JULKAISUJA 7/2016

Maailman luotetuinta digitaalista liiketoimintaa

Suomen tietoturvallisuusstrategia

LIIKENNE- JA VIESTINTÄMINISTERIÖ

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
19.4.2016

Julkaisun nimi
Maailman luotetuinta digitaalista liiketoimintaa. Suomen tietoturvallisuusstrategia.

Tekijät
Liikenne- ja viestintäministeriö ja tietoturvallisen liiketoiminnan kehittämisryhmä

Toimeksiantaja ja asettamispäivämäärä
Valtioneuvoston toimintasuunnitelma strategisten kärkihankkeiden ja reformien toimeenpanemiseksi 28.9.2015

Julkaisusarjan nimi ja numero

Liikenne- ja viestintäministeriön julkaisuja 7/2016

ISSN (verkkojulkaisu) 1795-4045
ISBN (verkkojulkaisu) 978-952-243-475-3
URN http://urn.fi/URN:ISBN:978-952-243-475-3
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 kehittämisryhmä. Ryhmä kokoontui 5 kertaa ja järjesti kuulemistilaisuuden strategian luonnoksesta. Työryhmä luovutti ehdotuksen tietoturvastrategiaksi liikenne- ja viestintäministerille 10. helmikuuta 2016. Ministeri hyväksyi strategian sisällön työryhmän ehdotuksen mukaisena 10. maaliskuuta 2016.

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 digitaalinen liiketoiminta tulee Suomesta. Strategian tavoitteina on, että: 1) Suomessa on digitaalisen liiketoiminnan kannalta kilpailukykyinen ja edistyksellinen lainsäädäntö; 2) EU:n sisämarkkinat toimivat nykyistä 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 ja kansalaisia tietoturvan parantamisessa.

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

KOMMUNIKATIONS-
MINISTERIET

Publikationsdatum
19.4.2016

Publikation
Världens mest tillförlitliga digitala affärsverksamhet.
En informationssäkerhetsstrategi för Finland.

Författare
Kommunikationsministeriet och utvecklingsgruppen för informationssäker affärsverksamhet

Tillsatt av och datum
Statsrådets handlingsplan för genomförande av spetsprojekten och reformerna i det strategiska regeringsprogrammet 28.9.2015

Publikationsseriens namn och nummer

Kommunikationsministeriets publikationer 7/2016

ISSN (webbpublikation) 1795-4045
ISBN (webbpublikation) 978-952-243-475-3
URN http://urn.fi/URN:ISBN:978-952-243-475-3
HARE-nummer

Ämnesord
Digitalisering, digital affärsverksamhet, informationssäkerhet, dataskydd, informations- och kommunikationssystem, riskhantering, skydd av den personliga integriteten, konfidentiell kommunikation

Kontaktperson
Olli-Pekka Rantala, Timo Kievari

Rapportens språk
Finska

Övriga uppgifter
Som stöd för beredningen av informationssäkerhetsstrategin tillsattes 28.9.2015 en utvecklingsgrupp för informationssäker affärsverksamhet. Gruppen sammanträdde fem gånger och ordnade ett diskussionsmöte om strategiutkastet. Arbetsgruppen överlämnade förslaget till en informationssäkerhetsstrategi åt kommunikationsministern den 10 februari 2016. Ministern godkände innehållet i strategin i oförändrad form enligt arbetsgruppens förslag den 10 mars 2016.

Sammandrag
Finland har goda förutsättningar att bli känt som ett kompetent, framgångsrikt och pålitligt land där det är tryggt att ta fasta på de möjligheter som digitaliseringen erbjuder. Genom att ta fram och erbjuda tjänster som bygger på att utnyttja digital information kan vi skapa och påskynda ekonomisk tillväxt. Vår framgång är beroende av att vi utvecklar, tar till oss och prövar nya modeller för affärsverksamhet och intjäning. Detta förutsätter i sin tur att vi kan lita på de nya tjänsterna, affärsmodellerna och aktörerna på marknaden.

Ett starkt kunnande i fråga om informationssäkerhet och marknadsutveckling ökar våra chanser att påverka vår roll och position i en snabbt föränderlig värld. Det är nödvändigt att garantera den digitala självständigheten för att Finland ska kunna ta sig in på den internationella marknaden och för att Finland ska kunna vara en brobyggare för en säker och tillförlitlig cybermiljö.

Visionen i den nationella informationssäkerhetsstrategin är att Finland är världens tillförlitligaste land inom digital affärsverksamhet. Målen för strategin är att 1) Finland med tanke på digital affärsverksamhet har en konkurrenskraftig och framstegsvänlig lagstiftning, 2) den inre marknaden i EU fungerar på ett tillförlitligare sätt än i dagsläget, 3) finska företag drar nytta av internationella standarder och av digitala nyttigheter med integrerad informationssäkerhet, 4) man forskar, mäter, följer upp och utvecklar informationssäkerheten och kunskapen på området, 5) myndigheterna hjälper organisationer och medborgare att förbättra informationssäkerheten.

I strategin beskrivs de centrala åtgärder som stödjer måluppfyllelsen. I motiveringen till strategin redogörs dessutom för nödvändiga mål och åtgärder.

MINISTRY OF TRANSPORT AND COMMUNICATIONS

Date
19 April 2016

Title of publication
Most reliable corporate digital systems and services. Finland's information security strategy

Author(s)
Ministry of Transport and Communications and the development group for business with information security

Commissioned by, date
The Finnish Government's plan of action for the implementation of key projects and reforms, 28 September 2015

Publication series and number

Publications of the Ministry of Transport and Communications 7/2016

ISSN (online) 1795-4045
ISBN (online) 978-952-243-475-3
URN http://urn.fi/URN:ISBN:978-952-243-475-3
Reference number

Keywords
Digitalisation, digital business, information security, data protection, information and communication management, risk management, protection of privacy, confidentiality of communications

Contact person
Olli-Pekka Rantala, Timo Kievari

Language of the report

Other information
For the preparation of the strategy a development group for business with information security was set up on 28 September 2015. The group met 5 times and arranged a hearing on the draft of the strategy. The working group submitted its proposal for the Information Security Strategy to Ms Anne Berner, Minister of Transport and Communications, on 10 February 2016. The Minister approved the proposed strategy on 10 March 2016.

