisia hyödykkeitä, joiden tietoturva on sisäänrakennettua

Suomessa kehitetään, tarjotaan ja käytetään tavaroita sekä palveluita, joihin on sisäänrakennettu tietoturvaa parantavia ominaisuuksia. Suomessa on tarjolla päätelaitteita, käyttöjärjestelmiä, selaimia, hakukoneita, viestintäsovelluksia, pilvipalveluita ja muita keskeisiä digitaalisia hyödykkeitä, joiden tietoturvaominaisuudet ovat niin yhteismitallisia, että niiden läpinäkyvyyttä, tehokkuutta ja todennettavuutta on helppo arvioida. Suomessa on tarjolla maailman edistyksellisimmät kaupalliset palvelut, joiden avulla yritykset voivat mitata ja pienentää (ml. vakuuttaa) liiketoiminnalleen taloudellista vahinkoa aiheuttavia tietoturvariskejä. Suomessa ja EU:ssa on käytössä standardeja ja merkintöjä, jotka helpottavat tietoturvan näkökulmasta luotettavan sopimuskumppanin valintaa.

TOIMENPITEET:

- Parannetaan luottamusta sähköisiin transaktioihin käynnistämällä sähköisen tunnistamisen kansallinen luottamusverkosto, jossa eri toimijat voivat luottaa toistensa välittämiin tunnistamistietoihin
- Kehitetään julkisen ja yksityisen sektorin yhteistyössä edellytyksiä henkilötietojen anonymisoinnin mahdollistaville palveluille, jotta palveluntarjoajat voisivat pienentää henkilötietojen käsittelyyn liittyviä tietoturvariskejään
- Selvitetään miten yleisimpien päätelaitteiden, käyttöjärjestelmien, internet-selainten, hakukoneiden ja viestintäsovellusten käyttöehdot sekä tiedonsuojausominaisuudet vaikuttavat käyttäjän mahdollisuuksiin suojata tietojaan omassa liiketoiminnassaan tai muussa toiminnassaan
- Selvitetään erilaisten tiedonsuojausominaisuuksien ja sertifiointien merkitys käyttäjien tarpeisiin ja heidän digitaalisia hyödykkeitä kohtaan kokemaan luottamukseen. Selvitetään luotettujen hyödykkeiden taustalla vaikuttavien sertifiointi- ja standardointielimien merkitys ICT-alan laite- ja palveluntuottajille sekä niiden asiakkaille
- Selvitetään, mitkä ovat sellaisia tietoturvahyödykkeitä, joita käytetään laajasti eri toimialoilla Suomessa toimivissa yrityksissä. Selvitetään myös, miten tällaista palveluntarjontaa ja avainosaamista on tarvittaessa mahdollista ankkuroida Suomeen esimerkiksi valtionomistuksen keinoin

3.4 Tietoturvaa ja siihen liittyvää osaamista tutkiaan, mitataan, seurataan ja kehitetään

Suomessa tutkitaan ja seurataan tietoturvariskien hallinnasta yrityksille aiheutuvia kustannusvaikutuksia. Suomessa tutkitaan ja seurataan T&K-investointeja, joita yritykset käyttävät tuottamiensa hyödykkeiden tietoturvallisuuden parantamiseen. Suomessa selvitetään mahdollisuuksia sisällyttää data-analyysin ja kryptologian perusvalmiuksia kehittävää opetusta ja tutkimusta eri oppi- ja tutkimuslaitosten opetusohjelmiin sekä muihin tutkimusohjelmiin.

TOIMENPITEET:

- Muodostetaan tilannekuva tietoturvariskien aiheuttamien vahinkojen ja niiden ennaltaehkäisyn kustannusvaikutuksista - ml. tieto- ja viestintärikosten aiheuttamat taloudelliset vahingot
- Kartoitetaan suomalaisia tietoturvahankkeita, joita Euroopan Komissio voisi rahoittaa osana vuonna 2016 perustettavaa kybertutkimusohjelmaansa[1]
- Etsitään valtioneuvoston päätöksentekoa tukevan tutkimus- ja kehitystoiminnan osana keinoja parantaa digitaalisten palvelujen ja liiketoimintamallien luotettavuutta[2]
- Seurataan tietoturvatuotteiden osuutta ja kehitystä ICT -toimialan liikevaihdosta
- Kartoitetaan Suomessa toimivien yritysten tarpeet tietoturva- ja tietosuojaosaajille. Selvitetään keinoja osaajien saatavuuden parantamiseksi

[1] Komission ohjelma eurooppalaisten tietoturvallisten tuotteiden saatavuuden parantamiseksi julkisen ja yksityisen sektorin välisenä yhteistyönä. Ohjelmaluonnos tulossa lausuntokierrokselle vielä vuoden 2015 aikana.

[2] Valtioneuvosto hyväksyi 3.12.2015 valtioneuvoston päätöksentekoa tukevan selvitys- ja tutkimussuunnitelman, jonka yhtenä hankkeen tuloksena selvitetään, miten voidaan parantaa digitaalisten hyödykkeiden ja liiketoimintamallien luotettavuutta?

3.5 Viranomaiset auttavat tietoturvan parantamisessa ja pidättäytyvät rajoittamasta epäsuhtaisesti kansalaisten ja yritysten tietoturvaa tai yksityisyyttä

Viranomaiset auttavat ja tukevat yrityksiä huolehtimaan tietoturvasta liiketoiminnassaan mm. keräämällä ja jakamalla tietoa tietoturvariskien hallinnasta. Yrityksillä on hyvät mahdollisuudet osallistua luotettavuutta parantavien hyödykkeiden sekä ominaisuuksien standardointiin viranomaisten ja järjestöjen tukemana.

TOIMENPITEET:

- Kartoitetaan, millaisia kaupallisia ja julkisia palveluita tietojärjestelmien ylläpitäjillä sekä käyttäjillä on piilevien tietoturvariskien havainnoimiseksi, niiden haitallisten vaikutusten arvioimiseksi sekä riskin pienentämiseksi tietoa jakamalla
- Ylläpidetään tietoturvallisuuden tilannekuvaa Viestintäviraston, yritysten ja muiden yhteisöjen luottamukseen perustuvan tiedonvaihdon avulla
- Edistetään asianomistajien mahdollisuuksia saattaa tieto- ja viestintärikokset tehokkaasti esitutkintaan ja tuomioistuinprosessiin
- Toimivaltaiset viranomaiset tukevat ennakoivalla tulkintakäytännöllään uusien tiedon käsittelyyn perustuvien ja luotettavuutta parantavien liiketoimintamallien syntymistä
- Muodostetaan kansallinen verkosto, joka edesauttaa suomalaisia yrityksiä osallistumaan standardointityöhön viestinnän luottamuksellisuutta parantavien tietoturvallisten palveluiden ja laitteiden kaupallisen saatavuuden, käytön ja viennin edistämiseksi

4. STRATEGIAN PERUSTELUOSA

4.1 Tilannekuva

Liiketoiminnan arvo kasvaa teknologiaa hyödyntämällä

Tieto- ja viestintäteknologia sekä niihin liittyvät palvelut muuttavat yhteiskunnan toimintaa sekä valtarakenteita mullistavalla tavalla. Tästä murroksessa parhaiten menestyvät ne, jotka kykenevät tarjoamaan asiakkaiden tarpeiden mukaisia korkealaatuisia ja luotettavia tietotekniikkaa hyödyntäviä tavaroita ja palveluita mahdollisimman kannattavasti. Suomella on erinomaiset edellytykset nousta takaisin digitalisaatiokilvan kärkisijoille ja profiloitua erityisen luotettavan digitaalisen liiketoiminnan kasvuympäristönä.

