VALTIOVARAINMINISTERIÖ

OECD
BETTER POLICIES FOR BETTER LIVES

Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi

OECD:n suositus ja liiteasiakirja

Valtiovarainministeriön julkaisu – 28/2016

Julkisen hallinnon ICT

VALTIOVARAINMINISTERIÖ

OECD
BETTER POLICIES FOR BETTER LIVES

Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi

OECD:n suositus ja liiteasiakirja

Valtiovarainministeriön julkaisu – 28/2016

Tämän OECD asiakirjan suomenkielisestä käännöksestä vastaa yksinomaan Suomen valtiovarainministeriö. Virallisia ovat ainoastaan englannin- ja ranskankieliset tekstit, jotka ovat saatavilla OECD:n internet-sivuilla.

Julkisen hallinnon ICT

4041 0017
Painotuote

VALTIOVARAINMINISTERIÖ
PL 28 (Snellmaninkatu 1 A) 00023 VALTIONEUVOSTO
Puhelin 0295 16001 (vaihde)
Internet: www.vm.fi
Taitto: Valtioneuvoston hallintoyksikkö/
Tietotuki- ja julkaisuyksikkö/Anitta Türkkan

Lönnberg Print & Promo, 2016

Kuvailulehti

Julkaisija ja julkaisuaika	Valtiovarainministeriö, syyskuu 2016	
Tekijät	Alkuperäinen julkaisu: OECD. Suomenkielinen käännös: valtiovarainministeriö	
Julkaisun nimi	Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi	
Julkaisun osat/ muut tuotetut versiot	Julkaisun kieliversiot: Englanti: Digital Security Risk Management for Economic and Social Prosperity	
Asiasanat	Digitaalinen ympäristö, turvallisuus, riskit	
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja 28/2016	
Julkaisun myynti/jakaja	Julkaisu on saatavissa pdf-tiedostona osoitteesta www.vm.fi/julkaisut.	
Painopaikka ja -aika	Lönnberg Print & Promo, 2016	
ISBN 978- 952-251-789-0 (nid.) **ISSN** 1459-3394 (nid.) **ISBN** 978-952-251-790-6 (PDF) **ISSN** 1797-9714 (PDF)	**Sivuja** 72	**Kieli** Suomi

Tiivistelmä

Nykyisessä taloustilanteessa digitaalisesta ympäristöstä on tullut välttämätön kasvulle sekä vauraudelle, hyvinvoinnille ja osallisuudelle. Tämän vuoksi digitaaliseen turvallisuuteen kohdistuvia riskejä tulisi käsitellä laajemmasta taloudellisesta ja yhteiskunnallisesta näkökulmasta ja niiden hallinta tulisi sisällyttää sidosryhmien päätöksentekoprosesseihin.

VASTUUVAPAUSLAUSEKE

Tämä asiakirja ja siinä esiintyvät kartat eivät vaikuta minkään alueen statukseen tai suvereniteettiin, kansainvälisten rajojen määrittelyyn eivätkä alueiden tai kaupunkien nimiin.

Julkaisun viitetiedot:

OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris.
DOI: http://dx.doi.org/10.1787/9789264245471-en

Kuvat:

OECD:n julkaisujen korjausluettelo on saatavilla verkossa osoitteessa: www.oecd.org/publishing/corrigenda.

Alkuperäinen OECD:n julkaisu englanniksi ja ranskaksi otsikoilla:

Digital Security Risk Management for Economic and Social Prosperity. OECD Recommendation and Companion /La gestion du risque de sécurité numérique pour la prospérité économique et sociale. Recommandation de l'OCDE et document d'accompagnement

Esipuhe

Tämä OECD:n suositus, joka koskee digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi, sekä sen liiteasiakirja tarjoavat ohjeita digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa käsitteleviin uuden sukupolven kansallisiin strategioihin, joilla pyritään optimoimaan digitaalisesta avoimuudesta odotettavissa olevat taloudelliset ja yhteiskunnalliset hyödyt.

Digitaaliseen turvallisuuteen kohdistuvien uhkien ja poikkeamien määrä on kasvanut viime vuosina sekä johtanut merkittäviin taloudellisiin ja sosiaalisiin seurauksiin niin julkisille ja yksityisille organisaatioille kuin yksilöillekin. Tällaisia ovat esim. toiminnan keskeytyminen (palvelunestohyökkäyksen tai sabotaasin seurauksena), välittömät taloudelliset tappiot, oikeusjutut, maineelle aiheutuva vahinko, kilpailukyvyn menettäminen (esim. liikesalaisuuksien anastuksen yhteydessä) sekä asiakkaiden luottamuksen menetys. Kasvava määrä sidosryhmiä on tullut tietoiseksi tarpeesta hallita digitaaliseen turvallisuuteen kohdistuvia riskejä, jotta digitaalista taloutta voitaisiin hyödyntää.

OECD:llä on kolmen vuosikymmenen ajan ollut merkittävä rooli digitaalisen talouden innovaatiotoimintaa ja digitaaliseen talouteen koettua luottamusta koskevien periaatteiden ja säädösten edistäjänä. Tämä suositus, jonka OECD:n neuvosto on hyväksynyt 17.9.2015, on OECD:n digitaalisen talouden turvallisuutta ja yksityisyydensuojaa käsittelevän työryhmän [Working Party on Security and Privacy in the Digital Economy, SPDE] vuonna 2012 käynnistämän monisidosryhmäisen työskentelyn tulosta. Työryhmän toimeksiantona oli tarkastella neuvoston vuoden 2002 suositusta koskien tietojärjestelmien ja -verkkojen turvallisuutta [Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, turvallisuutta koskevat ohjeet].

Prosessiin osallistuivat poliittiset päättäjät, liike-elämä ja teollisuus, kansalaisyhteiskunta ja tekniikan alan yhteisö. Prosessia johti SPDE-työryhmän puheenjohtaja Jane Hamilton (Kanada) ja se sai aktiivista tukea OECD:n toimistolta. Työhön osallistuivat aktiivisesti myös OECD:n jäsenmaiden ja kumppanitalouksien edustustot sekä OECD:n liike-elämän ja teollisuuden neuvoa-antava komitea (Business and Industry Advisory Committee BIAC), kansalais- ja tietoyhteiskuntaa käsittelevä toimikunta (Civil Society Information Society Advisory Council CSISAC) ja Internetin tekninen neuvoa-antava komitea (Internet Technical Advisory Committee ITAC). Tarkistettua suositusta käsiteltiin ja se hyväksyttiin digitaalisen talouden politiikan komiteassa 25.6.2015, minkä jälkeen OECD:n neuvosto antoi sille lopullisen hyväksyntänsä.

Suosituksessa kehotetaan hallitusten sekä julkisten ja yksityisten organisaatioiden ylintä johtoa omaksumaan digitaaliseen turvallisuuteen kohdistuvien riskien hallinnassa lähestymistavan, joka rakentaa luottamusta ja hyödyntää avointa digitaalista ympäristöä taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi. Suosituksen kahdeksasta toisiinsa liittyvästä, toisistaan riippuvaisesta ja toisiaan täydentävästä korkean tason periaatteesta koostuva yhtenäinen kehys heijastaa tätä lähestymistapaa.

Suosituksessa toistuu kaksi keskeistä viestiä.

Ensimmäinen on keskittyminen julkisten ja yksityisten organisaatioiden taloudellisiin ja yhteiskunnallisiin tavoitteisiin sekä tarve omaksua riskienhallintaan perustuva lähestymistapa. Sen sijaan, että digitaalisia riskejä käsiteltäisiin teknisenä ongelmana, joka edellyttää teknisiä ratkaisuja, niihin tulisi suhtautua taloudellisina riskeinä ja niiden tulisi näin ollen sisältyä olennaisena osana organisaation yleisiin riskienhallinnan ja päätöksenteon prosesseihin. On torjuttava käsitys, että digitaaliseen turvallisuuteen kohdistuviin riskeihin tulisi vastata muista riskiluokista perustavanlaatuisesti poikkeavalla tavalla. Siksi termit ”kyberturvallisuus”, tai etuliite ”kyber-”, jotka auttoivat luomaan tätä harhaanjohtavaa erillisyyden vaikutelmaa, eivät esiinny tässä suosituksessa.

Toiseksi tunnustetaan, että turvallisuuteen kohdistuva riski voidaan dynaamisen hallinnan avulla pienentää kyseessä olevasta toiminnasta odotettaviin hyötyihin nähden hyväksyttäväksi katsottavalle tasolle. Digitaalisen turvallisuuden toimenpiteet tulisi suunnitella tavalla, joka huomioi toisten edut, on soveltuva ja oikeasuhteinen aiheutuviin riskeihin nähden, eikä tuota haittaa sille taloudelliselle ja yhteiskunnalliselle toiminnalle, jota toimenpiteillä pyritään suojelemaan.

Asiakirja käsittää sekä suosituksen että sen liiteasiakirjan, joka on luonteeltaan tarkentava ja havainnollistava. Liiteasiakirja ei ole osa neuvoston suositusta, vaikka ne on kehitelty tiiviissä yhteydessä toisiinsa. Liiteasiakirjassa käsitellään suositukseen sisältyviä avainkäsitteitä, kommentoidaan periaatteiden soveltamista eri sidosryhmiin ja myös selvitetään tarkemmin kutakin suosituksessa esitettyä periaatetta.

Suosituksen täytäntöönpanon odotetaan edistävän kokonaisvaltaisempaa yhteistä lähestymistapaa digitaaliseen turvallisuuteen kohdistuvien riskien hallintaan ja tuottavan uusia koordinointimekanismeja sekä hallitusten sisällä että hallitusten ulkopuolisten sidosryhmien kanssa. Sen odotetaan myös kannustavan laajempaan julkisen ja yksityisen sektorin yhteistyöhön niin kansallisella, alueellisella kuin kansainväliselläkin tasolla.

Neuvoston suositus koskien digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi

17.09.2015 – C(2015)115

NEUVOSTO, joka

OTTAA HUOMIOON OECD:stä 14 päivänä joulukuuta 1960 tehdyn yleissopimuksen ja erityisesti sen 1 artiklan b- ja c-kohdat, 3 artiklan a- ja b-kohdat sekä 5 artiklan b-kohdan;

OTTAA HUOMIOON neuvoston antaman suosituksen ohjeiksi, jotka koskevat yksityisyyden suojaamista ja henkilötietojen liikkumista rajojen yli [Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data] [C(80)58/LOPULLINEN MUUTOKSINEEN), yksityisyyden suojaa koskevat ohjeet]; neuvoston suosituksen ohjeiksi, jotka koskevat salauskäytäntöjä [Recommendation of the Council concerning Guidelines for Cryptography Policy [C(97)62/LOPULLINEN]; neuvoston suosituksen koskien elintärkeitä tietoinfrastruktuureja [Recommendation of the Council on the Protection of Critical Information Infrastructures [C(2008)35]; Internet-talouden tulevaisuutta koskevan julistuksen [Seoul Declaration, C(2008)99]; neuvoston suosituksen koskien Internet-politiikan suunnittelun periaatteita [Recommendation of the Council on Principles for Internet Policy Making [C(2011)154]; neuvoston suosituksen koskien sääntelypolitiikkaa ja hallintotapaa [Recommendation of the Council on Regulatory Policy and Governance [C(2012)37]; neuvoston suosituksen koskien digitaalisen hallinnon strategioita [Recommendation of the Council on Digital Government Strategies [C(2014)88]; ja neuvoston suosituksen koskien kriittisten riskien hallintajärjestelmää [Recommendation of the Council on the Governance of Critical Risks [C/MIN(2014)8/LOPULLINEN];

OTTAA HUOMIOON neuvoston suosituksen ohjeiksi, jotka koskevat tietojärjestelmien ja -verkkojen turvallisuutta [Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security [C(2002)131/LOPULLINEN], jonka tämä suositus korvaa;

TUNNUSTAA, että digitaalinen ympäristö, Internet mukaan lukien, on olennaisen tärkeä talouden ja yhteiskunnan toiminnalle, ja että se edistää kasvua, innovaatioita, hyvinvointia ja osallisuutta;

TUNNUSTAA, että digitaalisen ympäristön hyödyt kattavat kaikki talouden sektorit ja kaikki yhteiskunnallisen kehityksen osa-alueet, ja että nämä hyödyt ovat lähtöisin tieto- ja viestintätekniikoiden ja järjestelmien sekä erityisesti Internetin globaalista, avoimesta, verkottuneesta ja dynaamisesta luonteesta;

TUNNUSTAA, että digitaalisen ympäristön käyttöön, hallinnointiin ja kehittämiseen kohdistuu epävarmuuksia, jotka ovat luonteeltaan dynaamisia;

TUNNUSTAA, että digitaaliseen turvallisuuteen kohdistuvien riskien hallinta on joustava ja ketterä tapa puuttua näihin epävarmuuksiin ja saavuttaa odotetut yhteiskunnalliset ja taloudelliset hyödyt täysimääräisinä, tarjota tarpeellisia palveluja ja hallita elintärkeitä infrastruktuureja, säilyttää ihmisoikeudet ja perusarvot, sekä suojella ihmisiä digitaaliseen turvallisuuteen kohdistuvilta uhkilta;

KOROSTAA, että digitaaliseen turvallisuuteen kohdistuvien riskien hallinta tarjoaa tehokkaan perustan OECD:n yksityisyyden suojaa koskevissa ohjeissa esitetyn turvallisuustakuuperiaatteen toteuttamiselle ja korostaa myös yleisemmin, että tämä suositus ja OECD:n yksityisyyden suojaa koskevat ohjeet tukevat toisiaan;

TIEDOSTAA, että hallitukset, julkiset ja yksityiset organisaatiot sekä yksilöt jakavat asiayhteyteen ja rooliinsa perustuvan vastuun digitaaliseen turvallisuuteen kohdistuvien riskien hallinnasta sekä digitaalisen ympäristön suojelemisesta, ja että yhteistyö kansallisella, alueellisella ja kansainvälisellä tasolla on välttämätöntä.