Abstract
Finland is in a good position to become known as a competent, successful and reliable country, where it is safe to take hold of the opportunities brought by digitalisation. By developing and offering services based on the utilisation of digital information, it is possible to create and accelerate economic growth. Our success depends on that we develop, assimilate and experiment with new kinds of business and earning models. This requires that we can trust on the new services, business models and market actors.

Strong grip on the development of information security expertise and market development will improve our chances to influence our role and position in the rapidly changing world order. Safeguarding this digital independence is necessary for Finland's efforts to go all out for international markets and act as a bridge builder for safe and reliable cyber environment.

The vision of the national information security strategy is that the world's most trusted digital business comes from Finland. The strategy's aims are that: 1) Finland will have a legislation that is competitive and progressive from the perspective of digital business; 2) the EU's internal market will operate more reliably than so far is the case; 3) Finnish companies will benefit from international standards as well as digital products and commodities with inbuilt information security; 4) information security and the related expertise will be investigated, measured, followed-up and developed; 5) the authorities will help communities and citizens in the improvement of information security.

The central measures supporting the realisation of the aims are described in the strategy. In addition, the need for these aims and measures is justified in the strategy's justification part.

Sisällysluettelo

1. JOHDANTO

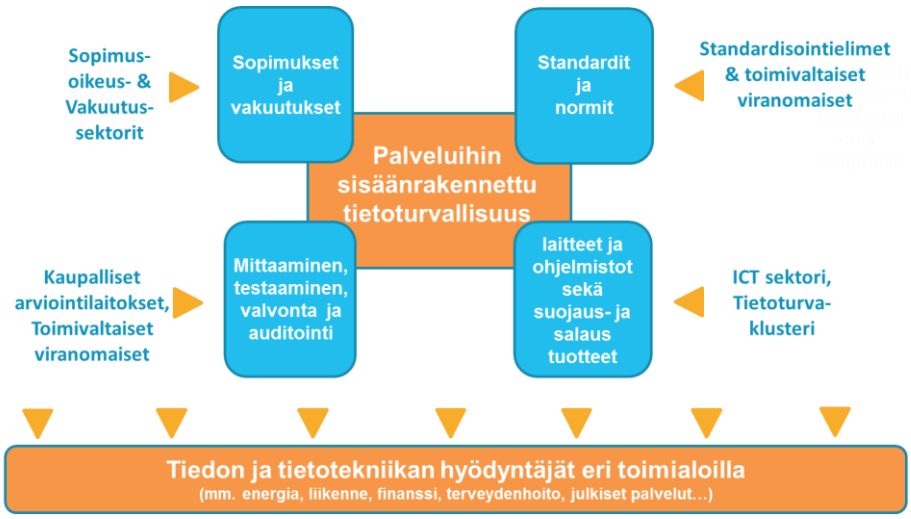
Pääministeri Juha Sipilän hallituksen kärkihankkeena Suomeen rakennetaan digitaalisen liiketoiminnan kasvuympäristö. Yhtenä kärkihankkeen keskeisenä toimenpiteenä valmistellaan ja toimeenpannaan luottamusta internetiin sekä digitaalisiin toimintatapoihin lisäävä kansallinen tietoturvastrategia.

Kärkihankkeiden toimeenpanosuunnitelmassa on kirjattu strategiatyön keskeiset tavoitteet ja lähtökohdat. 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 kuten esineiden internetiin, massadatan hyödyntämiseen ja erilaisiin älyteknologioihin. 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. Lisäksi eri toimijoiden tulisi yhdessä luoda edellytyksiä sille, että tulevaisuudessa yksi tai useampi maailman johtavista tietoturvayrityksistä on Suomalainen.

Kansallisen tietoturvastrategian visiona on se, että:

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

3. STRATEGIAN TAVOITTEET JA NIITÄ EDISTÄVÄT TOIMENPITEET

Strategian visio 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 tasolla.

Strategian tavoitteina on, että:

1) Suomessa on digitaalisen liiketoiminnan kannalta kilpailukykyinen ja edistyksellinen lainsäädäntö;
2) EU:n digitaaliset sisämarkkinat toimivat nykyistä 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 ja kansalaisia tietoturvan parantamisessa

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 Suomessa on digitaalisen liiketoiminnan kannalta kilpailukykyinen ja edistyksellinen lainsäädäntö

Lainsäädäntö luo edellytykset siihen, että Suomessa voidaan harjoittaa mahdollisimman kilpailukyistä liiketoimintaa. Suomi on houkutteleva kohde datan käsittelyyn ja hyödyntämiseen perustuville investoinneille. Suomi erottuu edukseen luotettavana sijoittautumispaikkana digitaalisuutta hyödyntäville yrittäjille.

TOIMENPITEET:

- Digitaalisen toimintaympäristöön ja erityisesti tiedon käsittelyyn ja tietoturvaan liittyvän lainsäädännön valmistelun ja säädösten sujuvoittamisen yhteydessä arvioidaan säädösten vaikutukset tietoturvallisuuteen ja liiketoiminnan harjoittamiselle.[1]
- Verkko- ja tietoturvadirektiivin voimaansaattamisen yhteydessä turvataan yritysten mahdollisuudet sovittaa tietoturvariskien hallintaan liittyvät uudet velvoitteet osaksi muiden liiketoiminnan riskiensä hallintaa. Tämän varmistamiseksi kootaan voimaansaattamista tukeva työryhmä arvioimaan nykyisen sääntelyn riittävyys kullakin direktiivin soveltamisalaan kuuluvalla toimialalla.[2]
- Valmisteltaessa EU:n tietosuoja-asetuksen edellyttämiä muutoksia kansalliseen sääntelyyn pyritään olemaan lisäämättä yrityksille kilpailukykyä haittaavaa ylimääräistä taakkaa.[3]
- Huolehditaan, että viestinnän välittäjän vastuuta koskevaa sääntelyä kehitetään EU:ssa teknologia- ja toimijaneutraalisti (vastuu yksityisyyden suojasta ja tietoturvasta viestejä välitettäessä).[4]
- Kyberturvallisuuden kehittämistyössä turvataan kaikin keinoin käyttäjien oikeuksien, kuten yksityisyyden suojan ja luottamuksellisen viestin suojan, säilyminen sähköisissä palveluissa ja verkkoympäristössä.[5]