Tieto- ja viestintäteknologia-ala muodostaa merkittävän osan Suomen bruttokansantuotteesta. Toimialan yritysten liikevaihto vuonna 2013 oli 43,4 MRD € (josta teleyritykset 4,5 MRD €, ohjelmistot, konsultointi ja tietopalvelut 7,9 MRD € sekä tietokoneiden ja sähkölaitteiden valmistus 31 MRD €)[3]. Toimiala on merkittävällä tavalla vientipainotteinen sillä Suomen loppukäyttäjäkulutusta kuvaavan IT-markkinan liikevaihto oli vuonna 2014 yhteensä 6 MRD € (josta laitteet 1,5 MRD €, ohjelmistot 1,3 MRD € ja IT-palvelut 3,2 MRD €)[4]. Suomen bruttokansantuote vuonna 2012 oli noin 200 MRD € ja ns. Internet-talouden osuuden on arvioitu muodostavan siitä noin 10 %[5]. Vaikka valtiolla ja kunnilla on merkittävä osuus Suomen IT-markkinan ostovoimasta, on julkisen hallinnon ostovoiman merkitys verrattain pieni suhteessa toimialan kansantaloudelliseen arvoon, joka nojaa pitkälti kansainväliseen vientiin.

Digitalisaatiolla tarkoitetaan tässä yhteydessä muutosta, jossa tieto- ja viestintäteknologiaa sekä siihen perustuvia palveluita hyödyntämällä pyritään muodostamaan aiempaa suurempi osuus liiketoiminnan tai julkisten palveluiden arvosta. Digitalisaatio voi siis toimia taloudellisen toimeliaisuuden katalyyttinä. Toisin sanoen, digitalisaatio voi kiihdyttää arvonlisän muodostamista yrityksissä ja julkishallinnossa. Suomessa onkin arvioitu voitavan saavuttaa 56 MRD €:n verran uutta liikevaihtoa sekä 48.000 uutta työpaikkaa, jos "suomalaiset yritykset ottavat roolin teollisen internetin alustojen ja ekosysteemien avaintoimijoina"[6].

Kansainvälisillä markkinoilla on keskeinen merkitys Suomessa harjoitettavalle liiketoiminnalle

Viestintäpalveluiden markkinoiden kehittyminen on johtanut internetin eksponentiaaliseen kasvuun. Internet kaksinkertaistuu alle kahden vuoden välein käyttäjämäärällä ja välitetyn datan määrällä mitattuna[7]. Laajeneminen on mahdollistanut yrityksille sellaisen liiketaloudellisen arvon muodostumisen, joka ei ole riippuvaista ajasta, alueesta ja aineesta. Sekä teknologian kehitys että internetin luonne eräänlaisena "rajattomana" tuotannontekijänä ovat avanneet myös Suomessa toimiville yrityksille mahdollisuuksia osallistua maailman markkinoille ja skaalata liiketoimintaansa uusille markkina-alueille erittäin nopeasti ja verrattain pienin muuttuvin kustannuksin. Näitä mahdollisuuksia ei ole kuitenkaan hyödynnetty täysimääräisesti.

---

[3] Tilastokeskus sekä Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, 2013.
[4] Teknologiateollisuus ry, Market Visio.
[5] Tilastokeskus ja Elinkeinoelämän tutkimuslaitos, 2012.
[6] Valtioneuvoston kanslian selvitys- ja tutkimushanke, jonka tekijöinä mm. Elinkeinoelämän tutkimuslaitos, Aalto-yliopisto, Valtion Teknillinen tutkimuslaitos, 2015.
[7] OECD, Maailmanpankki ja Kansainvälinen televiestintäliitto ITU.

Suomen kotimarkkinan pienuudesta sekä ICT-alan vientipainotteisuudesta johtuen on tärkeää turvata eurooppalaisen sisämarkkinan toimivuus sekä suomessa toimivien yritysten esteetön pääsy kansainvälisille markkinoille. Samalla on erittäin tärkeää huolehtia siitä, että Suomi on jatkossakin houkutteleva kohde sellaisille sijoituksille, joita liiketoimintaansa digitalisoivat yritykset tekevät arvonmuodostusta kehittääkseen.

EU:ssa on arvioitu, että digitaalisten sisämarkkinoiden täydellisellä toteutumisella voitaisiin saavuttaa 415 MRD €:n kasvu EU:n bruttokansantuotteeseen[8]. Lisäksi on laskettu, että EU:n kansalaisten henkilötiedoilla on vuositasolla yhteensä 315 MRD €:n liiketaloudellinen arvo[9]. Sisämarkkinoiden esteet ilmenevät mm. ylimääräisinä kustannuksina, joita tavaroiden ja palveluiden tarjoaminen toisiin jäsenvaltioihin aiheuttaa. Esimerkiksi rajat ylittävässä kuluttajakaupassa vieraan EU-jäsenvaltion lainsäädännön noudattamisesta aiheutuu yksittäiselle yritykselle keskimäärin 9000 €:n kustannukset per jäsenvaltio[10]. On tärkeää huolehtia siitä, ettei EU:n jäsenvaltioiden kansallisen lainsäädännön erilaisuus muodostu uusien markkinoiden kehityksen esteeksi.

Luottamuspula jarruttaa markkinoiden kehitystä

Globalisaation, digitalisaation ja verkostoitumisen kehitystrendit luovat uusia liiketoimintamahdollisuuksia. Samalla ne kuitenkin aiheuttavat myös monenlaista luottamuspulaa markkinatoimijoiden välille. Luottamuspulaa aiheuttaa tavanomaisten verkkorikosten ohella valtioiden ylimitoitettu verkkovalvonta- ja tiedustelutoiminta. Luottamuksen ansaitseminen on todennäköisesti sitä vaikeampaa, mitä merkittävämmällä tavalla tietotekniikka ottaa ohjat ihmisten arjen palveluissa. Esimerkiksi robottiauton tai täysin automaattisesti ohjautuvan lentokoneen kyytiläisten luottamus on ansaittava, jotta uudet palvelumuodot hyväksyttäisiin asiakkaiden taholta. Vähintäänkin palvelun luotettavuutta on mahdollista hyödyntää kilpailuetuna kilpailijoihin nähden.