Digitaalisen talouden politiikan komitean esityksestä neuvosto:

I. SUOSITTAA että jäsenmaat ja suosituksen hyväksyvät OECD:hen kuulumattomat maat (jäljempänä "suosituksen hyväksyvät maat");

1. Panevat täytäntöön osassa 1 esitetyt periaatteet (jäljempänä "periaatteet") kaikilla hallinnon tasoilla sekä julkisissa organisaatioissa;
2. Ottavat käyttöön osan 2 mukaisesti digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa koskevan kansallisen strategian.

II. KEHOTTAA hallitusten sekä julkisten ja yksityisten organisaatioiden ylintä johtoa omaksumaan digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan lähestymistavan luottamuksen rakentamiseksi sekä avoimen digitaalisen ympäristön hyödyntämiseksi taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämistä varten;

III. KANNUSTAA yksityisiä organisaatioita ottamaan periaatteet käyttöön omissa digitaaliseen turvallisuuteen kohdistuvien riskien hallintamenettelyissään;

IV. KANNUSTAA kaikkia sidosryhmiä panemaan periaatteet täytäntöön päätöksentekoprosesseissaan rooleihinsa, toimintakykyynsä ja toiminta-alueeseensa perustuen;

V. KEHOTTAA hallituksia sekä julkisia ja yksityisiä organisaatioita tekemään yhteistyötä vaikuttaakseen yksilöiden sekä pienten ja keskisuurten yritysten kykyyn yhteistoiminnassa hallita digitaaliseen turvallisuuteen kohdistuvia riskejä;

VI. TOTEAA, että periaatteet täydentävät toisiaan ja että niitä tulisi tarkastella kokonaisuutena, ja että ne on tarkoitettu sopimaan yhteen riskienhallintaa koskevien prosessien, parhaiden käytäntöjen, menettelytapojen ja standardien kanssa;

VII. TOTEAA lisäksi, että tässä suosituksessa:

1. Epävarmuuksien vaikutusta tavoitteisiin kutsutaan riskiksi. "Digitaaliseen turvallisuuteen kohdistuva riski" on ilmaisu, jota käytetään kuvailemaan riskiluokkaa, joka liittyy toiminnassa tapahtuvaan digitaalisen ympäristön käyttöön, kehittämiseen ja hallinnointiin. Riski voi aiheutua digitaalisen ympäristön uhkien ja haavoittuvuuksien yhdistelmästä. Se voi heikentää taloudellisten ja yhteiskunnallisten tavoitteiden saavuttamista haittaamalla toiminnan ja/tai ympäristön luottamuksellisuutta, eheyttä tai käytettävyyttä. Digitaaliseen turvallisuuteen kohdistuva riski on luonteeltaan dynaaminen. Se käsittää tekijöitä, jotka liittyvät digitaaliseen ja fyysiseen ympäristöön, toiminnassa mukana oleviin ihmisiin sekä toimintaa tukevaan organisatoriseen prosessiin.
2. Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta tarkoittaa organisaation sisällä ja/tai organisaatioiden välillä tehtäviä koordinoituja toimia, joiden tarkoituksena on puuttua digitaaliseen turvallisuuteen kohdistuvaan riskiin ja samalla maksimoida mahdollisuudet. Se on olennainen osa päätöksentekoa sekä taloudelliseen ja yhteiskunnalliseen toimintaan liittyvän riskienhallinnan viitekehystä. Se perustuu kokonaisvaltaisiin, systemaattisiin ja joustaviin prosesseihin, jotka ovat mahdollisimman avoimia ja yksikäsitteisiä. Nämä prosessit auttavat varmistamaan, että digitaaliseen turvallisuuteen kohdistuvien riskien hallinnassa käytettävät toimet ("turvatoimenpiteet") ovat soveltuvia ja oikeasuhteisia riskiin sekä kyseessä oleviin taloudellisiin ja yhteiskunnallisiin tavoitteisiin nähden.
3. Hallitukset, julkiset ja yksityiset organisaatiot sekä yksilöt, jotka käyttävät digitaalista ympäristöä taloudellisessa ja yhteiskunnallisessa toiminnassaan, ovat "sidosryhmiä". Sidosryhmillä voi olla useampi kuin yksi rooli. Hallitusten sekä julkisten ja yksityisten organisaatioiden ylimpään johtoon kuuluvista sidosryhmistä käytetään ilmaisua "johtajat ja päättäjät".

OSA 1. PERIAATTEET

Yleiset periaatteet

1. Tietoisuus, osaaminen ja vaikuttamismahdollisuudet

Kaikkien sidosryhmien tulisi ymmärtää digitaaliseen turvallisuuteen kohdistuvat riskit ja keinot niiden hallitsemiseksi.
Sidosryhmien tulisi tiedostaa, että digitaaliseen turvallisuuteen kohdistuva riski voi vaikuttaa heidän taloudellisten ja yhteiskunnallisten tavoitteidensa saavuttamiseen ja että keinot, joita he käyttävät riskin hallitsemiseen, voivat vaikuttaa toisiin. Heille tulisi antaa mahdollisuus hankkia riskin ymmärtämiseen tarvittava koulutus ja osaaminen, jotta he pystyisivät hallitsemaan riskiä sekä arvioimaan digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa koskevien päätöstensä mahdollisia vaikutuksia omaan toimintaansa ja digitaaliseen ympäristöön.

2. Vastuullisuus

Kaikkien sidosryhmien tulisi ottaa vastuuta digitaaliseen turvallisuuteen kohdistuvien riskien hallinnasta.
Sidosryhmien tulisi käyttäytyä vastuullisesti sekä vastata rooliensa, tehtävänsä ja toimintakykynsä puitteissa digitaaliseen turvallisuuteen kohdistuvien riskien hallinnasta sekä päätöstensä mahdollisten toisiin osapuoliin kohdistuvien vaikutusten huomioimisesta. Heidän tulisi tunnustaa, että taloudellisten ja yhteiskunnallisten tavoitteiden saavuttamiseksi on tarpeen hyväksyä tietyntasoinen digitaaliseen turvallisuuteen kohdistuva riski.

3. Ihmisoikeudet ja perusarvot

Kaikkien sidosryhmien tulisi hallita digitaaliseen turvallisuuteen kohdistuvia riskejä avoimesti sekä ihmisoikeus- ja perusarvomyönteisellä tavalla.
Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta tulisi toteuttaa tavalla, joka on linjassa demokraattisessa yhteiskunnassa tunnustettujen ihmisoikeuksien ja perusarvojen kanssa. Näitä ovat mm. ilmaisunvapaus, vapaa tiedonkulku, tietojen ja viestinnän luottamuksellisuus, yksityisyyden ja henkilötietojen suoja, avoimuus ja prosessien oikeudenmukaisuus. Digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan tulisi perustua eettiseen toimintaan, joka tunnustaa toisten sekä koko yhteiskunnan oikeutetut edut ja kunnioittaa niitä. Digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan käytännöissään ja menettelytavoissaan organisaatioiden tulisi noudattaa yleistä avoimuuden politiikkaa.

4. Yhteistyö

Sidosryhmien tulisi toimia yhteistyössä ja yhteistyön tulisi myös ulottua rajojen yli. Globaali verkottuneisuus tekee sidosryhmistä toisistaan riippuvaisia ja edellyttää siksi yhteistyötä digitaaliseen turvallisuuteen kohdistuvien riskien hallinnassa. Kaikki sidosryhmät tulisi sitouttaa yhteistyöhön, jonka tulisi tapahtua sekä hallitusten ja julkisten ja yksityisten organisaatioiden sisällä että niiden välillä ja myös yksilöiden kanssa. Yhteistyön tulisi lisäksi ulottua rajojen yli niin alueellisella kuin kansainväliselläkin tasolla.

Toimintaperiaatteet

5. Riskien arviointi ja riskien käsittelyprosessi

Johtajien ja päättäjien tulisi varmistaa, että digitaaliseen turvallisuuteen kohdistuvia riskejä käsitellään jatkuvan riskien arvioinnin periaatteella.
Digitaaliseen turvallisuuteen kohdistuvien riskien arvioinnin tulisi olla jatkuva ja systemaattinen prosessi, jossa arvioidaan uhkien ja haavoittuvuuksien mahdollisia vaikutuksia kyseessä olevaan taloudelliseen ja yhteiskunnalliseen toimintaan sekä hankitaan tietoa riskien käsittelyä koskevan päätöksentekoprosessin pohjaksi. Riskien käsittelyn tavoitteena tulisi olla riskien pienentäminen hyväksyttävälle tasolle toiminnasta odotettaviin taloudellisiin ja yhteiskunnallisiin hyötyihin nähden huomioiden samalla vaikutukset toisten oikeutettuihin etuihin. Riskien käsittelyyn on useita mahdollisia vaihtoehtoja: riskin hyväksyminen, pienentäminen, siirtäminen tai välttäminen sekä näiden yhdistelmät.

6. Turvatoimenpiteet

Johtajien ja päättäjien tulisi varmistaa, että turvatoimenpiteet ovat soveltuvia ja oikein mitoitettuja riskiin nähden.
Digitaaliseen turvallisuuteen kohdistuvien riskien arvioinnin tulisi ohjata turvatoimenpiteiden valintaa, käyttöä ja kehittämistä, jotta riskit voidaan pienentää niiden arvioinnissa ja käsittelyssä määritellylle hyväksyttävälle tasolle. Turvatoimenpiteiden tulisi olla soveltuvia ja oikein mitoitettuja, ja niiden valinnassa tulisi huomioida niiden mahdolliset kielteiset ja myönteiset vaikutukset taloudelliseen ja yhteiskunnalliseen toimintaan, jota toimenpiteillä on tarkoitus suojella, sekä myös vaikutukset ihmisoikeuksiin ja perusarvoihin ja toisten oikeutettuihin etuihin. Harkittaviksi tulisi ottaa niin fyysiset, digitaaliset kuin toiminnassa mukana oleviin ihmisiin, prosesseihin tai tekniikkaan liittyvät toimenpiteet. Organisaatioiden tulisi selvittää haavoittuvuudet ja puuttua niihin asianmukaisesti niin pian kuin mahdollista.

7. Innovaatiotoiminta

Johtajien ja päättäjien tulisi varmistaa innovaatiotoiminnan huomiointi.
Innovaatiotoiminnan tulisi olla olennainen osa digitaaliseen turvallisuuteen kohdistuvien riskien pienentämistä riskien arvioinnissa ja käsittelyssä määritellylle hyväksyttävälle tasolle. Innovaatiotoimintaa tulisi edistää sekä digitaalisessa ympäristössä tapahtuvan taloudellisen ja yhteiskunnallisen toiminnan suunnittelussa ja hoidossa että turvatoimenpiteiden suunnittelussa ja kehittämisessä.

8. Varautuminen ja jatkuvuus

Johtajien ja päättäjien tulisi varmistaa, että käytössä on valmius- ja jatkuvuussuunnitelma.
Valmius- ja jatkuvuussuunnitelma tulisi ottaa käyttöön digitaaliseen turvallisuuteen kohdistuvien riskien arvioinnin perusteella. Suunnitelman tarkoituksena on pienentää poikkeamien haitallisia vaikutuksia sekä tukea taloudellisen ja yhteiskunnallisen toiminnan jatkuvuutta ja häiriönsietokykyä. Suunnitelmassa tulisi määritellä keinot digitaalisen turvallisuuden poikkeamien estämiseksi ja havaitsemiseksi sekä niihin vastaamiseksi ja niistä toipumiseksi. Sen tulisi sisältää mekanismit, joilla määritellään digitaalisen turvallisuuden poikkeamien vaikutusten laajuuteen ja vakavuuteen perustuvat selkeät eskalaatiotasot. Vaikuttavana tekijänä tulisi niin ikään huomioida poikkeamien vaikutusten mahdollinen leviäminen myös toisiin digitaalisen ympäristön toimijoihin. Asianmukaiset ilmoitusmenettelyt tulisi sisällyttää suunnitelman täytäntöönpanoon.

OSA 2. KANSALLISET STRATEGIAT

A. Digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa koskevien kansallisten strategioiden tulisi noudattaa edellä mainittuja periaatteita ja luoda kaikille sidosryhmille edellytykset hallita taloudellista ja yhteiskunnallista toimintaa koskevia digitaaliseen turvallisuuteen kohdistuvia riskejä sekä edistää luottamusta digitaaliseen ympäristöön. Näiden strategioiden tulisi:

1. Saada hallituksen ylimmän tason tuki ja ilmentää selkeätä, koko hallinnon kattavaa toimintatapaa, joka on joustava, teknologianeutraali ja yhdenmukainen muiden taloudellista ja yhteiskunnallista hyvinvointia edistävien strategioiden kanssa.

2. Tuoda selvästi julki, että niillä pyritään hyödyntämään avointa digitaalista ympäristöä taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi vähentämällä digitaaliseen turvallisuuteen kohdistuvien riskien tasoa rajojen sisällä ja rajat ylittävästi kuitenkaan tarpeettomasti rajoittamatta tekniikan, viestinnän ja datan kulkua; ja että

niillä pyritään myös varmistamaan olennaisten palvelujen tarjonta sekä elintärkeän infrastruktuurin toiminta yksilöiden suojelemiseksi digitaaliseen turvallisuuteen kohdistuvilta uhkilta huomioiden samalla tarve varmistaa kansallinen ja kansainvälinen turvallisuus sekä ihmisoikeudet ja perusarvot.

3. Olla suunnattuja kaikille sidosryhmille ja tarvittaessa räätälöityjä pienten ja keskisuurten yritysten sekä yksilöiden tarpeisiin, ja myös ilmaista selkeästi sidosryhmien vastuut ja velvollisuudet niiden roolien, toimintakyvyn ja toiminnan sisällön mukaisesti.

4. Perustua koordinoituun hallituksen sisäiseen lähestymistapaan sekä kaikki sidosryhmät käsittävään avoimeen ja läpinäkyvään prosessiin. Strategiat tulisi myös tarkistaa säännöllisin väliajoin ja niitä tulisi kehittää kokemusten ja parhaiden käytäntöjen pohjalta hyödyntäen käytettävissä olevia kansainvälisesti vertailukelpoisia mittareita.