[1] Vastuutahot: kaikki ministeriöt
[2] Vastuutahot: liikenne- ja viestintäministeriö, työ- ja elinkeinoministeriö, valtiovarainministeriö, sosiaali- ja terveysministeriö, ympäristöministeriö
[3] Vastuutahot: oikeusministeriö ja muut ministeriöt
[4] Vastuutahot: liikenne- ja viestintäministeriö
[5] Vastuutahot: puolustusministeriö, sisäministeriö, oikeusministeriö, liikenne- ja viestintäministeriö, valtiovarainministeriö

3.2 EU:n digitaaliset sisämarkkinat toimivat nykyistä 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.[6]
- Suomi vaikuttaa aktiivisesti tietoturvastrategian tavoitteiden huomioimiseksi Euroopan Unionin verkko- ja tietoturvaviraston (ENISA) toiminnassa.[7]
- Suomi huomioi tietoturvastrategian tavoitteet OECD:n ministerikokouksessa Cancunissa 2016 annettavan julistuksen valmistelussa.[8]
- Tietoturvastrategian tavoitteet huomioidaan kyberturvallisuuden ulkopoliittisia ulottuvuuksia yhteen sovittavassa työssä sekä laadittaessa Suomea sitovia kansainvälisiä sopimuksia.[9]
- Suomi vaikuttaa tietoturvastrategian tavoitteiden huomioimiseksi EU:n komissioon kauppaneuvotteluissa.[10]

[6] Vastuutahot: liikenne- ja viestintäministeriö, ulkoasiainministeriö, työ- ja elinkeinoministeriö, valtiovarainministeriö
[7] Vastuutahot: liikenne- ja viestintäministeriö, Viestintävirasto
[8] Vastuutahot: liikenne- ja viestintäministeriö, työ- ja elinkeinoministeriö
[9] Vastuutahot: ulkoasiainministeriö
[10] Vastuutahot: ulkoasiainministeriö, liikenne- ja viestintäministeriö

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 (mukaan lukien vakuuttaa) liiketoiminnalleen taloudellista vahinkoa aiheuttavia tietoturvariskejä. Suomessa ja EU:ssa on käytössä standardeja, jotka helpottavat tietoturvan näkökulmasta luotettavan sopimuskumppanin valintaa. Nämä tavoitteet huomioidaan myös esineiden internetin kehitystyössä sekä kansallisesti että kansainvälisesti.

TOIMENPITEET:

- Parannetaan luottamusta digitaalisiin palveluihin ja sähköisiin transaktioihin käynnistämällä sähköisen tunnistamisen kansallinen luottamusverkosto, jossa eri toimijat voivat hyödyntää yksinkertaisemmin vahvaa sähköistä tunnistamista ja luottaa toistensa välittämiin tunnistamistietoihin. Valtio kehittää osana Kansallisen arkkitehtuurin toteuttamisohjelmaa julkishallinnolle keskitettyä palvelua kansalaisten sähköiseen tunnistamiseen.[11]
- Kehitetään julkisen ja yksityisen sektorin yhteistyössä edellytyksiä henkilötietojen anonymisoinnin mahdollistaville palveluille, jotta palveluntarjoajat voisivat pienentää henkilötietojen käsittelyyn liittyviä tietoturvariskejään.[12]
- Selvitetään miten yleisimpien päätelaitteiden, käyttöjärjestelmien, internet-selainten, hakukoneiden ja viestintäsovellusten käyttöehdot sekä tiedonsuojausominaisuudet vaikuttavat käyttäjän mahdollisuuksiin suojata tietojaan omassa liiketoiminnassaan tai muussa toiminnassaan.[13]
- Selvitetään erilaisten tiedonsuojausominaisuuksien sertifioinnin tarve käyttäjien näkökulmasta sekä niiden vaikutus digitaalisia hyödykkeitä kohtaan koettuun luottamukseen. Selvitetään sertifiointi- ja standardointielimien merkitys ICT-alan laite- ja palveluntuottajille sekä niiden asiakkaille.[14]

[11] Vastuutahot: liikenne- ja viestintäministeriö, valtiovarainministeriö, Väestörekisterikeskus
[12] Vastuutahot: liikenne- ja viestintäministeriö, valtiovarainministeriö, Väestörekisterikeskus, Tietosuojavaltuutetun toimisto
[13] Vastuutahot: Viestintävirasto, Tietosuojavaltuutetun toimisto, valtiovarainministeriö
[14] Vastuutahot: liikenne- ja viestintäministeriö, Viestintävirasto, Suomen Standardoimisliitto SFS ry

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 – mukaan lukien tieto- ja viestintärikosten aiheuttamat taloudelliset vahingot.[15]
- Kartoitetaan suomalaisia tietoturvahankkeita, joita Euroopan Komissio voisi rahoittaa osana vuonna 2016 perustettavaa kybertutkimusohjelmaansa.[16]
- Etsitään valtioneuvoston päätöksentekoa tukevan tutkimus- ja kehitystoiminnan osana keinoja parantaa digitaalisten palvelujen ja liiketoimintamallien luotettavuutta.[17]
- Seurataan tietoturvatuotteiden osuutta ja kehitystä ICT -toimialan liikevaihdosta. Päävastuu: Teknologiateollisuus ry, FISC ry
- Kartoitetaan Suomessa toimivien yritysten tarpeet tietoturva- ja tietosuojaosaajille. Selvitetään keinoja osaajien saatavuuden parantamiseksi. Huolehditaan siitä, että tietoturvallisuuteen liittyvään koulutukseen on käytettävissä riittävästi resursseja.[18]
- Järjestetään sarja kansallisten tietoturvaosaajien tunnistamista ja verkostoitumista tukevia tietoturvatapahtumia (Hackathon).[19]