Luottamuspulaa kuitenkin ilmenee monin tavoin. Jopa 88 % haastatelluista 28.000 eurooppalaisesta kertoi muuttaneensa tapojaan käyttää internetiä tietoturvahuolien vuoksi. Suomalaisista 59 % arvioi tuntevansa digitaalisiin palveluihin liittyvät riskit hyvin, kun EU:n keskiarvo oli 50 %. Suomalaiset pitävät mahdollisuuksiaan EU:ssa toiseksi parhaina verkkorikollisuudelta suojautumiseen.[11]

Edward Snowdenin paljastuksista kuulleista interentin käyttäjistä 39 % oli ryhtynyt toimiin yksityisyytensä suojaamiseksi[12]. Yhdysvalloissa paljastuneiden vakoiluskandaalien on arvioitu aiheuttaneen jo tähän mennessä noin 40 miljardin dollarin välittömät menetykset maan ICT-teollisuudelle[13]. Pilvipalvelun tarjoajien arvioidaan menettävän pahimmillaan jopa 20 prosenttia Yhdysvaltain ulkopuolisesta liikevaihdostaan PRISM-kohun seurauksena seuraavien kolmen vuoden aikana[14].

Isoimmat teknologiayritykset ovat Snowdenin paljastusten jälkeen alkaneet salata kuluttajapalveluidensa dataa ja tietoliikennettä sekä korostaneet asiakaslupauksissaan tietosuojan korkeaa merkitystä. Yhdysvaltojen 1000 suurimman yrityksen satsaukset

[8] Euroopan Unionin Parlamentti, 2015.
[9] Euroopan Unionin Komissio, Boston Consulting Group, 2013.
[10] Euroopan Unionin Komissio, 2011.
[11] EU komissio, 2015.
[12] OECD, 2014.
[13] Teknologiateollisuus ry & FISC ry, 2014.
[14] The Information Technology & Innovation Foundation, 2013.

tietosuojan parantamiseksi on arvioitu 2,4 MRD $:n suuruisiksi vuosittain. Tietosuoja-asiantuntijoiden kysyntä ja tulot ovat merkittävässä kasvussa.[15]

Tietoturvaloukkausten vaikutuksia uhreiksi joutuneiden yritysten varallisuudelle, maineelle, suhteille, yrityssalaisuuksille ja työntekijöille on vaikea selvittää, mutta ne voivat olla erittäin merkittäviä. Suuryrityksiltä on yksittäisissä tietomurtotapauksissa viety kymmenien miljoonien käyttäjien tietoja. Yksittäiset tapaukset ovat aiheuttaneet yksittäiselle yritykselle satojen miljoonien dollarien vahinkoja[16]. Iso-Britanniassa 81 % suurista organisaatioista oli joutunut vuoden sisällä tietoturvaloukkauksen kohteeksi. Loukkauksista aiheutuneet kustannukset kaksinkertaistuivat vuoden aikana 0,6 – 1,15 M £:n suuruisiksi per organisaatio[17]. Esimerkiksi kahden yhdysvaltalaisen kauppaketjun maksukorttirekisteriin tehty tietomurto on tähän mennessä aiheuttanut yrityksille 252 M $:n vahingot, joista n. 90 M $ on korvattu vakuutuksin. Näiden vahinkojen lisäksi oikeusprosessit ovat yhä kesken n. 200 M $:n arvoisista korvausvaatimuksista[18].

Tietoturvaongelmien aiheuttamilta vahingoilta suojaavien vakuutusten osuus vakuutusmarkkinoista on pieni, mutta se on kasvamassa. Tietoturvavakuutusmaksuja kertyy vuosittain USA:ssa 2,5 MRD $ ja Euroopassa 150 M $.[19]

EU:n tietosuoja-asetuksen velvoitteet voivat aiheuttaa joillekin yrityksille kustannuksia. Lisäksi EU:n Komission verkko- ja tietoturvadirektiiviehdotuksen mukaisesti harmonisoidut tietoturvavaatimukset aiheuttaisivat EU:ssa yrityksille 1-2 MRD:n €:n lisäkustannukset[20]. Suomessa lainsäädäntö turvaa jo nykyisin verrattain korkeatasoisen tietosuojan ja tietoturvan tason. Lainsäädäntömme on muodostanut yritystoiminnalle kilpailuedun mm. niihin valtioihin nähden, joissa viranomaisilla on laajemmat oikeudet puuttua yksityiselämän ja viestinnän luottamuksellisuuden suojaan tietoverkoissa ja tietojärjestelmissä.

Luottamuspulan pienentämiseen pyrkivä liiketoiminta sekä toisaalta julkisen vallan toimintaympäristön kehitystä tukevat toimenpiteet voivat luoda edellytyksiä luotettavasti digitalisoitujen hyödykkeiden uusien markkinoiden kehittymiselle. Tämä strategia keskittyy mainitun liiketoiminnan kehittymistä edistävien keinojen hahmottamiseen. Strategialla luodaan edellytyksiä käyttäjien tarpeiden mukaisten luotettavien ja turvallisten ICT-hyödykkeiden paremmalle saatavuudelle sekä niitä hyödyntävän uudenlaisen liiketoiminnan kehittymiselle. Luottamuspulaan liittyvien esteiden poistaminen markkinoilta parantaa samalla julkishallinnon mahdollisuuksia hankkia digitaalisia palveluita hyödynnettäväksi tehokkaasti ja turvallisesti toiminnassaan.

[15] OECD, 2015.
[16] OECD, 2015.
[17] Iso-Britannian elinkeino-, innovaatio- ja osaamisministeriö, 2015.
[18] OECD, 2015.
[19] OECD, 2015.
[20] EU komissio, 2013.

4.2 Eritasoiset tietoturvariskit

Tietoturvariskejä voidaan jaotella eri tavoin. Tietoturvariskeillä tarkoitetaan tässä strategiassa sellaisia liiketaloudellisia riskejä, jotka liittyvät tietotekniikan suunnittelemiseen, käyttämiseen, omistamiseen tai ylläpitämiseen liiketoiminnassa ja joiden toteutuminen on aina jollakin tavalla seurausta siitä, että:

1) ulkopuolinen taho pääsee oikeudetta käsiksi luottamukselliseen tietoon (luottamuksellisuus)
2) tietosisältö muuttuu ilman sen muuttamiseen oikeutetun tahon tarkoitusta (eheys) tai
3) tietosisältö ei ole siihen oikeutetun tahon saatavissa tai käytettävissä (saatavuus/käytettävyys).