B. Kansallisiin strategioihin tulisi sisältyä toimia, joilla hallitukset voivat:

1. **Johtaa esimerkillään** erityisesti seuraavilla tavoilla:

i). Ottamalla käyttöön kattavan kehyksen digitaaliseen turvallisuuteen kohdistuvien riskien hallitsemiseksi hallituksen omassa toiminnassa. Hallituksen toimintaan ja käytökseen kohdistuvan luottamuksen lisäämiseksi kehyksen ja sitä toteuttavien linjausten tulisi olla läpinäkyviä myös tunnistettujen digitaalisen turvallisuuden haavoittuvuuksien sekä niihin liittyvien kehitystoimien vastuullisen julki tuomisen osalta;

ii). Luomalla asianomaisten hallintotoimijoiden väliset koordinaatiomekanismit, jotta voidaan varmistaa, että niiden toimet digitaaliseen turvallisuuteen kohdistuvien riskien hallinnassa ovat yhteensopivia sekä edistävät taloudellista ja yhteiskunnallista hyvinvointia;

iii). Varmistamalla yhden tai useamman tietoturvaloukkauksiin reagoivan ja niitä tutkivan yksikön perustaminen kansallisella tasolla (Computer Security Incident Response Team, CSIRT); näistä käytetään myös nimeä Computer Emergency Response Teams, (CERT) ja tarvittaessa edistämällä myös yhteistyössä rajojen sisällä ja yli toimivien julkisten ja yksityisten CSIRT/CERT-yksiköiden syntymistä;

iv). Käyttämällä markkina-asemaansa digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan edistämiseksi talouselämässä ja yhteiskunnassa. Keinoina tähän voivat olla mm. julkiset hankintamenettelyt sekä asianmukaisen pätevän riskienhallinnan henkilöstön rekrytointi;

v). Kannustamalla digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan kansainvälisten standardien ja parhaiden käytäntöjen käyttöönottoon ja edistämällä niiden kehittämistä ja tarkistamista avoimien ja läpinäkyvien sekä monia sidosryhmiä osallistavien prosessien avulla;

vi). Ottamalla käyttöön innovatiivista turvallisuustekniikkaa digitaaliseen turvallisuuteen kohdistuvien riskien hallinnassa sen varmistamiseksi, että tietoja suojataan asianmukaisesti niin säilytyksen kuin välityksen aikana, sekä huomioimalla asianmukaisten tietojen keräämistä ja säilyttämistä koskevien rajoitusten hyödyt;

vii). Koordinoimalla ja edistämällä digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa koskevaa julkista tutkimusta ja kehitystyötä erityisesti innovaatiotoiminnan edistämiseksi;

viii). Tukemalla digitaaliseen turvallisuuteen kohdistuvien riskien hallintaan kykenevän ammattitaitoisen työvoiman kehittymistä varsinkin sisällyttämällä tällaisen riskienhallinnan koulutusta osaksi laajempia koulutusstrategioita. Hallitus voi mm. edistää työssä toteutettavan riskienhallintaa koskevan koulutus- ja sertifiointijärjestelmän kehittämistä sekä käyttää kansallisia opetusohjelmia keinona tukea koko väestön digitaalisen osaamisen kehittymistä erityisesti osana korkeakoulutusta;

ix). Ottamalla käyttöön ja toimeenpanemalla kattavan tietoverkkorikollisuuden vähentämistä koskevan ohjelman, joka pohjautuu olemassa oleviin kansainvälisiin säädöksiin;

x). Kohdentamalla riittävät resurssit strategian tehokkaaseen toteuttamiseen.

2. Vahvistaa kansainvälistä yhteistyötä ja keskinäistä avunantoa erityisesti seuraavilla tavoilla:

i). Osallistumalla asianomaisiin alueellisiin ja kansainvälisiin foorumeihin, luomalla kahden- ja monenvälisiä suhteita kokemusten ja parhaiden käytäntöjen jakamiseksi sekä edistämällä kansallisessa digitaaliseen turvallisuuteen kohdistuvien riskien hallinnassa menettelytapoja, jotka eivät kasvata muihin maihin kohdistuvia riskejä;

ii). Tarjoamalla tarvittaessa vapaaehtoispohjalta avunantoa ja tukea muille maille sekä luomalla kansallisia yhteyspisteitä digitaaliseen turvallisuuteen kohdistuvien riskien hallintaan liittyvien rajat ylittävien pyyntöjen oikea-aikaista käsittelyä varten;

iii). Työskentelemällä kotimaisiin ja rajat ylittäviin uhkiin vastaamisen kehittämiseksi mm. CSIRT-yksiköiden yhteistyön ja yhteisten harjoitusten sekä muiden yhteistyökeinojen avulla.

3. Tehdä yhteistyötä muiden sidosryhmien kanssa erityisesti seuraavilla tavoilla:

i). Selvittämällä keinoja, joilla hallitukset ja muut sidosryhmät voivat auttaa toisiaan parantamaan digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa toiminnassaan;

ii). Tunnistamalla hallituksen linjausten mahdolliset kielteiset vaikutukset toisten sidosryhmien toimintaan tai taloudelliseen ja yhteiskunnalliseen hyvinvointiin kansallisella tasolla sekä puuttumalla näihin vaikutuksiin;

iii). Kehittämällä suuren yleisön tietoon tuotavia käytäntöjä ja menettelytapoja digitaaliseen turvallisuuteen kohdistuvien riskien hallitsemiseksi;

iv). Kannustamalla sidosryhmiä toimimaan vastuullisesti digitaaliseen turvallisuuteen kohdistuvien haavoittuvuuksien havaitsemisessa, ilmoittamisessa ja/tai korjaamisessa;

v). Nostamalla tietoisuuden, osaamisen ja vaikutusmahdollisuuksien tasoa yhteiskunnassa digitaaliseen turvallisuuteen kohdistuvien riskien hallitsemiseksi eri sidosryhmien tarpeisiin räätälöityjen teknologianeutraalien hankkeiden avulla.

4. Luoda kaikille sidosryhmille edellytykset tehdä yhteistyötä digitaaliseen turvallisuuteen kohdistuvien riskien hallinnassa erityisesti seuraavilla tavoilla:

i). Edistämällä sidosryhmien aktiivista osallistumista yhteisiin virallisiin ja vapaamuotoisiin hankkeisiin ja kumppanuuksiin kansallisella, alueellisella ja kansainvälisellä tasolla niin yksityisellä sektorilla kuin julkisen ja yksityisen sektorin välilläkin. Tavoitteena on:

- Digitaaliseen turvallisuuteen kohdistuvien riskien hallintaan liittyvien tietojen, osaamisen, toimivien kokemusten ja käytäntöjen jakaminen sekä toimintalinjausten että käytännön tasolla;
- Digitaaliseen turvallisuuteen kohdistuvien riskien hallintaan liittyvien tietojen vaihtaminen;
- Tulevaisuuden haasteiden ja mahdollisuuksien ennakointi ja niihin varautuminen.

ii). Edistämällä sidosryhmien välistä yhteistyötä haavoittuvuuksien ja uhkien tunnistamisen ja korjaamisen kehittämiseksi sekä digitaaliseen turvallisuuteen kohdistuvien riskien pienentämiseksi;

iii). Kannustamalla sidosryhmiä tekemään yhteistyötä, jolla pyritään suojelemaan yksilöitä sekä pieniä ja keskisuuria yrityksiä digitaaliseen turvallisuuteen kohdistuvilta uhkilta sekä parantamaan heidän valmiuksiaan hallita omaan taloudelliseen ja yhteiskunnalliseen toimintaansa liittyviä digitaaliseen turvallisuuteen kohdistuvia riskejä;

iv). Tarjoamalla sidosryhmille tarvittaessa kannustimia digitaaliseen turvallisuuteen kohdistuvien riskien hallitsemiseksi sekä markkinoiden läpinäkyvyyden ja tehokkuuden lisäämiseksi;

v). Kannustamalla innovaatiotoimintaa digitaaliseen turvallisuuteen kohdistuvien riskien hallinnassa sekä sellaisten välineiden kehittämisessä, joiden avulla yksilöt ja organisaatiot voivat suojata toimintaansa digitaalisessa ympäristössä;

vi). Kannustamalla tarvittaessa yhteisiin mittausmenetelmiin, standardeihin ja parhaisiin käytäntöihin perustuvien kansainvälisesti vertailukelpoisten mittareiden kehittämiseen digitaaliseen turvallisuuteen kohdistuvan riskien hallinnan toimivuuden, tehokkuuden ja avoimuuden parantamiseksi.

VIII. SUOSITTELEE, että suosituksen hyväksyvät maat tekevät yhteistyötä tämän suosituksen täytäntöönpanossa sekä tiedottavat suosituksesta julkista ja yksityistä sektoria, suositusta hyväksymättömiä maita sekä kansainvälisiä foorumeja;

IX. KUTSUU OECD:hen kuulumattomia maita hyväksymään tämän suosituksen;

X. OHJEISTAA digitaalisen talouden politiikan komiteaa tarkastelemaan tämän suosituksen täytäntöönpanoa sekä antamaan neuvostolle raporttinsa kolmen vuoden kuluttua suosituksen hyväksymisestä sekä sen jälkeen tarvittaessa.

* * *

Liiteasiakirja OECD:n neuvoston suositukseen koskien digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi

Liiteasiakirja on luonteeltaan tarkentava ja havainnollistava. Se ei sisälly neuvoston suositukseen, joka koskee digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi.

Sisällys

Johdanto

Viimeksi kuluneen vuosikymmenen aikana tieto- ja viestintätekniikasta (ICT) Internet mukaan lukien on tullut olennainen tekijä talouden toimivuudelle sekä merkittävä kehityksen veturi kaikilla aloilla. Hallitukset, julkiset ja yksityiset organisaatiot sekä myös yksilöt ovat ydintoiminnassaan tulleet riippuvaisiksi digitaalisesta ympäristöstä. Ne kohtaavat kuitenkin yhä enenevässä määrin digitaalisen ympäristön käyttöön liittyviä epävarmuustekijöitä. Digitaaliseen turvallisuuteen kohdistuvien uhkien ja poikkeamien määrä on lisääntynyt, millä on ollut merkittäviä taloudellisia sekä yksityisyydensuojaan ja maineeseen liittyviä seuraamuksia. Joissakin tapauksissa on aiheutunut jopa aineellista vahinkoa. Vaikka sidosryhmät ovat yhä tietoisempia digitaaliseen turvallisuuteen kohdistuvien riskien aiheuttamista haasteista, asiaa lähestytään usein yksinomaan teknisestä näkökulmasta tavalla, joka on erillään taloudellisesta ja yhteiskunnallisesta päätöksenteosta. On tullut ajankohtaiseksi selventää, että digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan tulisi sisältyä olennaisena osana taloudelliseen ja yhteiskunnalliseen päätöksentekoon sen varmistamiseksi, että sidosryhmät voisivat täysimääräisesti hyödyntää digitaalisen ympäristön tarjoamia mahdollisuuksia.

Digitaaliseen turvallisuuteen liittyviin asioihin viitataan usein yleiskäsitteellä "kyberturvallisuus", joka kattaa kaikki digitaalisen turvallisuuden ulottuvuudet. Näitä ulottuvuuksia ovat mm. tekniset, taloudelliset ja yhteiskunnalliset, oikeudelliset, lainvalvonnalliset ja ihmisoikeudelliset sekä kansalliseen turvallisuuteen, sodankäyntiin, kansainväliseen vakauteen ja tiedustelutoimintaan liittyvät näkökohdat. Kyberturvallisuus-käsitteen yleinen käyttö usein hämärtää aihepiirin laajuutta ja monitahoisuutta. Digitaalista turvallisuutta voidaan lähestyä ainakin neljästä eri näkökulmasta, joista jokainen on lähtöisin omanlaisestaan kulttuurista ja taustasta, vakiintuneista käytännöistä ja tavoitteista:

- ***teknologia*** eli keskittyminen digitaalisen ympäristön toimintaan (josta asiantuntijat usein käyttävät sanoja "tietoturvallisuus" tai "verkkoturvallisuus")

- ***lainvalvonta*** sekä oikeudelliset näkökohdat laajemminkin (esim. tietoverkkorikollisuus)

- ***kansallinen ja kansainvälinen turvallisuus*** käsittäen mm. tieto- ja viestintätekniikoiden roolin tiedustelutoiminnassa, konfliktintorjunnassa, sodankäynnissä jne.

- ***taloudellinen ja yhteiskunnallinen hyvinvointi***, joka käsittää vaurauden luomisen, innovaatiotoiminnan, kasvun, kilpailukyvyn ja työllisyyden kaikilla talouden osa-alueilla,[1] sekä eri näkökulmat kuten yksilönvapaudet, terveys[2], koulutus[3], kulttuuri, demokraattinen osallistuminen, tiede, vapaa-aika ja muut hyvinvoinnin ulottuvuudet, joissa digitaalinen ympäristö toimii kehityksen veturina.

OECD:n mandaattina on edistää "parempaa politiikkaa parempaa elämää varten" ja näin ollen OECD lähestyy digitaaliseen turvallisuuteen kohdistuvia riskejä taloudellisesta ja yhteiskunnallisesta näkökulmasta.