[15] Vastuutahot: liikenne- ja viestintäministeriö, sisäministeriö, valtiovarainministeriö

[16] Komission ohjelma eurooppalaisten tietoturvallisten tuotteiden saatavuuden parantamiseksi julkisen ja yksityisen sektorin välisenä yhteistyönä. Vastuutahot: FISC ry, Teknologiateollisuus ry, liikenne- ja viestintäministeriö, puolustusministeriö

[17] Valtioneuvosto hyväksyi 3.12.2015 valtioneuvoston päätöksentekoa tukevan selvitys- ja tutkimussuunnitelman, jonka yhtenä hankkeena selvitetään, miten voidaan parantaa digitaalisten hyödykkeiden ja liiketoimintamallien luotettavuutta. Vastuutahot: valtioneuvoston kanslia, valtiovarainministeriö

[18] Vastuutahot: opetus- ja kulttuuriministeriö, työ- ja elinkeinoministeriö, Tekes

[19] Vastuutahot: Viestintävirasto, yritykset, työ- ja elinkeinoministeriö, Tekes

3.5 Viranomaiset auttavat yhteisöjä ja kansalaisia tietoturvan parantamisessa

Viranomaiset auttavat ja tukevat yrityksiä huolehtimaan tietoturvasta liiketoiminnassaan muun muassa 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.[20]
- Ylläpidetään tietoturvallisuuden tilannekuvaa Viestintäviraston, yritysten ja muiden yhteisöjen luottamukseen perustuvan tiedonvaihdon avulla.[21]
- Asetetaan viranomaisten ja elinkeinoelämän yhteistyöryhmä yrityksiin kohdistuvien rikosten ennalta estämisen ja torjunnan tehostamiseksi. Ryhmän erityisenä painopisteenä on muun muassa tietoverkkorikollisuuden torjunta.[22]
- Viranomaiset tukevat toimivaltansa puitteissa tulkintakäytännöllään, tarjoamillaan palveluilla sekä avoimuuteen pyrkivillä menettelytavoillaan uusien tiedon käsittelyyn perustuvien ja luotettavuutta parantavien liiketoimintamallien syntymistä.[23]
- Muodostetaan kansallinen verkosto, joka edesauttaa suomalaisia yrityksiä osallistumaan standardointityöhön viestinnän luottamuksellisuutta parantavien tietoturvallisten palveluiden ja laitteiden kaupallisen saatavuuden, käytön ja viennin edistämiseksi.[24]
- Selvitetään olisiko sellaisille tietoturvatuotteille ja -palveluille kysyntää, joiden tarjonnassa tai käytössä voidaan soveltaa yksinomaan Suomen tai EU:n lainsäädäntöä. Arvioidaan miten tällaista palveluntarjontaa on tarvittaessa mahdollista ankkuroida Suomeen, esimerkiksi valtionomistuksen keinoin.[25]
- Elinkeinoelämän edustajat ja keskeiset viranomaistahot kokoontuvat verkostona seuratakseen strategiassa esitettyjen toimenpiteiden toteutumista. Ministeriöt vievät strategian edellyttämät toimenpiteet omaan toiminnan- ja talouden suunnitteluunsa ja toimittavat tästä koosteen verkostolle.[26]

[20] Vastuutahot: liikenne- ja viestintäministeriö, Viestintävirasto, Huoltovarmuuskeskus, valtiovarainministeriö
[21] Vastuutahot: Viestintävirasto, yritykset, valtionvarainministeriö
[22] Vastuutahot: sisäministeriö, yritykset
[23] Vastuutahot: toimivaltaiset viranomaiset
[24] Vastuutahot: Viestintävirasto, Suomen Standardoimisliitto SFS ry
[25] Vastuutahot: valtioneuvoston kanslia
[26] Vastuutahot: liikenne- ja viestintäministeriö ja muut ministeriöt

STRATEGIAN PERUSTELUOSA

4. STRATEGIAN PERUSTELUOSA

4.1 Strategian tausta

Tieto- ja viestintäteknologia sekä niihin liittyvät palvelut muuttavat yhteiskunnan toimintaa sekä valtarakenteita mullistavalla tavalla. Esineiden internet, massadatan hyödyntäminen ja erilaiset älyteknologiat ovat esimerkkejä tulevaisuuden digitaalisesta maailmasta, jossa yritykset kilpailevat asiakkaista ja markkinaosuuksista. Tässä 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.

Uusien liiketoimintamahdollisuuksien lisäksi globaaliin digitalisaatioon liittyvät kehitystrendit aiheuttavat luottamuspulaa markkinatoimijoiden välille. Luottamuspulaa aiheuttaa tavanomaisten verkkorikosten ohella joidenkin 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 matkustajan luottamus on ansaittava, jotta uudet palvelumuodot hyväksyttäisiin asiakkaiden taholta. Vähintäänkin palvelun luotettavuutta on mahdollista hyödyntää kilpailuetuna kilpailijoihin nähden.