Tietoturvariskit voivat aiheutua hyvin erilaisten syy-yhteyksien seurauksena. Taloudellisen vahinkoon johtavan tietoturvariskin perimmäisenä syynä voi olla esim.:

1) virhe tekniikan suunnittelussa tai toiminnassa;
2) virhe sopimussuhteessa, (esim. epäluotettavan sopimuskumppanin valinta, sopimusehdon epäedullisuus, alihankkijan piilevien riskien tunnistaminen, sopimus ei pidä, vastuu omien asiakkaiden vahingoista jne.);
3) liiketoiminnan harjoittaminen maassa, jossa lainsäädäntö tai muut olosuhteet aiheuttavat liiketoiminnalle maariskin tai
4) liiketoiminnan aineettoman pääoman joutuminen alttiiksi mainehaitalle.

Tietoturvariskin toteutuminen voi olla seurausta:

1) tahattomasta vahingosta
2) tahallisesta oikeudettomasta teosta

Tietoturvariskin aiheuttama taloudellinen vahinko johtua:

1) liiketoiminnan keskeytymisestä,
2) omaisuuden vahingoittumisesta,
3) aineettomien oikeuksien loukkaamisesta tai
4) vahingoilta suojautumiseen käytettävistä kuluista.

Mitä tietosisällölle käy?	**Mikä on tiedon vaarantumisen juurisyy?**	**Onko seurausta vahingosta vai tahallisuudesta?**	**Mistä taloudellinen vahinko aiheutuu (vahinkolaji)?**
Tiedon luottamukselli-suus vaarantuu	suunnitelu- tai ylläpitovirhe		liiketoiminnan keskeytyminen
tiedon eheys vaarantuu	sopimusriski	tahaton vahinko	omaisuuden vahingoittuminen
tiedon käytettävyys vaarantuu	maariski	tahallinen teko	aineettoman oikeuden loukkaus
	maineriski		seuraamusmaksuista tai suojautumiskuluista

Digitaalisten tietokoneohjelmien tietoturvariskien voidaan ajatella saavan usein alkunsa jo ohjelman laatimisen hetkellä eli ohjelmia koodattaessa. Tässä suunnitteluvaiheessa tehdään valinta siitä, millaista ohjelmointikieltä, millaisia ohjelmointikirjastoja, millaisia tietoteknisiä protokollia ja millaisia suojausratkaisuja ohjelmaan sisällytetään. Kaikki nämä valinnat sekä tekijän osaaminen ja huolellisuus vaikuttavat siihen, millaisia tietoturvariskejä ohjelmaan voi myöhemmässä vaiheessa liittyä. Näistä puhutaan usein ohjelmistohaavoittuvuuksina tai ohjelmistovirheinä. Virhe saattaa aiheuttaa ohjelmiston kaatumisen itsestään jossakin tietyssä tilanteessa. Toisaalta virhe voi mahdollistaa ohjelmiston haitallisen väärinkäytön esimerkiksi tietomurroissa tai palvelunestohyökkäyksissä. Ohjelmistovirhe ei välttämättä näy ohjelmiston käyttäjälle millään tavalla mutta siitä johtuva tietoturvariski voi piillä ohjelmistossa ja sen avulla käytettävässä tuotteessa tai palvelussa jopa vuosikausia. Ohjelmointivirheiden hallinnassa korostuu ohjelmiston muutoshallintaan ja päivityksiin liittyvien menettelyiden tehokkuus.

Ohjelmistohaavoittuvuuksia voi torjua pitämällä ohjelmistot ajan tasalla eli tekemällä ohjelmistopäivityksiä. Tässä ylläpitovaiheessa voidaan korjata ohjelmiin suunnitteluvaiheessa syntyneitä, mutta vasta myöhemmin ilmenneitä virheitä. Vastuullisella ohjelmiston laatijalla on intressi kehittää ohjelmistoaan jatkuvasti siten, että ilmenneiden haavoittuvuuksien synnyttämiä tietoturva-aukkoja tilkitään. On kuitenkin mahdollista, että liiketoiminnan kannalta tärkeitäkin prosesseja ohjataan hyvin vanhoilla ohjelmistoilla, joiden laatijaa ja kehittäjää ei enää ole edes olemassa. Tällöin täytyy muilla keinoin (esim. itse) huolehtia ohjelman tietoturvan kehityksestä, tai se voi jäädä kokonaan tekemättä. Keskeistä on se, kuka ensimmäisenä havaitsee johonkin ohjelmaan tai useissa ohjelmissa käytettäviin ohjelmointikieliin (tai kirjastoihin) liittyvän haavoittuvuuden ja mitä hän tekee tällä haavoittuvuustiedolla. Tietoturvan kannalta olisi tärkeää että ohjelman valmistaja saisi nopeasti tiedon haavoittuvuudesta, jotta voisi päivittää ohjelmiston turvallisemmaksi. Toisaalta myös ohjelman käyttäjällä on intressi tietää, mikäli ohjelmaan liittyy tällainen haavoittuvuus, joka mahdollistaa ohjelman oikeudettoman käytön.

Haavoittuvuuksia koskevien tietojen vastuullinen kerääminen ja jakaminen, ns. haavoittuvuuskoordinaatio, on tietoturvan ylläpitämisen kannalta erittäin tärkeää. Lisäksi tietokoneohjelmistoja tuotteisiinsa, palveluihinsa tai tuotantoprosesseihinsa hankkivien yritysten olisi syytä arvioida, miten sopimuksissa määritellään ohjelmiston turvallinen toiminta ja millaisia ominaisuuksia on pidettävä ohjelmiston sopimusoikeudellisena virheenä.

Tietoturva voi vaarantua myös tilanteissa, joissa ohjelmisto sinänsä toimii tekijänsä tarkoittamalla tavalla, mutta esimerkiksi sähkökatko estää palvelimella olevan tiedon saatavuuden. Toisaalta tietoturva voi vaarantua jos henkilö väärinkäyttää pääsyään tietokoneelle esim. kopioidakseen palvelimelta luottamuksellisia tietoja myytäväksi. Riskien moninaisuudesta johtuen on tärkeää, että tietotekniikkaa liiketoiminnassaan hyödyntävällä yrityksellä on kyky arvioida tiedon hyödyntämiseen liittyviä riskejä ja suhteuttaa ne osaksi muuta riskienhallintaansa.

Sopimuskumppanin tietoturvariskien huomioiminen liiketoiminnassa

Digitaalisuutta hyödyntävälle liiketoiminnalle on leimallista se, että tuotteen tai palvelun tuotannossa käytetään lukuisia alihankkijoita. Samalla joudutaan luottamaan sopimuskumppaneina toimivien alihankkijoiden luotettavuuteen tiedonkäsittelijänä. Esimerkiksi tiedonsiirtoyhteydet hankitaan usein yleisiä viestintäpalveluja tarjoavilta teleyrityksiltä tai muilta tietoliikenneyhteyksiä tarjoavilta palveluntarjoajilta. Tällaisten alihankkijoiden tietoturvallisuuden taso voi vaikuttaa keskeisellä tavalla oman toiminnan tietoturvariskeihin.