Vuonna 2015 OECD:n neuvosto[4] hyväksyi neuvoston suosituksen digitaaliseen turvallisuuteen kohdistuvien riskien hallinnasta taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi [Recommendation of the Council on Digital Security Risk Management for Economic and Social Prosperity, jäljempänä suositus] osana laajempaa digitaaliseen talouteen liittyvien suositusten, ohjeiden ja analyysien kokonaisuutta.[5] Yli kahden vuoden ajan työstetty suositus rakentuu OECD:n kolmen vuosikymmenen kokemukselle digitaalisen talouden innovaatiotoimintaa ja luottamusta koskevien linjausten ja välineiden kehittämisessä, alkaen neuvoston vuonna 1980 antamasta suosituksesta ohjeiksi, jotka koskevat yksityisyyden suojaamista ja henkilötietojen liikkumista rajojen yli [Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, "yksityisyydensuojaa koskevat ohjeet", joita on muutettu vuonna 2013] (OECD, 2013b), sekä mm. salaustekniikkakäytäntöihin, sähköiseen tunnistamiseen ja elintärkeisiin tietoinfrastruktuureihin (OECD 2008) liittyviä säädöksiä. Nykyinen suositus korvaa vuoden 2002 neuvoston suosituksen ohjeiksi, jotka koskevat tietojärjestelmien ja verkkojen turvallisuutta [Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, "turvallisuutta koskevat ohjeet"] (OECD, 2002), joka puolestaan korvasi vuoden 1992 neuvoston suosituksen tietojärjestelmien turvallisuutta koskeviksi ohjeiksi [Recommendation of the Council concerning Guidelines for the Security of Information Systems, "ensimmäiset turvallisuutta koskevat ohjeet"]. Se edustaa näin ollen kolmatta kypsyysvaihetta, joka heijastaa digitaalisen talouden kehitystä ja varsinkin sen elintärkeätä roolia talouden ja yhteiskunnan toimivuudelle ja kehitykselle.

Suositukset ovat järjestön oikeudellisesti sitomattomia säädöksiä. Koska ne edustavat jäsenvaltioiden poliittista tahtoa, niille on käytännössä kuitenkin muodostunut merkittävä moraalinen vaikutusvalta. Jäsenmaiden ja suositukset hyväksyvien, järjestöön kuulumattomien maiden odotetaan tekevän parhaansa pannakseen suositukset täysimääräisesti täytäntöön.[6] Tämän suosituksen taustalla on konsensus, jonka syntymiseen vaikuttavaan monisidosryhmäiseen yhteistyöhön osallistuivat poliittiset päättäjät, liike-elämä ja teollisuus, kansalaisyhteiskunta sekä tekniikan alan yhteisö.[7] Myös OECD:hen kuulumattomia maita kannustetaan ottamaan suosituksesta vaikutteita kehittäessään kansallisia strategioitaan riippumatta siitä, tekevätkö ne muodollista päätöstä sen hyväksymisestä. Julkisia ja yksityisiä organisaatioita kehotetaan myös huomioimaan suosituksen periaatteet omissa riskienhallinnan viitekehyksissään. Muiden kansainvälisten ja alueellisten organisaatioiden toivotaan niin ikään huomioimaan suositus omassa työssään ja toiminnassaan, ja niitä itse asiassa kannustetaan tekemään näin.[8]

Suosituksessa tunnustetaan, että yllä mainitut eri ulottuvuudet (taloudellinen, yhteiskunnallinen, tekninen, lainvalvonta sekä kansalliseen ja kansainväliseen turvallisuuteen liittyvä) kietoutuvat yhtä lailla toisiinsa niin digitaalisessa ympäristössä kuin sen ulkopuolellakin. Hallitusten tulisi siksi pyrkiä lähestymään digitaaliseen turvallisuuteen kohdistuvien riskien eri ulottuvuuksia koko hallinnon kattavalla tavalla, jossa pyritään yhdenmukaisuuteen, täydentävyyteen ja keskinäiseen vahvistamiseen.

Tältä osin suosituksessa kehotetaan hallituksia hyväksymään kansallinen strategia digitaaliseen turvallisuuteen liittyvien riskien hallitsemiseksi (I.2). Ohjelmalla tulee olla hallituksen ylimmän tason tuki (osa 2. A. 1) keskenään kilpailevien poliittisten tavoitteiden asianmukaiseksi tasapainottamiseksi. Suosituksen täytäntöönpanon odotetaan edistävän digitaalisen turvallisuuden eri näkökulmia käsittelevien asiantuntijoiden välistä yhteistyötä niin kansallisella, alueellisella kuin kansainväliselläkin tasolla.

On tärkeätä korostaa, että suositus samoin kuin OECD:n työ tällä alalla laajemminkin on osa useiden järjestöjen kesken käytävää kansainvälistä vuoropuhelua. Niiden toisiaan täydentävä työ heijastaa kunkin nimenomaista mandaattia. Euroopan neuvosto esimerkiksi käsittelee tietoverkkorikollisuuteen liittyviä asioita (esim. vuoden 2001 verkkorikollisuutta koskeva yleissopimus eli Budapestin yleissopimus).[9] Interpol edistää operatiivista lainvalvontayhteistyötä[10], kun taas YK[11] ja Euroopan turvallisuus- ja yhteistyöjärjestö (ETYJ)[12] keskustelevat valtioiden toiminnasta digitaalisessa ympäristössä sekä luottamusta rakentavista toimista kansainvälisen vakauden ylläpitämiseksi. Teknisiä standardeja kehitetään useallakin taholla. Näitä ovat mm. Kansainvälinen standardointijärjestö ISO, Internet Engineering Task Force (IETF) -yhteisö, World Wide Web Consortium (W3C) ja Organization for the Advancement of Structured Information Standards (OASIS). Alueellisilla organisaatioilla kuten Aasian ja Tyynenmeren maiden talousjärjestöllä (APEC)[13] on myös merkittävä rooli parhaiden käytäntöjen ja ohjeiden toimeenpanon edistäjinä.

Suositus alkaa johdanto-osalla (”Ottaa huomioon”, ”Toteaa”, jne.). Sitten tulevat neuvoston (jäljempänä ”OECD”) hallituksille ja muille sidosryhmille antamat numeroidut suositukset (esim. ”I. Suosittelee…”, ”II. Kehottaa…” jne.). Seuraavaksi annetaan periaatteita koskevaa tietoa (esim. ”VI. Toteaa…” jne.) sekä selvennetään terminologiaa (esim. ”VII Toteaa lisäksi…” jne.). Tässä osiossa OECD kehottaa niin hallitusten kuin julkisten ja yksityisten organisaatioiden ylintä johtoa omaksumaan digitaaliseen turvallisuuteen kohdistuvien riskien hallinnassa lähestymistavan, joka rakentaa luottamusta ja hyödyntää avointa digitaalista ympäristöä taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi (II).

Osassa 1 esitellään yhtenäinen viitekehys, joka koostuu kahdeksasta digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa koskevasta, toisiinsa liittyvästä, toisistaan riippuvaisesta ja toisiaan täydentävästä korkean tason periaatteesta (jäljempänä ”periaatteet”). OECD suosittelee, että suosituksen hyväksyvät maat panisivat nämä periaatteet täytäntöön kaikilla hallinnon tasoilla[14] sekä julkisissa organisaatioissa (I.1) OECD myös kannustaa yksityisiä organisaatioita, yritykset ja voittoa tavoittelemattomat yhteisöt mukaan lukien, omaksumaan nämä periaatteet digitaaliseen turvallisuuteen kohdistuvien riskien hallinnassa (III) ja toteuttamaan niitä päätöksentekoprosesseissaan rooliensa, toimintakykynsä ja toimintakenttänsä perusteella[15] (IV).

Periaatteita voidaan näin ollen välittömästi käyttää ohjaamaan julkisia ja yksityisiä organisaatioita niiden liiketaloudellisen tai organisatorisen riskienhallintamenettelyiden kehittämisessä tai välillisesti innoittamaan kansallisen strategian ja siihen liittyvien linjausten kehittämisessä. Tarkemmin sanoen suosituksessa kehotetaan sen hyväksyviä maita ottamaan käyttöön digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa koskeva kansallinen strategia, joka perustuu suosituksen osassa 2 annettuihin ohjeisiin. Vaikka osa 2 esitetään rakenteeltaan erilaisena, se on kehitelty periaatteiden pohjalta.

Yleisesti ottaen suositus on kohdistettu ylimmälle johdolle (”johtajat ja päättäjät”), joilla on parhaat edellytykset vaikuttaa asianmukaisen digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa koskevan viitekehyksen käyttöönottoon organisaatioissa sekä taloudellista ja yhteiskunnallista hyvinvointia edistävän kansallisen strategian käyttöönottoon hallituksissa.

Suosituksen laatimisen alkuvaiheista lähtien OECD:n edustustot ovat tunnistaneet aihepiirin monitahoisuuden sekä tarpeen edesauttaa suosituksen täytäntöönpanoa luomalla taustatietoja ja selventävää aineistoa tarjoava erillinen asiakirja. Edustustot ovat myös olleet yhtä mieltä siitä, että tämän liiteasiakirjan olisi oltava lyhyt ja että siinä tulisi käsitellä vain digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan olennaisimpia kohtia. Näin ollen liiteasiakirjan tulisi keskittyä vain suosituksen osaan 1. Jatkotyöskentelyn kuluessa olisi mahdollista käsitellä yksityiskohtaisemmin joitakin tässä liiteasiakirjassa tunnistettuja ongelmia sekä suosituksen osan 2 heijastamaa tarvetta julkisten periaatteiden ohjaukseen. Liitteessä esitetään joukko mahdollisia jatkotyöskentelyn aihealueita, jotka ovat nousseet esiin tässä liiteasiakirjassa sekä konsultaatio- ja laatimisprosessin kuluessa.

Tässä asiakirjassa kuvaillaan ensin lyhyesti taustaa. Sitten käsitellään suosituksen avainkäsitteitä ja kommentoidaan periaatteiden soveltamista sidosryhmissä. Lopuksi kuvataan yksityiskohtaisemmin kutakin kahdeksasta periaatteesta.

Taustaa

Julkisten ja yksityisten organisaatioiden johtajat ja päättäjät ovat havahtumassa siihen, että innovaation, tuottavuuden ja kasvun ajurina toimimisen ohella digitaalinen ympäristö tuottaa myös epävarmuutta, joka saattaa vaarantaa taloudellisen ja yhteiskunnallisen hyvinvoinnin. Digitaalisen turvallisuuden poikkeamilla voi olla organisaatioille kauaskantoisia taloudellisia seurauksia. Tällaisia ovat esim. taloudelliset tappiot, oikeusjutut, maineelle aiheutuva vahinko, kilpailukyvyn menettäminen (esim. liikesalaisuuksien anastuksen yhteydessä), samoin kuin asiakkaiden, työntekijöiden, osakkaiden ja yhteistyökumppanien keskuudessa tapahtuva luottamuksen menetys. Vaikka tällaiset tapaukset ovat yhä harvinaisia, on huomattava, että teollisuuslaitosten, liikennejärjestelmien ja sairaaloiden lisääntyneen tieto- ja viestintätekniikan käytön myötä digitaalisen turvallisuuden poikkeamat voivat johtaa myös aineellisiin vahinkoihin ja jopa kuolemantapauksiin.

Hallitukset ovat alttiita samoille turvallisuuspoikkeamien mahdollisille seurauksille kuin muutkin organisaatiot. Julkisen politiikan vetäjinä niitä huolettavat myös poikkeamien makrotason seuraukset, joihin sisältyy taloudellista ja yhteiskunnallista piiriä laajemmalle ulottuvia kansallisen ja kansainvälisen turvallisuuden näkökohtia kuten yllä on todettu.

Myös yksilöt ovat yhä enenevässä määrin tietoisia siitä, että digitaalisen ympäristön käytöstä saatujen hyötyjen lisäksi sillä voi olla myös varjopuolia. Kun ihmisen henkilötiedot julkistetaan tai ne päätyvät vääriin käsiin, hänen yksityisyyttään loukataan tavalla, josta saattaa aiheutua fyysistä, aineellista ja moraalista vahinkoa.[16] Ihminen voi joutua identiteettivarkauden takia talouspetoksen kohteeksi, kun hänen henkilötietonsa tai digitaaliset tunnisteensa anastetaan omalta laitteelta, tietomurron kohteeksi joutuneesta yrityksestä tai valtiollisista tietojärjestelmistä.

Poikkeamien lisääntyneen määrän ja niiden yhä korkeamman kehittyneisyyden taustalla on useita tekijöitä, joista yksi on rikollisen toiminnan siirtyminen verkkoon. Se on johtanut yhä ammattimaisempiin hyökkäyksiin ja nostanut yleistä digitaaliseen turvallisuuteen kohdistuvaa uhkatasoa. Niin satunnaiset ja yksittäiset varkaat kuin järjestäytyneet kansainväliset rikollisryhmätkin ovat osoittaneet huomattavaa teknistä innovaatiokykyä talousrikosten, tietoturvarikosten ja identiteettivarkauksien tekemisessä sekä yksilöiden, yritysten ja valtioiden kiristämisessä.

Laatikko 1. 2007–2014: Esimerkkejä laajamittaisista poikkeamista

Vaikka tällä alueella on vaikea kehittää tehokkaita ja kansainvälisesti vertailukelpoisia määrällisiä indikaattoreita (OECD, 2012c), empiirisen näytön mukaan digitaalisen turvallisuuden poikkeamien määrä on nousussa ja ne koskettavat kaikkia: julkisia ja yksityisiä organisaatioita, yksilöitä ja hallituksia. Tästä ovat esimerkkinä mm. seuraavat:

Vuonna 2007 Viroon kohdistuneet massiiviset ”kyberhyökkäykset” vaikuttivat parlamenttiin, ministeriöihin, pankkeihin, sanomalehtiin sekä televisio- ja radioyhtiöihin.

Vuonna 2010 Stuxnet-haittaohjelma teki aineellista tuhoa sadoille sentrifugeille ydinaineen rikastuslaitoksessa Iranissa. Vuonna 2011 tunkeutujat veivät Sony PlayStation Network verkosta henkilötietoja yli 77 miljoonalta pelaajatililtä. Tietomurron kustannukset yritykselle olivat viralisen tiedon mukaan 171 miljoonaa dollaria, joidenkin arvioiden mukaan jopa 250 miljoonaa dollaria (Gaudiosi, 2014).

Vuonna 2012 tunkeilijat pyyhkivät tyhjiksi yli 30 000 öljy-yritys Saudi Aramcon sisäiseen verkkoon liitettyä kovalevyä. Yritykseltä meni toipumiseen yli kaksi viikkoa.