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

4.2 Tilannekuva tietoturvallisuuden taloudellisesta merkityksestä

Liiketoiminnan arvo kasvaa teknologiaa hyödyntämällä

Tieto- ja viestintäteknologia sekä niihin liittyvät palvelut muuttavat yhteiskunnan toimintaa sekä valtarakenteita mullistavalla tavalla. Esineiden internet, massadatan hyödyntäminen ja erilaiset älyteknologiat ovat esimerkkejä tulevaisuuden digitaalisesta maailmasta, jossa yritykset kilpailevat asiakkaista ja markkinaosuuksista. Tässä 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 miljardia euroa (josta teleyritykset 4,5 miljardia euroa, ohjelmistot, konsultointi ja tietopalvelut

7,9 miljardia euroa sekä tietokoneiden ja sähkölaitteiden valmistus 31 miljardia euroa)[27]. Toimiala on merkittävällä tavalla vientipainotteinen sillä Suomen loppukäyttäjäkulutusta kuvaavan IT-markkinan liikevaihto oli vuonna 2014 yhteensä 6 miljardia euroa (josta laitteet 1,5 miljardia euroa, ohjelmistot 1,3 miljardia euroa ja IT-palvelut 3,2 miljardia euroa)[28]. Suomen bruttokansantuote vuonna 2012 oli noin 200 miljardia euroa ja niin sanotun internet-talouden osuuden on arvioitu muodostavan siitä noin 10 prosenttia[29]. 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 miljardin euron verran uutta liikevaihtoa sekä 48.000 uutta työpaikkaa, jos "suomalaiset yritykset ottavat roolin teollisen internetin alustojen ja ekosysteemien avaintoimijoina"[30].

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[31]. Laajeneminen on mahdollistanut yrityksille sellaisen liiketaloudellisen arvon muodostumisen, joka ei ole riippuvaista ajasta, alueesta tai aineesta. Sekä teknologian kehitys että internetin luonne eräänlaisena "rajattomana" tuotannontekijänä ovat avanneet 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.

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 miljardin euron kasvu EU:n bruttokansantuotteeseen[32]. Lisäksi on laskettu, että EU:n kansalaisten henkilötiedoilla on vuositasolla yhteensä 315 miljardin euron liiketaloudellinen arvo[33]. Sisämarkkinoiden esteet ilmenevät muun muassa ylimääräisinä kustannuksina, joita tavaroiden ja palveluiden tarjoaminen toisiin jäsenvaltioihin aiheuttaa. Esimerkiksi rajat ylittävässä kuluttajakaupassa vieraan EU-jäsenvaltion lainsäädännön noudattamisesta aiheutuu yksittäiselle yritykselle keskimäärin 9000 euron kustannukset per jäsenvaltio[34]. On tärkeää huolehtia siitä, ettei EU:n

[27] Tilastokeskus sekä Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, 2013.
[28] Teknologiateollisuus ry, Market Visio.
[29] Tilastokeskus ja Elinkeinoelämän tutkimuslaitos, 2012.
[30] Valtioneuvoston kanslian selvitys- ja tutkimushanke, jonka tekijöinä mm. Elinkeinoelämän tutkimuslaitos, Aalto-yliopisto, Valtion Teknillinen tutkimuslaitos, 2015.
[31] OECD, Maailmanpankki ja Kansainvälinen televiestintäliitto ITU.
[32] Euroopan Unionin Parlamentti, 2015.
[33] Euroopan Unionin Komissio, Boston Consulting Group, 2013.
[34] Euroopan Unionin Komissio, 2011.

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 joidenkin 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 matkustajan 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 prosenttia haastatelluista 28.000 eurooppalaisesta kertoi muuttaneensa tapojaan käyttää internetiä tietoturvahuolien vuoksi. Suomalaisista 59 prosenttia arvioi tuntevansa digitaalisiin palveluihin liittyvät riskit hyvin, kun EU:n keskiarvo oli 50 prosenttia. Suomalaiset pitävät mahdollisuuksiaan EU:ssa toiseksi parhaina verkkorikollisuudelta suojautumiseen.[35]

Edward Snowdenin paljastuksista kuulleista internetin käyttäjistä 39 prosenttia oli ryhtynyt toimiin yksityisyytensä suojaamiseksi[36]. Yhdysvalloissa paljastuneiden vakoiluskandaalien on arvioitu aiheuttaneen jo tähän mennessä noin 40 miljardin dollarin välittömät menetykset maan ICT-teollisuudelle[37]. Pilvipalvelun tarjoajien arvioidaan menettävän pahimmillaan jopa 20 prosenttia Yhdysvaltain ulkopuolisesta liikevaihdostaan PRISM-kohun seurauksena seuraavien kolmen vuoden aikana[38].

Isoimmat teknologiayritykset ovat Snowdenin paljastusten jälkeen alkaneet salata kuluttajapalveluidensa dataa ja tietoliikennettä sekä korostaneet asiakaslupauksissaan tietosuojan korkeaa merkitystä. Yhdysvaltojen tuhannen suurimman yrityksen satsaukset tietosuojan parantamiseksi on arvioitu 2,4 miljardin dollarin suuruisiksi vuosittain. Tietosuoja-asiantuntijoiden kysyntä ja tulot ovat merkittävässä kasvussa.[39]

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 yksittäisille yrityksille satojen miljoonien dollarien vahinkoja[40]. Iso-Britanniassa 81 prosenttia suurista organisaatioista oli joutunut vuoden sisällä tietoturvaloukkauksen kohteeksi. Loukkauksista aiheutuneet kustannukset kaksinkertaistuivat vuoden aikana 0,6–1,15 miljoonan punnan suuruisiksi per organisaatio[41]. Esimerkiksi kahden yhdysvaltalaisen kauppaketjun maksukorttirekisteriin tehty tietomurto on tähän mennessä aiheuttanut yrityksille 252 miljoonan dollarin vahingot, joista noin 90 miljoonaa dollaria on korvattu vakuutuksin. Näiden vahinkojen lisäksi oikeusprosessit ovat yhä kesken noin 200 miljoonan dollarin arvoisista korvausvaatimuksista[42].

[35] EU komissio, 2015.
[36] OECD, 2014.
[37] Teknologiateollisuus ry & FISC ry, 2014.
[38] The Information Technology & Innovation Foundation, 2013.
[39] OECD, 2015.
[40] OECD, 2015.
[41] Iso-Britannian elinkeino-, innovaatio- ja osaamisministeriö, 2015.
[42] OECD, 2015.