Toisaalta yritys joutuu luovuttamaan usein omia tietoaineistojaan asiakkailleen ja tällöin yrityksen on voitava luottaa vastaavasti asiakkaansa kykyyn käsitellä tälle luovutettuja tietoja turvallisesti. Tietoaineistojen avaaminen ulkopuolisille ohjelmisto- ja palvelukehittäjille on omiaan avaamaan yrityksille uusia liiketoimintamahdollisuuksia. Samalla tietojen avaamisesta saattaa kuitenkin aiheutua tietoturvariskejä omalle liiketoiminnalle. Yritysten tulisikin voida mahdollisimman kustannustehokkaasti vakuuttua sopimuskumppaneidensa piirissä olevien tietoturvariskien vaikutuksista omalle liiketoiminnalleen.

Sopimusriskejä voidaan pienentää huomioimalla sopimusehdoissa molempien osapuolten edellyttämä riskienhallinnan taso. Sopimuskumppanien keskinäistä luotettavuutta voi lisätä se, että ne toteuttavat yhteismitallisia riskinhallintakeinoja. Tällöin standardoidut ja sertifioidut riskienhallinnan tavat voivat lisätä yritysten välistä luottamusta toisiinsa.

Maariskien ja lainsäädäntöjen kollision vähentäminen

Pilviarkkitehtuurin yleistymisen myötä yhä suurempi osa tavaroista ja palveluista tuotetaan tavalla, jossa digitaalista tietoa käsitellään tuotantoprosessin eri vaiheissa eri valtioissa ja siirretään rajojen yli. Eri maissa sovellettava lainsäädäntö voi muodostaa riskejä tiedon käsittelylle ja uusille liiketoimintamalleille.

Euroopan neuvoston tieto- ja viestintärikosten tunnusmerkistöjä harmonisoivan ns. budapestin sopimuksen voimaansaattaneissa maissa tietyt tietoturvaloukkaukset on säädetty rangaistaviksi teoiksi. Rangaistavuus saattaa useissa maissa koskea kuitenkin yksinomaan "oikeudettomia" tekoja. Tietoturvaloukkauksen aiheuttavan teon rangaistavuudesta huolimatta onkin mahdollista, että jokin valtio oikeuttaa kansallisen viranomaisen tekemään tietoturvaloukkauksen, joka tavalla tai toisella kohdistuu toisessa valtiossa olevaan henkilöön. Teon oikeudettomuuden poistuminen tekomaassa ei poista teon rangaistavuutta sen kohteena olevan uhrin kohdemaassa, johon teolla voidaan niin ikään katsoa olevan rikosoikeudellinen liityntä.

Tämä oikeudellisen kolliission ongelma on käynyt erittäin ilmeiseksi vuonna 2013 paljastuneissa tiedusteluviranomaisten massavalvontamenetelmissä. Useiden keskeisten teknologiayritysten johtajat ovat ilmaisseet huolensa massavalvonnasta ja erityisesti sen vaikutuksista asiakkaidensa luottamukseen[21].

Suomen perustuslain mukaan julkisen vallan on ensinnäkin turvattava perus- ja ihmisoikeuksien toteutuminen pidättäytymällä itse loukkaamasta perusoikeuksia. Sen lisäksi julkisen vallan on aktiivisilla toimenpiteillä edistettävä perusoikeuksien toteutumista. Perustuslain esitöiden mukaan yksityiselämän suojan lähtökohtana on, että yksilöllä on oikeus elää omaa elämäänsä ilman viranomaisten tai muiden ulkopuolisten

[21] New York Times 9.12.2013: Microsoftin **Brad Smith**: "*People won't use technology they don't trust. Governments have put this trust at risk, and governments need to help restore it*". Facebookin **Mark Zuckerberg**: *"Reports about government surveillance have shown there is a real need for greater disclosure and new limits on how governments collect information. The U.S. government should take this opportunity to lead this reform effort and make things right."* Googlen **Larry Page**: "*The security of users' data is critical, which is why we've invested so much in encryption and fight for transparency around government requests for information. This is undermined by the apparent wholesale collection of data, in secret and without independent oversight, by many governments around the world."* Yahoon **Marissa Mayer**: *"Recent revelations about government surveillance activities have shaken the trust of our users, and it is time for the United States government to act to restore the confidence of citizens around the world."* Twitterin **Dick Costolo**: *"Unchecked, undisclosed government surveillance inhibits the free flow of information and restricts their voice. The principles we advance today would reform the current system to appropriately balance the needs of security and privacy while safeguarding the essential human right of free expression."*

tahojen mielivaltaista tai aiheetonta puuttumista hänen yksityiselämäänsä. Yksityiselämän suojan takaamiseksi valtiolta on jo perinteisesti edellytetty sen ohella, että se itse pidättäytyy loukkaamasta kansalaisten yksityiselämää, myös aktiivisia toimenpiteitä yksityiselämän suojaamiseksi toisten yksilöiden loukkauksia vastaan. Julkisen vallan on siis aktiivisesti arvioitava, millä tavoin yksityisyyden suojaan ja viestinnän luottamuksellisuuteen kohdistuvia laajamittaisia loukkauksia voidaan estää. [22] Monien maiden tapaan Suomessa onkin säädetty lakeja, jolla pyritään turvaamaan kansalaisten tietosuojaa henkilötietojen käsittelyssä ja sähköisen viestinnässä. Ongelmia ei voida kuitenkaan ratkaista yksinomaan kansallisella lainsäädännöllä.

Suomen hallitus on katsonut, että EU:n digitaalisten sisämarkkinoiden toteutumisen edistämiseksi EU:ssa tulisi etsiä pelisääntöjä sille, missä määrin viestinnän luottamuksellisuutta voidaan rajoittaa toisen jäsenvaltion toimin[23]. EU:n sisämarkkinoiden toteutumisen, kansainvälisen kaupan sekä tiedon vapaan liikkuvuuden kannalta olisi varsin ongelmallista, jos valtiot alkavat rajoittaa tiedon vapaata liikkuvuutta rajojen yli. Vaikutukset kohdistuisivat vääjäämättä tiedon lisäksi myös tavaroihin, palveluihin ja kokonaisiin liiketoimintamalleihin. Tällaisesta kehityksestä on kuitenkin jo monenlaisia merkkejä.