Vuonna 2013 toteutettiin roskapostia valvovaa Spamhaus-järjestöä vastaan laajamittainen palvelunestohyökkäys, jonka nopeus korkeimmillaan oli ennenkuulumattomat 300 gigabittiä sekunnissa, kuusi kertaa enemmän kuin vastaavissa keskivertohyökkäyksissä ja kolme kertaa enemmän kuin suurimmassa siihen asti havaitussa hyökkäyksessä (Leyden, 2013). Samana vuonna amerikkalaista vähittäiskauppaketju Targetia vastaan tehtiin joulusesongin aikaan kehittynyt isku, jossa käytettiin hyväksi kassapäätteitä. Niiden kautta anastettiin 40 miljoonaa luotto- ja pankkikorttinumeroa sekä yli 110 miljoonaa asiakasta koskevat tiedot. Yritykselle koituneet kustannukset arvioidaan vähintään 148 miljoonaksi dollariksi ja kenties jopa yli miljardiksi. Muutamaa viikkoa myöhemmin Targetin toimitusjohtaja jätti paikkansa (O’Connor, 2014).

Vuonna 2014 varastettiin 56 miljoonan luotto- ja pankkikortin tiedot amerikkalaiselta Home Depot -yritykseltä. Koreassa yksi mies varasti henkilötietoja kolmen merkittävän pankin antamilta 104 miljoonalta luottokortilta, mikä vaikutti 20 miljoonaan henkilöön eli 40 prosenttiin maan väestöstä. Tapaus johti kymmenien johtajien irtisanomiseen (Choe, 2014; Kim, 2014). Myöhemmin samana vuonna 76 miljoonaan yhdysvaltalaiseen talouteen ja 7 miljoonaan pienyritykseen liittyviä tilitietoja varastettiin amerikkalaispankki JPMorgan Chasesta, minkä jälkeen pankin toimitusjohtaja ilmoitti yrityksen digitaaliturvallisuusbudjetin todennäköisesti kaksinkertaistuvan 250 miljoonasta dollarista 500 miljoonaan dollariin (Kiteen, 2014). Samana vuonna tunkeuduttiin syvälle Sony Pictures Entertainment yrityksen sisäiseen tietoverkkoon, minkä seurauksena julkisuuteen pääsi sisäisiä sähköpostiviestejä, yrityksen henkilöstöä ja yhteistyökumppaneita koskevia henkilötietoja sekä myös vielä julkaisemattomia elokuvia. Vuonna 2014 havaittiin myös pääasiassa eurooppalaisiin ja yhdysvaltalaisiin lääke- ja mahdollisesti myös energia-alan yrityksiin kohdistunut laajamittainen verkkovakoiluoperaatio (Dragonfly) (Peters, 2014). Lisäksi tietomurto saksalaisen teräslaitoksen verkkoon johti ”massiivisiin aineellisiin vahinkoihin” (Lee, Assante and Conway, 2014).

Muita vaikuttavia tekijöitä ovat terrorismi ja terrorismin tukijat, jotka myös ovat laajentaneet toimintaansa digitaaliseen ympäristöön. Verkkosivustoihin kohdistuvien hyökkäysten määrä, joko yhdessä fyysisten hyökkäysten kanssa tai niiden lisäksi, on kasvanut moninkertaisesti. Digitaalisen teollisuusvakoilun sanotaan myös olevan kasvussa, vaikka tarkkoja tietoja on saatavilla vain muutamasta tällaisesta tapauksesta.[17] Niin sanonut ”haktivistit” hankkivat säännönmukaisesti lisänäkyvyyttä poliittisille tarkoitusperilleen hyökkäämällä valittujen kohteiden kimppuun. Monet valtiot myös harjoittavat tiedustelutoimintaa ja hyökkäysluonteisia operaatioita digitaalisessa ympäristössä, johon usein viitataan sanalla ”kyberavaruus”. Ne ajat ovat kaukana takanapäin, kun digitaaliseen turvallisuuteen liittyvän epävakauden takana olivat pääasiassa teinit, jotka tekivät sattumanvaraisia iskuja käyttäen verkosta valmiina saatavia välineitä.

Hyökkäyksissä käytettävät tekniset välineet ovat muuttuneet yhä kehittyneemmiksi uhkan lähteiden ammattimaistumisen myötä. Jotkut näistä välineistä ovat automatisoituja ja niitä käytetään laajamittaisesti mahdollisimman suuren vaikutuksen aikaansaamiseksi, kun taas toiset on räätälöity nimenomaisia arvokkaita kohteita varten siten, että havaituksi tulemisen ja kiinnijäämisen riski voidaan minimoida. On syntynyt maanalainen tietoverkkorikollistalous. Niin sanottua nollapäivähaavoittuvuutta hyväksi käyttäviä haittaohjelmia, jotka pystyvät ohittamaan useimmat tietoturvaohjelmistot, voi ostaa digitaalisilta kauppapaikoilta. Niiden avulla on mahdollista tunkeutua tietojärjestelmiin vaivihkaa, seurata niitä ja poimia rikolliseen käyttöön luottamuksellisia tietoja kuten liike- tai poliittisia salaisuuksia pitkänkin ajan kuluessa. Tällaisista tapauksista käytetään termiä ATP-hyökkäys (Advanced Persistent Threat, kehittynyt jatkuva uhka).[18] Tuhansista tai jopa miljoonista[19] saastuneista tietokoneista ja muista laitteista koostuvia bottiverkkoja voi vuokrata palvelunestohyökkäystä varten, ja kiristää sitten hyökkäyksen kohteena olevan sivuston omistajaa. Tarkoituksena voi olla vain myös yleisesti osoittaa tyytymättömyyttään. Käyttäjien manipulointiin perustuvat tekniikat (”social engineering”) ovat myös erittäin yleisiä. Tällaisten esimerkkinä ovat mm. aidolta näyttävät sähköpostiviestit, jotka mahdollistavat hyökkääjän saavan valtuustietoja tai tunkeutuvan käyttäjän järjestelmään (verkkourkinta tai kalastelu eli ”phishing”). Laatikossa 1 annetaan esimerkkejä laajamittaisista poikkeamista, jotka ovat lisänneet tietoisuutta tämän haasteen laajuudesta ja mittakaavasta.

Digitaaliseen turvallisuuteen kohdistuvista haasteista on alkanut muodostua ensisijaisen tärkeä yhteiskuntapoliittinen kysymys OECD-maissa vuodesta 2009 lähtien, jolloin joukko valtioita ryhtyi korkeimman poliittisen tason tuella ottamaan käyttöön ”kansallisia kyberturvallisuusstrategioita”. Näissä strategioissa edistettiin kokonaisvaltaista yhteiskuntapoliittista lähestymistapaa ja luotiin uusia sekä hallinnon sisäisiä että hallinnon ulkopuolisten sidosryhmien kanssa toteutettavia koordinointimekanismeja.[20]

Laatikko 2. Tietojärjestelmäturvallisuudesta digitaaliseen turvallisuuteen kohdistuvien riskien hallintaan (2002–2015)

Vuoden 2015 suositus edustaa sekä jatkoa vuoden 2002 turvallisuutta koskeville ohjeille että merkittävää muutosta niihin.

Molempien suositusten lähtökohtana on sama analyysi: i) digitaalisen ympäristön globaali, verkottunut, avoin ja dynaaminen luonne on välttämätön taloudellisen ja yhteiskunnallisen hyvinvoinnin ajuri, ja ii) on mahdotonta luoda "varmaa ja turvallista" digitaalista ympäristöä, jossa riskit voidaan välttää täysin, muutoin kuin poistamalla sen avoimuus, verkottuneisuus ja dynaamisuus sekä luopumalla niistä taloudellisista ja yhteiskunnallisista hyödyistä, joita nämä ominaisuudet voivat tuottaa. Näin ollen molemmissa suosituksissa vahvistetaan siirtyminen Internetiä edeltävän ajan staattisesta ja jäykästä "ulkorajojen turvallisuudesta" prosessimaiseen ja ketterään riskipohjaiseen toimintatapaan, jolla riskit voidaan hallita, ts. pienentää hyväksyttävälle tasolle kulloisenkin kontekstin ja kyseessä olevien tavoitteiden mukaisesti.

Merkittävin muutos on se, että periaatteiden painopiste on siirretty "tietojärjestelmien ja verkkojen turvallisuudesta" digitaalisessa ympäristössä tapahtuvaan taloudelliseen ja yhteiskunnalliseen toimintaan kohdistuviin turvallisuusriskeihin. Suosituksessa oletetaan, että toiminnasta viime kädessä vastaavilla johtajilla ja päättäjillä on parhaat edellytykset määritellä hyväksyttävä riskitaso kyseiselle toiminnalle ja varmistaa, että digitaaliset turvatoimenpiteet ovat soveltuvia ja oikeasuhteisia riskiin nähden sen sijaan, että ne haittaisivat toimintaa, jota niillä on tarkoitus suojella. Tästä huolimatta suosituksessa korostetaan yhteistyön tarvetta digitaalisen ympäristön suunnittelusta ja ylläpidosta vastaavien asiantuntijoiden (ts. ICT-ammattilaisten) kanssa, sillä heillä on todennäköisesti parempi ymmärrys digitaaliseen turvallisuuteen kohdistuvista riskitekijöistä ja niihin liittyvistä mahdollisista turvatoimenpiteistä.

Näin ollen riskeihin liittyvää tekstiä on tarkennettu. Asiakirjaa laadittaessa huomattiin, että "turvallisuuden" sanakirjamääritelmä – suojaisuus, vaarattomuus, varmuus – viittaa binaariseen ja staattiseen tavoitteeseen, joka on jo lähtökohtaisesti ristiriidassa riskienhallinnan käsitteen kanssa. Joillekin tahoille turvallisuus viittaa "kansalliseen turvallisuuteen", mikä alue usein joko aiheesta tai aiheetta yhdistetään kulttuuriin, jolle "turvallisuus" on ensisijainen ja kaikenvoittava prioriteetti. Näin ollen toisin kuin vuoden 2002 turvallisuutta koskevissa ohjeissa tässä suosituksessa käytetään turvallisuutta adjektiivina luonnehtimaan riskiä, riskitekijöitä ja riskienhallinnan toimintatapaa pikemminkin kuin erilliseen tavoitteeseen viittaavana substantiivina. Suosituksessa ei myöskään käytetä termiä "kyberturvallisuus" eikä "kyber"-etuliitettä (esim. "kyberavaruus"), koska nämä termit ymmärretään eri tavoin eri tahoilla ja voivat näin ollen aiheuttaa sekaannusta. Lisäksi ne voivat antaa virheellisen käsityksen, jonka mukaan digitaaliseen turvallisuuteen kohdistuvat riskit jotenkin perustavanlaatuisesti eroaisivat muista riskiluokista.

Julkisen ja yksityisen sektorin organisaatiot alkavat yhä enenevässä määrin[21] tunnistaa haasteen laajuutta ja tarkistaa käytäntöjään. Kasvava joukko ennen kaikkea suuryritysten ylintä johtoa ymmärtää, että puhtaan tekninen lähestymistapa ei riitä digitaaliseen turvallisuuteen kohdistuvien riskien hallintaan. Monissa julkisissa ja yksityisissä organisaatioissa sekä erityisesti pienissä ja keskisuurissa yrityksissä (pk-yrityksissä) ei kuitenkaan olla vielä valmiita hallitsemaan digitaaliseen turvallisuuteen kohdistuvia riskejä taloudellisesta näkökulmasta, vaan niissä katsotaan ongelman olevan yhä luonteeltaan lähinnä tekninen. Kasvanut määrä merkittäviä, henkilötietojen paljastamiseen ja jopa talouspetoksiin ja identiteettivarkauksiin johtaneita tietomurtoja aiheuttaa huolta myös yksilöille[22], jotka keinojen, tiedon ja osaamisen puutteen vuoksi eivät usein kuitenkaan pysty hallitsemaan tätä riskiä, vaan jäävät usein oman onnensa nojaan.

Avainkäsitteitä

Tässä osassa esitellään suosituksessa käytetyt avainkäsitteet.

Sidosryhmät ja niiden roolit

Tässä suosituksessa “sidosryhmien” katsotaan olevan “hallitukset, julkiset ja yksityiset organisaatiot sekä yksilöt, jotka käyttävät digitaalista ympäristöä taloudellisessa ja yhteiskunnallisessa toiminnassaan. Sidosryhmällä voi olla useampi kuin yksi rooli.” (vrt. VII.3)

Termillä pyritään kattamaan kaikki, jotka vaihtelevassa määrin käyttävät digitaalista ympäristöä taloudellisessa ja/tai yhteiskunnassa toiminnassa tavoitteidensa saavuttamiseksi. Käsite on pikemminkin sosiologinen kuin juridinen ja sillä viitataan välittömään ja/tai välilliseen digitaalisen ympäristön käyttämiseen. Termi ”hallitus” kattaa hallintoelimet kaikilla tasoillaan (esim. valtionhallinto/liittovaltion hallinto, kansainvälinen/alueellinen/kansallinen/maakunnallinen/ kunnallinen jne.). ”Julkisen sektorin organisaatioihin” kuuluvat kaikki muut julkis- tai hallinto-oikeudelliset yhteisöt kuten verovaroin ylläpidetyt laitokset (esim. sairaalat, koulut, kirjastot jne.) sekä valtionyhtiöt. Yksityiset organisaatiot ovat yksityisoikeudellisesti säänneltyjä ja niihin kuuluvat niin yritykset kuin voittoa tavoittelemattomat yhteisöt.