Tietoturvaongelmien aiheuttamilta vahingoilta suojaavien vakuutusten osuus vakuutusmarkkinoista on pieni, mutta se on kasvamassa. Tietoturvavakuutusmaksuja kertyy vuosittain USA:ssa 2,5 miljardia dollaria ja Euroopassa 150 miljoonaa dollaria.[43]

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 miljardin euron lisäkustannukset[44]. Suomessa lainsäädäntö turvaa jo nykyisin verrattain korkeatasoisen tietosuojan ja tietoturvan tason. Lainsäädäntömme muodostaa yritystoiminnalle kilpailuedun muun muassa niihin valtioihin nähden, joissa viranomaisilla on laajemmat oikeudet puuttua yksityiselämän ja viestinnän luottamuksellisuuden suojaan tietoverkoissa ja tietojärjestelmissä. Kilpailuedun säilyttäminen tuleekin huomioida myös säädettäessä uutta lainsäädäntöä. Esimerkiksi kotimaisten tiedustelulakien valmistelussa on jo hyvin varhaisessa vaiheessa lähdetty siitä, ettei yrityksiä velvoiteta luovuttamaan salausavaimia tai asentamaan takaportteja ohjelmistoihin ja laitteistoihin. Valmistelun yhteydessä kiinnitetään muutenkin huomiota perus- ja ihmisoikeuksien toteutumiseen.

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.

[43] OECD, 2015.
[44] EU komissio, 2013.

4.3 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. Taloudelliseen vahinkoon johtavan tietoturvariskin perimmäisenä syynä voi olla esim.:

1) virhe tekniikan suunnittelussa tai toiminnassa;
2) virhe sopimussuhteessa, (esimerkiksi 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 riskin liiketoiminnalle 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	suunnittelu- 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

Tietoturvakyvykkyyden perusta luodaan usein jo suunnitteluvaiheessa, esimerkiksi koodausalihankkijaa tai toteutusalustaa valittaessa. Seuraava kriittinen vaihe digitaalisten tietokoneohjelmien tietoturvariskien syntymisessä on ohjelman laatimisen hetki eli ohjelmien koodaus. Tässä vaiheessa 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 (esimerkiksi 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, niin sanottu 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.

Rajat ylittäviin tiedonsiirtoihin liittyvien riskien pienentäminen

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 niin sanotun 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 kollision ongelma on käynyt erittäin ilmeiseksi vuonna 2013 paljastuneissa tiedusteluviranomaisten massavalvontamenetelmissä. Useiden keskeisten teknologiayritysten johtajat ovat ilmaisseet huolensa massavalvonnasta ja erityisesti sen vaikutuksista asiakkaidensa luottamukseen[45].

Suomessa asiat ovat viranomaisnäkökulmasta varsin hyvällä mallilla. 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

[45] 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."*

omaa elämäänsä ilman viranomaisten tai muiden ulkopuolisten 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. [46] Monien maiden tapaan Suomessa onkin säädetty lakeja, jolla pyritään turvaamaan kansalaisten tietosuojaa henkilötietojen käsittelyssä ja sähköisessä viestinnässä. Ongelmia ei voida kuitenkaan ratkaista yksinomaan kansallisella lainsäädännöllä.

Suomen hallitus on katsonut, että EU:n digitaalisten sisämarkkinoiden toteutumisen edistämiseksi EU:ssa tulisi etsiä yhteisiä pelisääntöjä sille, missä määrin viestinnän luottamuksellisuutta voidaan rajoittaa toisen jäsenvaltion toimin[47]. EU:n sisämarkkinoiden toteutumisen, kansainvälisen kaupan sekä tiedon vapaan liikkuvuuden kannalta olisi hyvin ongelmallista, jos valtiot alkavat rajoittaa tiedon vapaata liikkuvuutta rajojen yli. Vaikutukset kohdistuisivat vääjäämättä tiedon lisäksi myös tavaroihin, palveluihin ja kokonaisiin liiketoimintamalleihin. Tällaisesta kehityksestä on jo merkkejä.

EU:n komissio antoi 25.8.2000 niin sanotun 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[48]. EU:n tuomioistuin kuitenkin katsoi 6.10.2015 antamassaan niin sanotun Schrems-tapauksen tuomiolauselmassa, että kyseinen Safe Harbour -päätös on pätemätön[49]. Tuomioistuin totesi, että Yhdysvaltojen kansalliseen turvallisuuteen, yleiseen etuun ja lakien noudattamiseen liittyvät vaatimukset ovat Safe Harbour -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. Komissio ja Yhdysvallat ilmoittivat 2.2.2016 päässeensä sopuun Privacy Shield -tietosuojasopimuksesta, joka korvasi Safe Harbour -sopimuksen. Sopimusneuvotteluista saatujen tietojen mukaan Yhdysvallat on luvannut olla harjoittamatta kohdentamatonta eurooppalaisten massavalvontaa ja se on antanut sitovan vakuutuksensa siitä, että viranomaisten pääsyä eurooppalaisten henkilötietoihin kansallisen turvallisuuden perusteella rajoitetaan[50].

EU neuvottelee useiden eri maiden kanssa kauppasopimuksista, joihin sisältyy muun muassa sääntelyyn ja yritysten liiketoimintaympäristön parantamiseen liittyviä määräyksiä eri sektoreilla. Suomen neuvottelukannat valmistellaan tiiviissä yhteistyössä toimivaltaisten ministeriöiden ja eri sidosryhmien kanssa. Suomi vaikuttaa komissioon, joka neuvottelee EU:n kauppasopimuksista yhteisesti sovittujen kantojen pohjalta. Suomen tulisi kauppaneuvotteluissa kiinnittää huomiota erityisesti siihen, ettei kauppasopimuksilla rajoiteta sopimusosapuolten sääntelyoikeutta tilanteissa, joissa sen katsotaan olevan tarkoituksenmukaista. Strategian tavoitteet huomioiden esimerkiksi salaustuotteiden käyttöön, ICT-tuotteiden auditointeihin tai kansalaisten perusoikeuksiin kohdistuviin rajoituspyrkimyksiin tulisi kiinnittää erityistä huomiota Suomen kantoja muodostettaessa.