EU:n komissio on 25.8.2000 antanut ns. safe harbour -päätöksen, jonka nojalla Yhdysvaltojen todettiin takaavan sen alueelle siirrettyjen henkilötietojen suojan riittävän tason ja jonka nojalla eurooppalaisten henkilötietoja on voitu siirtää Yhdysvalloissa käsiteltäväksi[24]. EU:n tuomioistuin kuitenkin katsoi 6.10.2015 antamassaan ns. Schrems-tapauksen tuomiolauselmassa kyseisen safe harbour -päätöksen pätemättömäksi[25]. Tuomioistuimen mukaan mikään henkilötietodirektiivin säännös ei estä kansallisia viranomaisia valvomasta henkilötietojen siirtoja komission -päätöksen kohteena oleviin kolmansiin maihin. Tuomioistuin totesi, että Yhdysvaltojen kansalliseen turvallisuuteen, yleiseen etuun ja lakien noudattamiseen liittyvät vaatimukset ovat ns. safe harbor -järjestelmään verrattuina ensisijaisia, joten yhdysvaltalaiset yritykset ovat velvollisia syrjäyttämään safe harbour -järjestelmän mukaiset suojasäännöt rajoituksetta silloin, kun ne ovat ristiriidassa mainittujen vaatimusten kanssa. Päätöksellä voi olla merkittäviäkin vaikutuksia siihen, minkä lainsäädännön alaisuudessa EU-kansalaisten henkilötietoja voidaan oikeudellisesti kestävällä tavalla käsitellä tulevaisuudessa ja mihin palveluntarjoajat sijoittavat liiketoimintojaan.

Henkilötietoja siirtävät yritykset joutuvat hankkimaan uuden perusteen tietojen siirrolle, mikäli yritys on nojannut safe harbor -päätökseen. Yritykset voivat joutua tulevaisuudessa miettimään, onko niillä muu oikeusperusta siirtääkseen tietoja ETA-alueen ulkopuolelle, tai onko niillä mahdollisesti tarvetta sijoittaa tietojaan EU:n alueella oleviin palvelimiin, jotta voidaan välttää tietojen siirtäminen ETA-alueen ulkopuolelle. EU:n jäsenvaltioiden tietosuojavaltuutettujen työryhmä (ns. working party 29) on antanut yrityksille tammikuun 2016 loppuun saakka aikaa neuvotella uusi siirtoperuste, jonka jälkeen tietosuojaviranomaiset ovat sitoutuneet aloittamaan safe harbour -päätöksen pätemättömyydestä johtuvat täytäntöönpanotoimet[26].

Oikeudellisella sääntelyllä voi olla yritysten sijoittautumista estävä vaikutus ja siksi on tärkeää huolehtia liiketoiminnan harjoittamisen kannalta suotuisasta säännösympäristöstä. Myös kansallisten viranomaisten tiedusteluvaltuuksilla on vaikutus yritysten sijoittautumista koskeviin arvioihin. Samalla yksityisyyden suojan merkitys on korostunut ja tietosuojasta on tullut osa vastuullista liiketoimintaa.

---

[22] Perustuslain 10 ja 22 §:t sekä HE 309/1993 vp.
[23] Hallituksen selvitys eduskunnalle 12.6.2015, E21/2015 vp.
[24] Komission päätös 520/2000.
[25] EU:n tuomioistuimen 6.10.2015 antama ratkaisu asiassa C-362/14.
[26] Tietosuojavaltuutettujen julkilausuma 16.10.2015.

Suomella on tätä kehitystä vasten poikkeuksellisen hyvät edellytykset profiloitua valtiona, jossa lainsäädäntö turvaa digitaalisen tiedon käsittelylle korkean yksityisyyden suojan ja viestinnän luottamuksellisuuden suojan. Suomi voi profiloitua edullisena sijoittautumiskohde sellaisille yrityksille, joiden asiakaslupaukselle tietosuojalla ja tietoturvalla on tärkeä merkitys. Tällaisten yritysten määrän voidaan olettaa kasvavan samalla kun yhä suurempi osa liiketoiminnan arvonmuodostuksesta tapahtuu digitaalisen tiedon tuottamisessa tai käsittelyssä.

4.3 Tietoturvariskien taloudellinen arvottaminen

Tietoturvariskien hallinnan tarkoituksenmukaisuus ja tehokkuus edellyttää erittäin hyvää tietopohjaa siitä, millaisia riskejä tiedon käsittelystä liiketoimintaan kohdistuu, mikä on niiden todennäköisyys ja millaisilla keinoilla riskejä voidaan mahdollisimman kustannustehokkaasti pienentää. Toisin sanottuna erilaisille tietoturvariskeille sekä erilaisille riskienhallintakeinoille on laadittava euromääräinen hintalappu.

Keskeisin ongelma tässä arvottamisessa on soveliaan tiedon puute. Ongelmaa kuvaa esimerkiksi tutkimus, jonka mukaan tietoturvan vaarantuminen johtuu 60%:ssa tapauksia tahattomasta teosta. Toisaalta on kuitenkin arvioitu, että tahallisten tietoturvaloukkausten aiheuttamat vahingot olisivat suuruudeltaan merkittävämpiä[27]. Erilaisten tietoturvariskien ja hallintakeinojen yhdistelmien lukumäärästä johtuen todennäköisyyksien ja vaikutusten laskeminen edellyttää erittäin massiivista ja jäsentynyttä tietoa.

Tietoturvariskin aiheuttama taloudellinen vahinko voi seurata:

1. liiketoiminnan keskeytymisestä
2. omaisuuden vahingoittumisesta tai
3. aineettomien oikeuksien loukkaamisesta
4. seuraamusmaksuista tai suojaustoimien aiheuttamista kuluista

Tietoturvariskien voidaan arvioida johtavan siihen, että yritykset joutuvat tietotekniikkaa hyödyntäessään väkisinkin eräänlaiseen kilpajuoksuun tietoturvaloukkauksia tekevien rikollisten kanssa. Useimpien yritysten osalta tällainen tietoturvariskien hallinta tuntuu kaukaiselta liiketoiminnan ydinalueesta ja yrityksen osaamisesta. Niinpä johtaa todennäköisesti myös siihen, että kysyntä turvallisuudella ja luotettavuudella erottuville tuotteille kasvaa.

Tiedon käsite tulee ymmärtää tässä yhteydessä laajasti sillä, valtaosa nykyisten liiketoimintamallien arvosta perustuu digitaalisen tiedon hyödyntämiseen lukemattomilla eri tavoilla. Kyse voi siis olla liikesalaisuuden sisältävästä asiakirjasta, asiakasrekisteristä tai robottiajoneuvon liikkumista ohjaavasta ohjelmakoodin rivistä. Tietoturvariskiin liittyvä tieto voi olla asiakasrekisterissä, yrityksen sisäisessä tietojärjestelmässä taikka yrityksen tuottamassa tavarassa tai palvelussa.