Eri sidosryhmillä voi olla erilaisia rooleja ja myös useampia kuin yksi rooli. Esimerkiksi yksilö voi olla kansalainen, kuluttaja, vanhempi, opiskelija, työntekijä jne. riippuen kulloinkin tarkasteltavasta toiminnasta. Useimmat organisaatiot ovat digitaalisen ympäristön käyttäjiä. Osana ydintoimintaansa jotkut ovat myös tekemisissä digitaalisen ympäristön ylläpidon, hallinnan tai suunnittelun kanssa (esim. ohjelmistojen tai tietokonelaitteiden valmistaja, teleoperaattori tai Internet-palvelun tarjoaja). Tietyn kokoluokan ylittävillä organisaatioilla on yleensä erillinen IT-osasto, joka vastaa organisaation toimintaa tukevasta digitaalisesta infrastruktuurista. Joskus yksilö voi olla tekemisissä digitaalisen ympäristön ylläpidon kanssa olematta osa organisaatiota. Mm. sovellus- ja ohjelmistokehittäjät ovat tällaisia henkilöitä. Hallituksilla voi myös olla useampia rooleja: ne käyttävät digitaalista ympäristöä ja tukeutuvat siihen laajalti (esim. valtionhallinnon sähköisten palvelujen tarjoamiseksi sekä useimpien muiden valtionhallinnon tehtävien kuten virkamiesten palkanmaksun hallinnoimiseksi) ja ne myös tekevät taloudellista ja yhteiskunnallista hyvinvointia edistäviä linjauksia digitaalisen ympäristönkin osalta.

Digitaaliseen turvallisuuteen kohdistuvat riskit

Ote suosituksesta (VII.1):

> *"Epävarmuuksien vaikutusta tavoitteisiin kutsutaan riskiksi. "Digitaaliseen turvallisuuteen kohdistuva riski" on ilmaisu, jota käytetään kuvailemaan riskiluokkaa, joka liittyy toiminnassa tapahtuvaan digitaalisen ympäristön käyttöön, kehittämiseen ja hallinnointiin. Riski voi aiheutua digitaalisen ympäristön uhkien ja haavoittuvuuksien yhdistelmästä. Se voi heikentää taloudellisten ja yhteiskunnallisten tavoitteiden saavuttamista haittaamalla toiminnan ja/tai ympäristön luottamuksellisuutta, eheyttä ja käytettävyyttä. Digitaaliseen turvallisuuteen kohdistuva riski on luonteeltaan dynaaminen. Se käsittää tekijöitä, jotka liittyvät digitaaliseen ja fyysiseen ympäristöön, toiminnassa mukana oleviin ihmisiin sekä toimintaa tukevaan organisatoriseen prosessiin."*

Toimintaan, johon sidosryhmät ryhtyvät tavoitteidensa saavuttamiseksi, kohdistuu tekijöitä, jotka saattavat vaikuttaa sidosryhmien onnistumisen todennäköisyyteen. Epävarmuus on osa elämää. Tietomme ja ymmärtämyksemme tällaisista tekijöistä ja niiden mahdollisista vaikutuksista tavoitteisiimme ovat rajalliset. "Riski" on epävarmuustekijöiden vaikutukset tai seuraukset sidosryhmien tavoitteille, ts. poikkeama todellisuuden ja odotusten välillä. Tämä lähestymistapa riskiin perustuu ISO/IEC 31000:2009 -standardiin, ISO/IEC 27000 -sarjaan sekä ISO Oppaaseeen 73 (ks. Laatikko 3). Riski ilmaistaan usein todennäköisyyden ja vaikutuksen avulla ja riskitasoja tyypillisesti esitetään x-/y-akselilla, mikä edesauttaa näiden kahden ulottuvuuden mahdollisten yhdistelmien käsittelyä.

Digitaaliseen turvallisuuteen kohdistuva riski sellaisena kuin se on tässä suosituksessa määritelty (ks. Laatikko 3) on vain yksi monista sidosryhmien kohtaamista riskiluokista. Se:

- ***Liittyy "digitaaliseen epävarmuuteen", mutta ei yksinomaisesti.*** Missä ikinä tieto- ja viestintätekniikkaa käytetäänkin, siellä vallitsee vastaavasti myös digitaalisen ympäristön käyttöön liittyvä epävarmuus ("digitaalinen epävarmuus"). Digitaaliseen turvallisuuteen kohdistuva riski ei kuitenkaan liity vain "nolliin ja ykkösiin": digitaalisen ympäristön käyttö edellyttää ohjelmistoja, laitteita sekä välitöntä tai välillistä ihmisen toimintaa tai vuorovaikutusta, ja näihin kaikkiin voi kohdistua uhkia, haavoittuvuuksia ja poikkeamia. Esimerkiksi palvelun tai tuotantolinjan käytettävyyden voi estää datakeskuksen energiansyöttöön vaikuttava tai ilmajohdot katkaiseva luonnonmullistus. Liikesalaisuuksia voivat anastaa rikolliset, jotka käyttävät sosiaalisen manipuloinnin tekniikoita, jotka harhauttavat ihmisiä tekemään asioita, jotka mahdollistavat laittoman pääsyn tietojärjestelmiin. Näin ollen uhkilla, haavoittuvuuksilla ja poikkeamilla voi olla niin digitaalinen, fyysinen kuin inhimillinenkin ulottuvuus.

Laatikko 3. Määritelmistä, terminologiasta ja standardeista

Suosituksessa käytetyille termeille ja määritelmille ei tulisi antaa määräävää tai jäykkää tulkintaa eikä niiden tulisi katsoa suosivan mitään tiettyä riskeihin liittyvää terminologiaa tai alan termistöä. Ne on valittu tukemaan korkean tason linjausten ohjausta sekä soveltumaan eri maita, kulttuureja ja oikeusjärjestelmiä edustaville johtajille ja päättäjille, joiden taloudelliset, yhteiskunnalliset ja poliittiset tilanteet myös eroavat toisistaan. Sama pätee niin OECD:n jäsenmaihin kuin myös OECD:hen kuulumattomiin maihin.

Suosituksen riskiin liittyvä terminologia perustuu riskienhallintaa koskeviin kansainvälisiin ISO/IEC-standardeihin ja oppaisiin sikäli kuin mahdollista. Erityisenä perustana ovat toimineet ISO/IEC 31000:2009 sekä ISO Opas 73 – jota myös ISO/IEC 27000 -sarja heijastaa – samalla huomioiden, että riskeihin liittyviä standardeja on lukuisia muitakin ja että näiden terminologiat toisinaan eroavat toisistaan[23]. Monesti termit ja määritelmät on räätälöity vastaamaan suosituksen kohderyhmiä, tavoitteita ja soveltamisalaa. Kuten suosituksessa todetaan, periaatteet on tarkoitettu sopimaan yhteen riskienhallintaa koskevien prosessien, parhaiden käytäntöjen, menettelytapojen ja standardien kanssa. Suosituksen odotetaan edesauttavan rakentamaan siltaa johtajien ja korkean tason päättäjien sekä näiden standardien täytäntöönpanosta vastaavien asiantuntijoiden välille ja edistävän näin taloudellista ja yhteiskunnallista hyvinvointia.

Riskienhallinta on monitahoinen ala, joka koskettaa useita eri sektoreita terveydenhuollosta rahoitusalaan ja teollisuudesta vakuutustoimintaan. Jokaisen alan prosesseihin liittyy niiden oma riskikulttuuri, terminologia ja riskejä koskevat standardit. Suosituksessa ei väitetä esitettävän ehdotonta ja yleistä käsitystä riskistä ja riskienhallinnasta. Riski on käsitteenä vanha. Se on muuttunut kautta historian ja kehittyy edelleen. Riskille tai riskiterminologialle ei ole yhtä yleisesti hyväksyttyä määritelmää: eräs tutkija vastikään analysoi peräti 27 riskin määritelmää, jotka ryhmittyivät yhdeksään eri luokkaan, ja hänkin totesi niitä todennäköisesti olevan vielä enemmän (Aven, 2012).

- ***On taloudellista ja yhteiskunnallista***. Digitaalisella epävarmuudella on taloudellisia ja yhteiskunnallisia vaikutuksia tai seurauksia, jotka voivat kohdistua aineelliseen tai aineettomaan omaisuuteen. Riski tulisi näin ollen muotoilla talouden ja yhteiskunnan termein: taloudellinen menetys, kilpailukyvyn heikentyminen, mahdollisuuden menettäminen, maineeseen, mielikuvaan tai luottamukseen kohdistuva vahinko jne. Aihealueesta riippuen vaikutuksia eli riskiluokkia voi olla myös tämän suosituksen soveltamisalan ulkopuolella ja niihinkin olisi aiheellista puuttua. Organisaatiot saattavat esim. ottaa huomioon puhtaan tekniset (eli tieto- ja viestintätekniset) seuraukset, kun taas hallitukset voivat käsitellä kansalliseen ja kansainväliseen turvallisuuteen liittyviä seurauksia.

- ***Vaikuttaa saatavuteen, eheyteen ja luottamuksellisuuteen*** (ts. "tietoturvallisuuteen"). Vaikutuksia voivat aiheuttaa keskeytykset saatavuudessa, eheydessä ja luottamuksellisuudessa liittyen joko itse toimintaan tai siihen digitaaliseen ympäristöön, jossa toimintaa harjoitetaan tai jota toiminnassa välittömästi tai välillisesti käytetään. Nämä kolme ominaisuutta ovat englanniksi *availability, integrity ja confidentiality*, ja niihin viitataan termillä AIC-kolmio. Se edustaa klassisia tietoturvaominaisuuksia tai -määreitä, jotka auttavat rajaamaan digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan omaksi

erikoisalakseen. Näin ollen digitaaliseen turvallisuuteen kohdistuvat riskit eivät kata epävarmuustekijöitä, jotka liittyvät esim. teollis- ja tekijänoikeuksien rikkomiseen tai sopimattomien tietojen (ts. sisällön) levittämiseen digitaalisessa ympäristössä[24].

- ***Vaikuttaa kielteisesti.*** Jokapäiväisessä kielenkäytössä "riski" yleensä kattaa vain epävarmuuden haitalliset vaikutukset ja näin ollen suosituksessa keskitytään epävarmuuteen, joka saattaa haitata taloudellisten ja yhteiskunnallisten tavoitteiden saavuttamista. Suosituksessa suhtaudutaan digitaaliseen turvallisuuteen kohdistuvien riskien hallintaan keinona suojella arvoa, jolla taloudelliset ja yhteiskunnalliset tavoitteet voitaisiin saavuttaa parhaalla mahdollisella tavalla. Epävarmuudella voi kuitenkin olla myös myönteisiä vaikutuksia ja se voi olla toiminnalle eduksi. Epävarmuuden myönteisiä vaikutuksia kutsutaan usein "mahdollisuuksiksi" pikemminkin kuin "riskiksi". Riskien ja mahdollisuuksien välinen suhde on tärkeä, sillä digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa voitaisiin myös käyttää *lisäarvon luomiseen* siten, että epävarmuudet selvitettäisiin ja hyödynnettäisiin järjestelmällisesti innovaatiotoiminnan ajurina. Tätä aihetta käsitellään tarkemmin jäljempänä (innovaatiotoimintaperiaate).

Riskitekijät: uhkat, haavoittuvuudet ja poikkeamat

Riskit aiheutuvat tilanteista, joissa uhkat yhdessä haavoittuvuuksien kanssa tuottavat taloudellisia seurauksia. Tapahtumia, jotka saattavat muuttaa odotettavissa olevaa toiminnan kulkua ja vaikuttaa tavoitteisiin, kutsutaan usein *poikkeamiksi*. Toiminnalle aiheutuviin seurauksiin tarvitaan sekä uhkia että haavoittuvuuksia. Uhkat ilman haavoittuvuuksia sen enempää kuin haavoittuvuudet ilman uhkia eivät kasvata riskiä.

Arkisessa kielenkäytössä sanaa "riski" käytetään monilla tavoin. Sillä voidaan viitata esimerkiksi uhkaan, haavoittuvuuteen, poikkeamaan, todennäköisyyteen, sattumaan ja vaaraan.[25] Riskienhallintaa varten on kuitenkin tarpeen tehdä selkeä ero syiden ja niiden seurausten välillä ja puuttua ensin mainittuihin (uhkat, haavoittuvuudet ja poikkeamat) jälkimmäisten (riskien) hallitsemiseksi. Tätä eroa korostetaan käyttämällä tässä asiakirjassa uhkista, haavoittuvuuksista ja poikkeamista termiä "riskitekijät", ts. riskien aiheuttajat tai myötävaikuttajat.

Uhkat esiintyvät yleensä toiminnan ulkopuolella, kun taas haavoittuvuudet ovat toiminnan sisäisiä heikkouksia. Näin ollen sidosryhmien kyky vaikuttaa uhkiin on usein rajallinen, kun taas haavoittuvuuksiin ne pystyvät yleensä puuttumaan välittömämmin. Joissakin tapauksissa sekä uhka että haavoittuvuus ovat lähtöisin toiminnan sisältä. Esimerkki tällaisesta olisi tyytymätön työntekijä, joka käyttöoikeuksiensa avulla tekee työnantajalle haitallisiin seurauksiin johtavia luvattomia toimia.

Uhkia, haavoittuvuuksia ja poikkeamia voidaan luokitella monella eri tavalla. Uhka voi esimerkiksi olla tahallinen (ts. hyökkäys, esim. rikolliset varkaissa) tai tahaton (ts. seurausta vahingosta, esim. tietyömaalla erehdyksessä katkaistu valokuitukaapeli). Poikkeama voi myös olla seurausta ihmisen toiminnasta kuten tahattomista virheistä tai henkilöön kohdistuvasta manipuloinnista johtuvista toimista (esim. verkkourkinta eli phishing-toiminta).

Poikkeama voi niin ikään johtua luonnonilmiöistä kuten myrskyt, tulvat tai maanjäristykset. Tahallisten uhkien kehittyneisyyden taso voi vaihdella hyvin yksinkertaisesta erittäin monimutkaiseen, mitä havainnollistaa kansainvälisten uhkien lähteiden kirjo teineistä valtion tukemiin ryhmiin. Poikkeamien kesto voi lopuksi myös vaihdella erittäin lyhyistä, kuten esimerkiksi yllättävä palvelunestohyökkäys, joka heikentää viestintää asiakkaiden kanssa vuoden kiireisimpään myyntiaikaan, aina erittäin pitkäkestoisiin (ts. monivuotisiin), kuten esimerkiksi vaivihkainen tietojärjestelmään tunkeutuminen, jonka pyrkimyksenä on poistaa yritys markkinoilta anastamalla sen liikesalaisuudet.