[46] Perustuslain 10 ja 22 §:t sekä HE 309/1993 vp.
[47] Hallituksen selvitys eduskunnalle 12.6.2015, E21/2015 vp.
[48] Komission päätös 520/2000.
[49] EU:n tuomioistuimen 6.10.2015 antama ratkaisu asiassa C-362/14.
[50] Komission lehdistötiedote 2.2.2016.

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.

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.

4.4 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 prosentissa tapauksia tahattomasta teosta. Toisaalta on kuitenkin arvioitu, että tahallisten tietoturvaloukkausten aiheuttamat vahingot olisivat suuruudeltaan merkittävämpiä[51]. 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 tämä kehitys 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.

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

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.

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 palveluntarjoajaan, sen käyttäjään tai toiseen 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.

4.5 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. Poliisi tekee Viestintäviraston kanssa tiivistä yhteistyötä tietoverkkorikosten selvittämisen lisäksi myös tietoverkkorikosten ennaltaehkäisemiseksi ja tilannetietoisuuden parantamiseksi.

Tietoturvaan liittyvä osaaminen

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

Kryptologisten menetelmien hallinta edellyttää kehittyneitä matemaattisia valmiuksia. Kryptologian opetus ja tutkimus Suomalaisissa yliopistoissa ja korkeakouluissa vaikuttaa olevan verrattain ohutta osaajien kysyntään nähden. Myös muulle teknologiselle osaamiselle sekä liiketaloudelliselle ja oikeudelliselle osaamiselle on tarvetta. EU:n tietosuoja-asetuksen ja verkko- tietoturvadirektiivin myötä tietosuojaan ja tietoturvaan liittyvän osaamisen kysyntä oletettavasti kasvaa.

Oikeanlaisten osaajien löytäminen on osoittautunut alan toimijoille haastavaksi myös siksi, etteivät parhaat osaajat välttämättä tule perinteisiä koulutusväyliä pitkin. Esimerkiksi osa huipputason koodareista saattaa olla täysin itseoppineita. Erityisesti tietoturva-ala onkin pyrkinyt käyttämään rekrytoinneissa myös perinteisestä poikkeavia keinoja ja yritykset ovat kehitelleet myös omia koulutusohjelmiaan potentiaalisille työntekijöille.

Tietoturvariskien vakuuttaminen

Tietoturvariskien aiheuttamien vakuutusten markkinat ovat Suomessa ja Euroopassa vielä verrattain kehittymättömiä, 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 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 standardointitekniikoita 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 kuluessa, voidaan sopimuksessa edellyttää, että tuotteeseen tehtävistä muutoksista ilmoitetaan auditoijalle, joka arvioi muutosten vaikutukset sopimuksessa määriteltäviin vaatimuksiin.

4.6 Lainsäädäntö

Strategian osana toteutettaisiin hyväksyntää vaille valmiina olevan EU:n verkko- ja tietoturvadirektiiviehdotuksen edellyttämät lainsäädäntömuutokset[52]. Samalla arvioitaisiin kansallisen sääntelyn vaikutukset kansalaisten ja yritysten mahdollisuuksiin hyödyntää tietotekniikan mahdollistamia palveluja sekä liiketoimintamalleja turvallisesti ja tiedonkäsittelyyn liittyvät riskit halliten.

Sisämarkkinoiden toimivuuden parantamisen tähtäävä EU:n verkko- ja tietoturvadirektiiviehdotus edellyttää, että kunkin jäsenvaltion tulee laatia kansallinen strategia, jossa määritellään puitteet, visio, tavoitteet ja painopisteet verkko- ja tietoturvallisuudesta kansallisella tasolla. Direktiiviehdotuksen neuvottelut ovat loppusuoralla ja käytännössä direktiivi odottaa enää EU:n ministerineuvoston hyväksyntää.

Suomen oikeusjärjestyksen mukaisena lähtökohtana voidaan pitää sitä, että verkko- ja tietoturvallisuuden puitteet, tavoitteet ja painopisteet määritellään ensisijaisesti voimassaolevassa lainsäädännössä. Perustuslain oikeusvaltioperiaate esimerkiksi edellyttää, että julkisen vallan käytön tulee perustua lakiin, joten myös tietoturvaan liittyvien viranomaisvastuiden tulee perustua lainsäädäntöön. Strategiassa esitetään tiettyjä tavoitteita lainsäädännön laadun varmistamiseksi siltä osin kuin lainsäädännöllä voi olla vaikutuksia verkko- ja tietoturvallisuuteen ja sitä kautta digitaalisen liiketoiminnan kasvuympäristön kehittymiseen. Strategian toimenpiteiden yhteydessä on tunnistettu vastuullinen viranomais- tai muu taho. Vastuunjako perustuu nykyiseen lainsäädäntöön viranomaisten toimivaltuuksista.

Strategiatyön puitteet on määritelty pääministeri Juha Sipilän hallituksen hallitusohjelman toimintasuunnitelmassa ja esitelty strategian johdannossa. Strategian visio on laadittu näistä lähtökohdista kumpuavien tavoitteiden ja painopisteiden mukaiseksi.

Hallitusohjelman lisäksi strategian sisältöön vaikuttavat verkko- ja tietoturvadirektiiviehdotuksessa strategialle asetetut vaatimukset. Strategiassa tarkastellaan verkko- ja tietoturvadirektiiviehdotuksen edellyttämällä tavalla tietoturvaan

[52] Komission ehdotus Euroopan parlamentin ja neuvoston direktiiviksi verkko- ja tietoturvallisuuden korkean tason varmistamiseksi Euroopan unionin alueella (COM(2013)48 lopullinen - U13/2013 vp).

liittyvää osaamista ja yleisen tietoisuuden kehittämistä sekä tutkimus- ja kehitystyön merkitystä. Riskienhallinnan ja niiden tunnistamisen osalta strategian keskeinen viesti on, että toimijoilla on oltava mahdollisuus arvioida tietoturvatoimenpiteitään riskiperusteisesti eli suhteuttaa ne osaksi muiden riskien hallintaa. Julkisen ja yksityisen sektorin välistä yhteistyötä verkko- ja tietoturvallisuuteen liittyvässä ennaltaehkäisyssä, reagoinnissa ja korjaavissa toimenpiteissä on myös käsitelty useissa strategian toimenpiteissä.