Verkottuneissa ja keskinäisriippuvaisissa liiketoiminnan arvoketjuissa saattaa syntyä kriittisiä resursseja, joista monet yritykset ovat toisistaan tietämättä riippuvaisia. Tällaisten kohteiden tunnistaminen olisi ainakin periaatteessa mahdollista riskien vakuuttajalle, joka voi puolestaan reagoida vaatimalla kriittisten jaetun resurssin kahdentamista tai muuta riskin hajauttavaa toimenpidettä, kuten esim. riittävän kapasiteetin varaamista jaetun resurssin tuottajalta palvelutasosopimuksessa.

[27] Iso-Britannian elinkeino-, innovaatio- ja osaamisministeriö, 2015.

Saatavilla ei kuitenkaan ole selvää tietoa siitä, kuinka paljon yritykset käyttävät rahaa tietoturvariskien hallintaan. Ei myöskään ole tiedossa sitä, paljonko tietoturvariskien hallinta aiheuttaa sopimussuhteissa ylimääräisiä transaktiokustannuksia tai paljonko yritysten T&K-investointien kokonaismäärästä käytetään liiketoiminnan tietoturvaa ja tietosuojaa parantaviin kehitysprojekteihin.

Palveluiden käyttäminen voi teknisen tietoturvan näkökulmasta estyä palveluntarjoajan, sen käyttäjän tai toisen kriittiseen kumppaniin kohdistuvasta ongelmasta johtuen. Kriittisiä kumppaneita voivat olla esimerkiksi tiedonsiirtoyhteyden tarjoava teleyritys ja palvelun toteuttamiseen tarvittavaa tietojenkäsittelykapasiteettia tarjoava palveluntarjoaja. Käyttäjän näkökulmasta ei ole useinkaan merkitystä sillä, johtuuko palvelun käytön estyminen tai siihen liitetty muu tietoturvaongelma palvelua tarjoavan yrityksen vai sen kumppanin toiminnasta.

4.4 Tietoturvariskien hallinta

Korkealaatuisten ja luotettavien digitaalista tietoa hyödyntävien palveluiden tarjoaminen edellyttää tietoturva-asioiden kokonaisvaltaista huomioimista liiketoimintaa järjestettäessä. Tuotteet ja palvelut on suunniteltava, valmistettava ja ylläpidettävä siten, että tietoturva muodostaa niiden erottamattoman ja sisäänrakennetun osan. Toisin sanoen tietoturva on huomioitava liiketoiminnan koko elinkaaren aikana.

Oikean toimintaympäristön valinta

Palvelun tarjoamiseen kohdistuvia riskejä voidaan hallita eri keinoin. Esimerkiksi saatavuuteen liittyvää riskiä voidaan pienentää valitsemalla toimintaympäristö, jossa palvelun tarjoamisen kannalta keskeisten palveluntarjoajien toiminnan korkeaan laatuun ja turvallisuuteen voidaan luottaa. Suomen lainsäädäntö tarjoaa mahdollisuuden harjoittaa liiketoimintaa, jossa voidaan antaa korkeatasoinen asiakaslupaus tietoturvan ja tietosuojan korkeasta laadusta. Yritykset selvittävät usein sopimuskumppaneidensa palvelinten sijaintia arvioidakseen liiketoimintaan kohdistuvaa maariskiä.

Hyvänä esimerkkinä voidaan mainita myös suomalaisten teleyritysten tarjoamien viestintäverkkojen ja -palveluiden kansainvälisesti vertailtuna vähäinen häiriötilanteiden määrä ja teleyritysten kehittyneistä prosesseista johtuva nopeus erilaisista häiriötilanteista toivuttaessa.

Tietoturvan huomioiminen sopimussuhteissa

Oman tietoturvallisuuden lisäksi palvelun tarjoaminen edellyttää myös turvallisen ja toimintavarman tiedonsiirtoyhteyden muodostamista palveluntarjoajan ja sen käyttäjän välille. Tiedonsiirtopalveluita tarjoaviin teleyrityksiin ja tiedonsiirtoon käytettäviin viestintäverkkoihin ja -palveluihin on voitava luottaa kaikissa tilanteissa. Ja kuten edellä on selostettu, kaikki muutkin sopimussuhteessa ja ns. sopimusketjuissa olevat alihankkijat ja asiakkaat vaikuttavat riskin muodostumiseen ja sopimussuhteiden merkitys tulisikin huomioida valittaessa tarkoituksenmukaisia riskien hallinnan keinoja. Liiketoiminnassa tulisi arvioida huolellisesti, millaisia ohjelmistoja tai palveluita käytetään liiketoiminnassa tiedon käsittelyyn. Laadukkaan ohjelmisto- tai palvelutuottajan valinnalla voidaan pienentää riskiä merkittävästi.

Tietoteknistä palvelun laatua määrittävien ehtojen osalta neuvotteluvoima on usein palveluntarjoajalla. Tämä vaikeuttaa tietoturvariskin huomioimista kustannustehokkaasti palvelun hankintasopimuksessa. Sopimuksissa palvelun tarjoajan vastuu rajautuu usein kapeaksi ja se harvoin kattaa välillisiä vahinkoja.

Erityiset luottamuspalvelut ja tietoturvatuotteet

Yritykset voivat sisällyttää omiin tuotteisiinsa tai palveluihinsa monenlaisia markkinatoimijoiden tarjoamia luottamusta lisääviä palveluita, kuten esimerkiksi tunnistautumispalveluita, sähköisiä allekirjoituksia ja monenlaisia muita tiedon suojausmenetelmiä.

Hyvistäkin sopimuksista huolimatta tietoturvauhkien havaitseminen ja niihin reagoiminen edellyttää turvallisten laitteiden lisäksi tehokkaita ja luottamukseen perustuvia laajoja yhteistoimintaverkostoja. Yhden toimijan havaitsema tietoturvaloukkaus tai sen uhka voi kohdistua myös muihin toimijoihin. Yritykset tarjoavatkin yhteisöille ja yksityishenkilöille palomuureja, virustorjuntaohjelmistoja, tietoturvaloukkausten havainnointi- ja suojauspalveluita, joissa hyödynnetään myös kaikkia niitä havaintoja, joita saadaan muilta verkoston jäseniltä / muilta asiakkailta.

Myös Viestintävirasto kansallisena tietoturvaviranomaisena kerää ja jakaa tietoa tietoturvaloukkauksista sekä niiden uhkista. Virasto tuottaa tietoturvallisuuden tilannekuvaa ja tarjoaa Suomessa toimiville yrityksille luotettavan ja tehokkaan tavan vaihtaa tietoa tietoturvaongelmista muiden Suomessa toimivien yritysten sekä yhteisöjen kanssa.

Tietoturvaan liittyvä osaaminen

Hallitakseen tietoturvariskejä, yritykset tarvitsevat erittäin monipuolista osaamista niin työntekijöiden kuin alihankkijoidensa piirissä. Tietoturvan suojaaminen perustuu teknisellä tasolla hyvin paljon tehokkaisiin tiedon salaus- ja suojaus- ja pääsynhallintamenetelmiin, joiden tuottamiseen ja hyödyntämiseen liittyvän osaamisen perusvalmiuksien kehittäminen edellyttää pitkäjänteistä tutkimusta ja opetusta.