Digitaaliseen turvallisuuteen kohdistuvien riskien dynaaminen luonne juontuu niiden kaikkien osatekijöiden eli taloudellisen ja yhteiskunnallisen toiminnan, riskitekijöiden ja digitaalisen ympäristön alati muuttuvasta luonteesta.

Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta

Ote suosituksesta (VII.2):

> *”Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta tarkoittaa organisaation sisällä ja/tai organisaatioiden välillä tehtäviä koordinoituja toimia, joiden tarkoituksena on puuttua digitaaliseen turvallisuuteen kohdistuvaan riskiin ja samalla maksimoida mahdollisuudet. Se on olennainen osa päätöksentekoa sekä taloudelliseen ja yhteiskunnalliseen toimintaan liittyvän riskienhallinnan yleistä viitekehystä. Se perustuu kokonaisvaltaisiin, systemaattisiin ja joustaviin prosesseihin, jotka ovat mahdollisimman avoimia ja yksiselitteisiä. Nämä prosessit auttavat varmistamaan, että digitaaliseen turvallisuuteen kohdistuvien riskien hallinnassa käytettävät toimet (”turvatoimenpiteet”) ovat soveltuvia ja oikeasuhteisia riskiin sekä kyseessä oleviin taloudellisiin ja yhteiskunnallisiin tavoitteisiin nähden.”*

Digitaaliseen turvallisuuteen kohdistuvia riskejä ei ole mahdollista poistaa täysin, mutta niitä voidaan hallita taloudellisen ja yhteiskunnallisen toiminnan edistämiseksi ja suojelemiseksi. Näin ollen digitaaliseen turvallisuuteen kohdistuvien riskien hallinnalla pyritään edistämään taloudellisten ja yhteiskunnallisten tavoitteiden saavuttamista. Erityisesti se:

- ***On strategista taloudelliseen ja yhteiskunnalliseen päätöksentekoon nähden***. Riskienhallinta on prosessi, jonka avulla päättäjät toimintansa suunnittelussa ja hallinnoinnissa huomioivat tekijät, jotka saattavat vaikuttaa tavoitteiden saavuttamiseen. Sikäli kuin taloudellisessa ja yhteiskunnallisessa toiminnassa käytetään digitaalista ympäristöä joko välittömästi tai välillisesti, digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan tulisi olla olennainen osa päätöksentekoprosessia ja sitä tulisi käsitellä yhdessä strategioiden kanssa mahdollisuuksien maksimoimiseksi (ks. jäljempänä innovaatiotoimintaperiaate). Johtajien tulisi suhtautua digitaaliseen turvallisuuteen kohdistuvien riskien hallintaan taloudellisena ja yhteiskunnallisena haasteena ennemmin kuin vain puhtaan teknisenä haasteena. Heidän tulisi kuitenkin tehdä yhteistyötä muiden sidosryhmien,

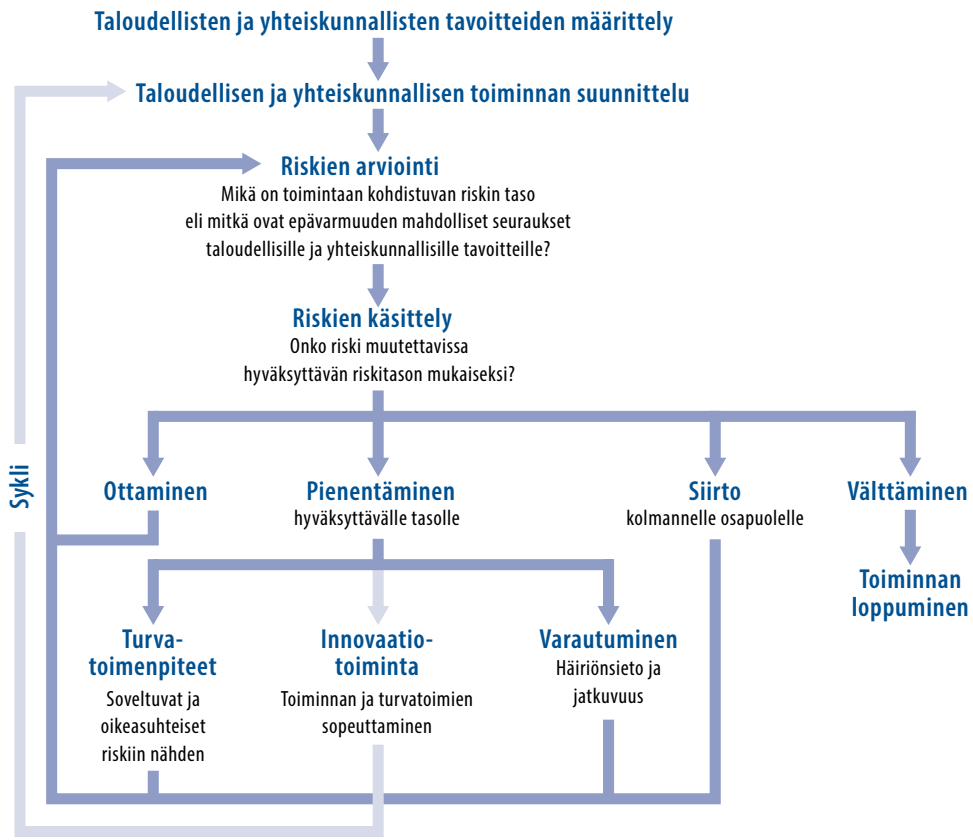
kuten digitaalisen ympäristön hallinnasta ja ylläpidosta vastaavien kanssa, jotta he voisivat paremmin ymmärtää olennaiset riskitekijät kuten tiettyjen ICT-alan turvallisuusuhkien todennäköisyyden, joidenkin ICT-alan turvallisuutta koskevien haavoittuvuuksien yleisyyden, joidenkin mahdollisten ICT-turvallisuuden poikkeamien ominaisuudet (esim. niiden leviämis- ja eskalaatiomahdollisuudet) sekä ICT-toimet, jotka muiden muassa voivat toimia riskien käsittelyn tukena. ICT-asiantuntijat pystyvät havaitsemaan poikkeamat ja puuttumaan niihin teknisellä tasolla, mutta he eivät pysty analysoimaan poikkeamien tai niihin puuttumiseen käytettyjen teknisten toimien taloudellisia seurauksia organisaatiolle. Vastaavasti vain johtajat ja päättäjät voivat ottaa digitaaliseen turvallisuuteen kohdistuvat riskit huomioon organisaation yleisissä strategisissa tavoitteissa ja suunnitelmissa.

- ***Varmistaa, että "turvatoimenpiteet" tukevat täysimääräisesti kyseessä olevaa taloudellista ja yhteiskunnallista toimintaa eivätkä haittaa sitä***. Toiminnan suojaaminen jokaiselta mahdolliselta uhkalta, haavoittuvuudelta ja poikkeamalta on mahdotonta, ja siksi on tehtävä päätöksiä digitaaliseen turvallisuuteen kohdistuvien riskien hallintatoimien ("turvatoimenpiteiden") valinnasta ja toteutuksesta. Turvatoimenpiteet eivät myöskään aina ole neutraaleja sen toiminnan suhteen, jota ne suojaavat. Ne voivat luoda erilaisia toimintaa haittaavia esteitä ja rajoituksia. Ne voivat mm. kasvattaa kustannuksia, lisätä järjestelmien monimutkaisuutta, hidastaa markkinoille pääsyä ja vähentää toimivuutta, käyttökelpoisuutta, kehittymismahdollisuuksia, innovaatioita ja käyttäjämukavuutta. Ne voivat myös uhata yksityisyydensuojaa (ks. Laatikko 4) ja aiheuttaa muita yhteiskunnallisia haittavaikutuksia. Näitä rajoitteita ja haittavaikutuksia voidaan torjua, mutta sillä on hintansa. Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta yhdistää turvallisuutta koskevat päätökset kyseessä olevan toiminnan taloudelliseen ja yhteiskunnalliseen todellisuuteen. Se estää tekemästä päätöksiä eristyksissä pelkästään teknisestä tai turvallisuusnäkökulmasta. Se ohjaa valitsemaan turvatoimenpiteitä, jotka ovat soveltuvia ja oikeasuhteisia riskiin ja kyseessä olevaan toimintaan nähden, ja varmistaa täten, että turvatoimenpiteet tukevat kyseessä olevaa taloudellista ja yhteiskunnallista toimintaa sen sijaan, että ne haittaisivat sitä esim. sulkemalla ympäristöä aiheettomasti tai heikentämällä toimivuutta tavalla, joka rajoittaa mahdollisuuksia hyödyntää tieto- ja viestintätekniikoita innovaatiotoimintaan ja tuottavuuden lisäämiseen.

- ***On olennainen osa yleistä riskienhallinnan kehystä*** erillisen ja yksittäisen siilon sijaan. Digitaaliseen turvallisuuteen kohdistuvat riskit ovat yksi monista taloudelliseen ja yhteiskunnalliseen toimintaan kohdistuvien riskien lähteistä. Digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan integrointi laajempaan, koko organisaation kattavaan riskienhallinnan kehykseen antaa ylemmän tason johtajille ja päättäjille paremman kokonaiskuvan riskikentästä, mikä mahdollistaa strategisemman ja toimivamman johtamisen ja päätöksenteon. Olisi epätarkoituksenmukaista luoda erillinen, olemassa olevan riskienhallinnan kehyksen ulkopuolinen kehys pelkästään digitaaliseen turvallisuuteen kohdistuvien riskien hallinnalle.

Tyypillisen riskienhallintaprosessin tulisi olla olennainen osa toiminnan harjoittamiseen liittyvää päätöksentekoprosessia ja sen tulisi ajoittua toiminnan koko elinkaarelle. Kaaviossa 1 on suosituksen toimintaperiaatteita heijastava yleisluontoinen esitys riskienhallinnasta. Se alkaa tavoitteiden määrittelyllä ja toiminnan suunnittelulla. Sitten riskit arvioidaan ja ne käsitellään arvion perusteella tavalla, joka tukee ja turvaa tavoitteiden toteutumaista. Riskien käsittely määrittää, onko riskiä tarpeen muuttaa toiminnan onnistumisen todennäköisyyden lisäämiseksi ja kertoo, millaisia muutosten tulisi olla. Toisin sanoen on päätettävä, mitkä riskit otetaan, pienennetään, siirretään tai vältetään (periaate 1). Riskin pienentämiseksi voidaan sitten valita ja ottaa käyttöön turvatoimenpiteitä (periaate 2), voidaan harkita innovaatiotoimintaa sekä turvatoimenpiteiden että kyseessä olevan toiminnan osalta (periaate 3), ja voidaan määritellä ja soveltaa varautumistoimia poikkeamien tapahtuessa (periaate 4). Aihetta käsitellään tarkemmin toimintaperiaatteita koskevassa osassa.

Kaavio 1: Yleiskatsaus digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan prosessista



Huom. Tämä kaavio edustaa yhtä mahdollista riskienhallintaprosessin esittämistapaa ja se keskittyy suosituksen osan 1 toimintaperiaatteisiin. Yleiset periaatteet tulisi nähdä prosessia tukevina pilareina.

Lähde: OECD.

Suurehkoissa organisaatioissa digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan monimutkaisuus edellyttää usein asiaa koskevan muodollisen kehyksen käyttöönottoa koko organisaation kattavuuden ja yhdenmukaisen toimintatavan varmistamiseksi. Tällainen kehys yleensä ilmenee yrityksen tai organisaation periaatteita tai käytäntöjä käsittelevästä asiakirjasta ja sen muodot voivat olla yhtä moninaiset kuin organisaatioiden kulttuurit ja johtamistyylitkin. Muodollinen kehys heijastelee suosituksen periaatteita ja on yhdenmukainen organisaation mahdollisesti jo käytössä olevan yleisen riskienhallintakehyksen kanssa, johon se kuuluu olennaisena osana.

Kehyksen laatimiseen osallistuvat yleensä kaikki asiaan liittyvät toimijat ja kehys hyväksytetään ylimmällä tasolla mahdollisimman suuren yhdenmukaisuuden ja näkyvyyden varmistamiseksi. Tämä saattaa nostaa esiin monitahoisia hallinnointiin liittyviä kysymyksiä, joita tässä asiakirjassa ei käsitellä mutta joita olisi aiheellista analysoida tarkemmin. Kehyksessä yleensä ilmaistaan selkeästi sen toimeenpanijoiden vastuut ja velvollisuudet. Eräs keskeinen kehyksessä käsiteltävä osa-alue, on menettelytavat joilla varmistetaan, että organisaation liiketoiminnallinen ja ICT-johto työskentelevät käsi kädessä digitaaliseen turvallisuuteen kohdistuvien riskien hallinnassa.

Kehys käsittää kaikki organisaation digitaalisessa ympäristössä tapahtuvaan taloudelliseen ja yhteiskunnalliseen toimintaan liittyvät näkökohdat toiminnan koko elinkaaren ajan. Se selventää organisatorisia prosesseja sen varmistamiseksi, että riskienhallinta toimii jatkuvalla ja systemaattisella tavalla. Sen joustavuus mahdollistaa ketterän, eteenpäin katsovan vastaamisen esiin nouseviin digitaaliseen turvallisuuteen kohdistuviin riskeihin. Kuten jäljempänä (toimintaperiaatteissa) todetaan, kehys mahdollistaa kokonaisvaltaiset, systemaattiset ja joustavat prosessit, joiden toteuttamisen tarkoituksena on sopeutua riskien dynaamiseen luonteeseen. Siinä huomioidaan parhaat käytännöt ja standardit samalla, kun siinä käsitellään myös asiayhteyteen liittyviä osatekijöitä, joita nämä eivät välttämättä kata. Avoimuus auttaa kasvattamaan uskottavuutta ja luottamusta niin organisaation sisällä kuin sen ulkopuolellakin osoittamalla, että organisaatio on sitoutunut puuttumaan digitaaliseen turvallisuuteen kohdistuviin riskeihin. Kehyksen tulisi olla vaivatta ja riippumattomasti todennettavissa. Sitä varten voidaan esimerkiksi kannustaa noudattamaan yksinkertaista sääntöä: kirjoita muistiin, mitä teet, ja tee niin kuin olet muistiin kirjoittanut. Jatkuva kehyksen tarkistamisen ja kehittämisen malli on välttämätön tehokkaan riskienhallinnan varmistamiseksi sekä luottamuksen kasvattamiseksi. Malli yleensä käsittää prosesseja, joilla testataan, tarkastellaan ja optimoidaan käytössä olevia toimia.