Strategia on jatkumoa vuosien 2003 ja 2008 tietoturvastrategioille sekä vuoden 2013 kyberturvallisuustrategialle. Nyt laadittu strategia painottuu toimeksiantonsa mukaisesti erityisesti digitaaliseen liiketoimintaan sekä tulevasta verkko- ja tietoturvadirektiivistä seuraaviin strategisiin vaatimuksiin.

4.7 Valmistelu

Liikenne- ja viestintäministeriö asetti 28.9.2015 työryhmän tukemaan hallitusta luotettavan ja tietoturvallisen digitaalisen liiketoiminnan kasvuympäristön rakentamisessa. Työryhmässä oli laaja edustus liiketoiminnan tietoturvariskien hallintaan erikoistuneista yrityksistä ja järjestöistä. Työryhmä kokoontui viisi kertaa, järjesti kuulemistilaisuuden ja kuuli myös muita asiantuntijoita.

Kuulemistilaisuuden (15.12.2015) jälkeen strategialuonnoksesta oli mahdollisuus jättää kirjallisia kommentteja. Luonnosta kommentoi kirjallisesti yli 30 tahoa. Kirjallisen lausunnon toimittivat Aalto yliopisto, Cinia Group Oy, Cyber Trust -ohjelma, DigiSuomi2017, Elinkeinoelämän keskusliitto, Evira, FiCom, Finanssialan keskusliitto, Finnet, Fujitsu Finland Oy, Helsingin Kaupunki, Huoltovarmuuskeskus, Jyväskylän seudun kehittämisyhtiö, Kilpailu- ja kuluttajavirasto, KPMG Oy Ab, opetus- ja kulttuuriministeriö, Turvallisuuskomitean pysyvä sihteeristö, puolustusministeriö, SAK, Samlink, sisäministeriö, sosiaali- ja terveysministeriö, SSH Communications Security Oy, Suomen Erillisverkot, Tampereen yliopisto, TEKES, työ- ja elinkeinoministeriö, ulkoasiainministeriö, valtiovarainministeriö, VTT sekä Yrkehögskolan Arcada. Yksittäiset lausunnot löytyvät liikenne- ja viestintäministeriön verkkosivuilta.

Kuulemistilaisuudessa ja lausunnoissa ilmeni suurelta osin positiivinen näkökulma strategian laatimiseen ja työ luottamuksen edistämiseksi nähtiin tärkeänä ja tavoitteet kannatettavina. Lausunnoissa kiinnitettiin huomiota tietoturvastrategian otsikkoon ja rajaukseen etenkin siitä näkökulmasta, että strategia keskittyy vain elinkeinoelämän tietoturvallisuuden ja kilpailukyvyn edistämiseen. Lausunnoissa esitettiin, että strategiassa tulisi selventää tietoturvastrategian suhdetta kansalliseen kyberturvallisuusstrategiaan. Lausunnoissa kannatettiin tilannekuvan luomista ja sisäänrakennettua tietoturvaa koskevia kirjauksia. Kuulemistilaisuudessa ja lausunnoissa esitettiin ajatuksia tuotevastuun ulottamisesta ohjelmistoihin ja internetiin liitettävien laitteiden vähimmäisvaatimuksista.

Viranomaisten tiedonsaantioikeuksia koskevat kirjaukset jakoivat mielipiteitä sekä kuulemistilaisuudessa että kirjallisissa lausunnoissa. Viranomaisten ja yritysten yhteistyö nähtiin tärkeänä. Lausunnoissa esitettiin, että strategiassa tuotaisiin enemmän ”Public-Private partnership” -näkökulmaa

Tietoturvaa koskevan osaamisen parantaminen ja edistäminen nähtiin tärkeänä. Osaamisen osalta eräissä lausunnoissa kiinnitettiin huomiota myös siihen, osaaminen tulisi nähdä kokonaisuutena ja huomioida myös muu kuin tekninen osaaminen. Kriittisen infrastruktuurin ankkurointi Suomeen valtionomistuksen keinoin nähtiin joissain lausunnoissa hyvänä keinona tavoitteisiin pääsemiseen. Toisaalta lausunnoissa esiintyi

myös näkökulma, jonka mukaan valtionomistuksen lisääminen olisi vastoin yleistä kehitystä.

Lausunnoissa myös peräänkuulutettiin konkretiaa. Vastuutahoihin ja aikatauluihin toivottiin tarkennusta. Toisaalta nähtiin myös positiivisena, että lähestymistapa painottuu vahvasti liiketoimintanäkökulmiin ja katsottiin, että toimenpiteitä on ehdotettu kattavasti ja selkeästi. Lausunnoissa esitettiin muutamia konkreettisia ehdotuksia. Ehdotuksia tuli muun muassa koskien toimeenpanon mittausta, tutkimuksen suurempaa painottamista, kyberturvallisuuskeskuksen toimivaltuuksia sekä internetiin kytkettävien laitteiden rekisteröimisvelvoitteita. Kuulemistilaisuudessa ja lausuntokierroksella saatu palaute on pyritty huomioimaan strategian jatkovalmistelussa.

Lisäksi liikenne- ja viestintäministeriö kävi tarkentavia keskusteluja useiden ministeriöiden (muun muassa valtiovarainministeriön, työ- ja elinkeinoministeriön, ulkoasiainministeriön, oikeusministeriön, sisäministeriön ja puolustusministeriön) kanssa.