Tiedon suojaaminen perustuu pitkälti kryptologisiin menetelmiin, joiden hallinta edellyttää kehittyneitä matemaattisia valmiuksia. Kryptologian opetus ja tutkimus Suomalaisissa yliopistoissa ja korkeakouluissa vaikuttaa olevan verrattain ohutta osaajien kysyntään nähden. Myös muuta teknologista osaamista sekä liiketaloudellista ja oikeudellista osaamista kysytään. EU:n tietosuoja-asetuksen ja verkko-tietoturvadirektiivin myötä tietosuojaan ja tietoturvaan liittyvän osaamisen kysyntä oletettavasti kasvaa.

Tietoturvariskien vakuuttaminen

Tietoturvariskien aiheuttamien vakuutusten markkina on Suomessa ja Euroopassa vielä verrattain kehittymätön mutta ilmeisessä kasvussa. Useat vakuutusyhtiöt ovat ottaneet tuotevalikoimaansa erilaisia tietoturvariskeistä aiheutuvien vahinkojen vakuutustuotteita. Nykyisin vakuutuksilla korvataan ennen kaikkea liiketoiminnan keskeytyksestä aiheutuvia kustannuksia (esim. kriisinhallintakuluja, katemenetyksiä, puolustusmenoja, sanktiomaksuja). Kysyntää olisi myös vakuutuksille, jotka kattaisivat kolmansille osapuolille aiheutuvia taloudellisia vastuita sekä vakuutuksille, jotka kattaisivat hallinnollisista seuraamusmaksuista johtuvia kuluja.

Vakuutusten laajempaa hyödyntämistä hidastaa tiedonpuute. Tietoturvasta johtuvien vahinkojen juurisyitä on vaikeaa hahmottaa, koska tilastollista tarkastelua kestäviä tietoja ei ole tarpeeksi saatavilla ja syy-yhteyden määrittäminen on siksi vaikeaa. Tällä hetkellä tietoturvariskeihin liittyvä ns. jäännösriski jääkin hyvin usein yrityksen omalle vastuulle vaikka monilla aloilla jäännösriskiä voi vakuuttaa.

Tietoturvaan liittyvien sertifikaattien ja standardien merkitys

Sopimussuhteissa osapuolten olisi voitava varmistua siitä, että sopimuskumppani huolehtii tietoturvariskien hallinnasta. Yksi keino lisätä tätä luottamusta on tehdä sopimuksia sellaisten osapuolten kanssa, jotka noudattavat jotakin tunnettua standardia ja jonka edellyttämien toimien toteutuminen voidaan riippumattomasti arvioida ja todentaa (auditointi).

Suomen kilpailukyvyn kannalta olisi olennaista, että kansainväliset standardit suosisivat tuotteita, joiden valmistuksessa suomalaisilla yrityksillä on vahvuuksia. On tärkeää, että suomessa liiketoimintaa harjoittavilla yrityksillä on mahdollisuus osallistua erilaisten tuotteiden, palveluiden ja tuotantomenetelmien standardointiin. Standardisointi on lähtökohtaisesti kaikille avointa ja siihen osallistuminen vapaaehtoista. Kansainvälisen standardointiorganisaatio ISO:n kansallisena jäsenjärjestönä toimiva Suomen Standardisoimisliitto SFS:n koordinoi tietoturvatekniikoiden standardisointia ja tiedottaa standardoitavista kohteista. Standardoinnin on oltava yritysten liiketoiminnallisista tarpeista lähtevää, mutta viranomaiset voivat eri tavoin tukea yritysten osallistumista standardointityöhön.

Standardisointi nähdään usein muusta liiketoiminnasta erillisenä osa-alueena, johon osallistuminen ei kuulu organisaation varsinaiseen ydintoimintaan. Standardointiin osallistumalla ja niitä hyödyntämällä yritykset voivat kuitenkin luoda edellytyksiä uuden liiketoiminnan kehittämiselle ja kasvattamiselle. Standardointi voikin olla merkittävä kasvun väline digitalisaation muuttaessa perinteisiä markkina- ja valta-asetelmia erittäin nopealla tavalla. Jotta tietoturva voisi olla laajasti sisäänrakennettuna tuotteisiin ja palveluihin, tulisi standardeissa esitettyjen menetelmien ja ohjeiden olla upotettuna tietoturvatoteutuksiin.

Lisäksi yksittäiset, pienet tai keskisuuret yritykset eivät useinkaan halua tai pysty ottamaan kovin pitkälle menevää strategista ja ennakoivaa lähestymistapaa standardisointiin. Standardisoinnista tuleekin helposti isojen yritysten pelikenttä, vaikka vaikutusmahdollisuudet itsessään olisivatkin suurelta osin tasavertaiset. Suomen tai sisämarkkinoiden kilpailukykyä kohennettaessa standardisointia voitaisiin lähestyä järjestelmällisemmin ja tavoitelähtöisesti. Keskiössä olisi tällöin omien kilpailuasemien kannalta keskeisten standardien tunnistaminen, niihin vaikuttaminen ja niiden systemaattinen implementointi kansallisessa toimiympäristössä. Tämä edellyttäisi yhteistyön tiivistämistä yhteisten tavoitteiden hahmottamiseksi.

Tietoturvallisuuteen läpinäkyvyyttä auditoinneilla

Luotettavaksi todettua puolueetonta auditoijaa voidaan käyttää sen arvioimiseksi, vastaako sopimuskumppanin järjestelmät ja menetelmät sopimuksessa edellytettyjä tietoturvaa parantavia tekniikoita, menetelmiä ja standardeja. Lähtökohta on, että sopimuskumppanit määrittelevät ne vaatimukset jotka auditoidaan.

Auditoinnin merkitys korostuu silloin, kun tietoturvan kannalta olennaisesta tekijästä ei voida normaalisti ulkopuolisen havainnoilla varmistua. Esimerkiksi suljettuun lähdekoodiin perustuvissa ohjelmistoissa asiakas ei pääse näkemään, miten ohjelmisto tosiasiassa toimii ja miten turvallinen se on. Ulkopuoliselle auditoijalle voidaan tarjota mahdollisuus tutustua suljettuihinkin lähdekoodin osiin.

Auditoitu tuote, palvelu tai yritys voi saada todistuksen tai sertifikaatin, joka on osoitus auditointivaatimusten täyttämisestä. Jotta todistuksella olisi merkitystä ajan hampaassa, voidaan sopimuksessa edellyttää, että tuotteseen tehtävistä muutoksista ilmoitetaan auditoijalle, joka arvioi muutosten vaikutukset sopimuksessa määriteltäviin vaatimuksiin.