Yksityiskohtaisempaa tietoa mm. digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan prosessin luonteesta annetaan toimintaperiaatteita käsittelevässä osiossa.

Laatikko 4. Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta ja yksityisyydensuoja

Digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan ja yksityisyydensuojan välistä suhdetta voidaan tarkastella ainakin kolmesta eri näkökulmasta.

Ensinnäkin digitaaliseen turvallisuuteen kohdistuvien riskien hallinta tarjoaa rekisterinpitäjille (ts. henkilötietojen sisällöstä ja käytöstä päättäville tahoille) tehokkaan mahdollisuuden panna täytäntöön OECD:n yksityisyyden suojaa koskevien ohjeiden turvajärjestelyjä koskeva periaate, jonka mukaan "on ryhdyttävä kohtuullisiin turvatoimenpiteisiin henkilötietojen suojaamiseksi tietojen häviämisen, tuhoutumisen, käytön, muuttamisen tai julkistamisen sekä laittoman tietoihin pääsyn riskin estämiseksi".

Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta auttaa erityisesti varmistamaan, että turvatoimenpiteet ovat soveltuvia ja oikeasuhteisia riskiin nähden. Tämä on toimiva tapa määritellä turvajärjestelyjen "kohtuullisuus". Rekisterinpitäjän hyväksymän henkilötietoihin kohdistuvan riskin taso voi kuitenkin olla korkeampi kuin rekisteröidyn eli sen henkilön, jonka tiedoista on kyse. Mahdollinen ristiriita rekisterinpitäjän ja rekisteröidyn intressien välillä onkin olennainen kysymys yksityisyydensuojan kannalta. Yleisemmin ottaen se, että riskejä arvioiva taho (rekisterinpitäjä) ei ole se, jolle riski aiheutuu (rekisteröity henkilö), on olennainen ero turvallisuuteen ja yksityisyydensuojaan kohdistuvien riskien arvioinnissa.

Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta saattaa heikentää yksityisyydensuojaa myös esimerkiksi tuottamalla turvatoimenpiteitä, jotka lisäävät siihen kohdistuvia riskejä. Tällaisia ovat mm. verkkoseuranta sekä riskejä koskevan tiedon jakaminen kolmansien osapuolten kanssa. Yksityisyyden suojeleminen on näin ollen sisällytetty suosituksen osan 1 kolmanteen ihmisoikeuksia ja perusarvoja koskevaan periaatteeseen, jossa edellytetään toisten oikeutettujen etujen kunnioittamista ja tunnustamista.

On myös yhä yleisemmin tunnistettu, että riskienhallintaa voidaan pitää toimivana menetelmänä OECD:n yksityisyydensuojaa koskeviin ohjeisiin sisältyvien periaatteiden parempaan täytäntöönpanoon. Jatkotyöskentely on kuitenkin tarpeen käytännön sovellusten ja vaikutusten ymmärtämiseksi.

Periaatteiden soveltaminen

Sidosryhmien tulisi panna periaatteet täytäntöön "rooliensa, toimintakykynsä ja toiminta-alueensa" (IV) mukaisesti. Tämä koskee yleisesti kaikkia periaatteita. Se on erityisen tärkeätä kuitenkin vastuullisuusperiaatteen osalta ja se vaikuttaa toimintaperiaatteiden soveltamiseen.

Roolit: käyttäjien erottaminen digitaalisesta ympäristöstä vastaavista sidosryhmistä

Kuten määritelmässä todettiin, sidosryhmien roolit voivat vaihdella ja niillä voi olla useampia kuin yksi rooli. On syytä erottaa toisistaan sidosryhmät ylipäänsä sekä ne, jotka kehittävät ja levittävät digitaalisia tuotteita ja palveluja. Kaikki sidosryhmät ovat digitaalisen ympäristön käyttäjiä ja niiden tulisi siten hallita digitaaliseen turvallisuuteen kohdistuvia riskejä omassa toiminnassaan. Näiden sidosryhmien joukossa niiden, jotka vastaavat digitaalisen ympäristön kehittämisestä ja ylläpidosta (esim. ICT-alan ammattilaiset)[26], tulisi myös mahdollisuuksien mukaan[27] toteuttaa asianmukaisia turvatoimenpiteitä omissa tuotteissaan ja palveluissaan, jotta niiden käyttäjillä olisi mahdollisuus hallita digitaaliseen turvallisuuteen kohdistuvia riskejä. Näin ollen heidän tulisi kehittää kaksinkertainen digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan kulttuuri: ensimmäinen käsittelee heidän oman digitaalista ympäristöä käyttävän toimintansa riskejä, kun taas toisella pyrittäisiin optimoimaan heidän tuotteensa ja palvelunsa siten, että kuluttajille ja käyttäjille tarjottaisiin asianmukaisia apukeinoja heidän omaan digitaalisen ympäristön käyttöönsä liittyvien riskien hallintaan. He voivat esim. suunnitella tuotteita ja palveluja siten, että kuluttajat pystyvät ymmärtämään tuotteisiin "sisäänrakennetut", käyttäjäystävälliset ja oletusasetuksia hyödyntävät turvallisuusominaisuudet ja käyttämään niitä.

Nämä kaksi asiaa liittyvät toisiinsa. Jos ICT-alan tuotteiden ja palvelujen kehittämiseen liittyvää turvallisuusriskiä ei hallita asianmukaisesti, se voi vaikuttaa niihin sisällytettyjen turvatoimenpiteiden toimivuuteen ja näin ollen lisätä käyttäjille aiheutuvaa riskiä. Esimerkiksi Hollannin varmenneviranomaisen DigiNotarin tietojärjestelmiin murtauduttiin vuonna 2011, mikä mahdollisti 300 000 Gmail-sähköpostitiliin kohdistuneet hyökkäykset, kasvatti DigiNotarin asiakkaiden turvallisuusriskiä ja heikensi luottamusta Hollannin valtion sähköisen asioinnin järjestelmään, jonka toiminnassa yritys oli välillisesti mukana. Yritys meni lopulta konkurssiin. Toisena esimerkkinä voidaan mainita turvallisuusalan yritys RSA:han vuonna 2011 kohdistunut tietomurto, joka vaaransi noin 40 miljoonan

tunnistevälineen tietoturvallisuuden ja mahdollisti anastettujen tietojen käytön hyökkäyksiin joitakin yrityksen puolustusalalla toimivia asiakkaita vastaan.[28] ICT-alalla toimivien sidosryhmien ja ennen kaikkea tietoturva-alan toimijoiden tulisi näyttää esimerkkiä digitaaliseen turvallisuuteen kohdistuvien riskien hallinnassa.

Toimintakyky: pk-yritysten ja yksilöiden erottaminen muista sidosryhmistä

Sidosryhmien kyky toimia voi vaihdella merkittävästi myös riippuen mm. seuraavista tekijöistä: i) yleinen digitaaliseen turvallisuuteen kohdistuvien riskien ymmärtäminen, ii) tälle haasteelle kohdennettavissa olevan huomion ja resurssien määrä, iii) oikeudellinen toimivalta, johon joskus viitataan myös valtuutuksena tai toimintavaltuutena, ja iv) mahdollisuudet vaikuttaa digitaaliseen ympäristöön. Näiden neljän tekijän osalta hallitukset ja suuret organisaatiot tulisi erottaa pk-yrityksistä ja yksilöistä, joiden toimintakyvyn voidaan yleisesti katsoa olevan rajallisempi. Tämä pätee erityisesti yksilöihin. Pk-yritysten ja yksilöiden mahdollisuudet vaikuttaa digitaaliseen ympäristöön riippuvat erityisesti yleisesti saatavilla oleviin digitaalisiin tuotteisiin ja palveluihin sisältyvien turvatoimenpiteiden saatavuudesta, hinnasta, käytettävyydestä ja soveltuvuudesta.[29]

Suosituksessa tunnistetaan tämä rajallisuus ja kehotetaan hallituksia sekä julkisia ja yksityisiä organisaatioista tekemään yhteistyötä yksilöiden ja pk-yritysten digitaaliseen turvallisuuteen kohdistuvien riskien hallintaan liittyvien vaikutusmahdollisuuksien lisäämiseksi. Lisäksi, vaikka osan 1 toimintaperiaatteet on laadittu pääasiassa opastamaan tietyn kokoluokan ylittäviä organisaatioita niiden digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan kehyksen kehittämisessä, käsitteellisellä tasolla ne koskettavat kaikkia sidosryhmiä. Suosituksen hyväksymisen jälkeen tapahtuvan jatkotyöskentelyn odotetaan johtavan parempaan käsitykseen näiden periaatteiden käytännön vaikutuksista ja julkisten periaatteiden vaikutuksista yksilöiden ja pk-yritysten kannalta sekä mahdollisesti myös tuottavan lisäohjeistusta tältä saralta.

Asiayhteys: tilanteiden erottaminen toisistaan

Asiayhteydellä on olennainen merkitys periaatteita tulkittaessa. Oikeudelliset tai sääntelyyn liittyvät vaatimukset voivat esim. vaikuttaa siihen, millä keinoin digitaaliseen turvallisuuteen kohdistuvien riskien hallinta on toteutettavissa. Elintärkeiden palvelujen tarjoajien voidaan esim. edellyttää suorittavan virallisen riskiarvioinnin ja osoittavan, että asianmukaisiin toimiin on ryhdytty. Toimintaperiaatteita on myös sovellettava eri tavoin pk-yrityksiin ja yksilöihin johtuen näiden rajallisesta toimintakyvystä, mutta jotkut pk-yritykset ja yksilöt kuitenkin toimivat alueilla, jotka nostavat digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan tärkeyttä. Tällaisia ovat esim. elintärkeillä sektoreilla toimivat pk-yritykset tai erittäin arkaluonteisia tietoja käsittelevät henkilöt kuten lääkärit tai toimittajat.

On syytä huomata, että yksilöt voivat myös toimia sidosryhminä, jotka kehittävät ja ylläpitävät digitaalisen ympäristön osia organisaatiorakenteiden ulkopuolella. Tämä koskee mm. miljoonien käyttämien avainasemassa olevien turvakomponenttien (esim. OpenSSL tai GNU Privacy Guard [GPG][30]) joitakin ylläpitäjiä, jotka joskus työskentelevät näiden komponenttien parissa vapaaehtoispohjalta tai hyvin vähäisen budjetin ja tuen varassa. Sama pätee useimpiin sovelluskehittäjiin, jotka erään tutkimuksen mukaan ansaitsevat sovelluksellaan vähemmän kuin 500 $ kuussa.[31]

Periaatteet

Periaatteiden rakenne

Periaatteita on kahdeksan ja niihin tulisi suhtautua kokonaisuutena;[32] kaikki ovat välttämättömiä eikä yksikään niistä toimi yksinään tulkittuna tai toteutettuna, jos jokin muu niistä jätetään huomiotta. Periaatteiden numerointi heijastaa pikemminkin loogista jatkumoa kuin tärkeysjärjestystä. Periaatteet on järjestetty kahteen osioon:

- Yleiset periaatteet (1–4) kohdistuvat kaikkiin sidosryhmiin, ts. hallituksiin, julkisiin ja yksityisiin organisaatioihin ja yksilöihin, jotka käyttävät digitaalista ympäristöä joko välittömästi tai välillisesti taloudellisessa ja yhteiskunnallisessa toiminnassaan.

- Toimintaperiaatteet (5–8) kohdistuvat nimenomaan "johtajiin ja päättäjiin", joilla hallituksissa sekä julkisissa ja yksityisissä organisaatioissa olevan korkean asemansa ansiosta on parhaat edellytykset ohjata organisaatiotaan kohti asianmukaisen digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan kehyksen käyttöönottoa.

Yleiset periaatteet

Operatiivinen digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan prosessi voidaan perustaa neljän periaatteen varaan.

1. Tietoisuus, osaaminen ja vaikuttamismahdollisuudet

Digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa varten on ensin ymmärrettävä tällaisten riskien olemassaolo ja hankittava vastuullisten päätösten edellyttämä osaaminen joko opetuksen, koulutuksen, kokemuksen tai käytännön kautta (vaikutusmahdollisuudet). Digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan ensimmäinen vaihe on näin ollen tietoisuuden lisääminen ja osaamisen hankkiminen, jotta sidosryhmillä olisi mahdollisuus vaikuttaa riskienhallintaan.

Koska kaikki sidosryhmät ovat digitaalisessa ympäristössä riippuvaisia toisistaan, yhden tietämättömyys sille aiheutuvista riskeistä tai kyvyttömyys hallita niitä saattaa kasvattaa toisille aiheutuvia riskejä.[33] Näin ollen toimet tietoisuuden lisäämiseksi ja osaamisen kehit-

tämiseksi kohdeyleisön keskuudessa vaikuttavat myönteisesti kaikkiin osapuoliin auttamalla pienentämään riskitasoa kaiken kaikkiaan, edellyttäen että tietoisuus ja osaaminen siirtyvät tehokkaasti käytäntöön.

Tietoisuus riskistä on eri asia kuin tietoisuus riskitekijöistä, ts. uhkista, haavoittuvuuksista ja poikkeamista. Auto-onnettomuuden mahdolliset seuraukset – ruumiinvammat ja kuolema – tiedetään intuitiivisesti, kun taas digitaalisen ympäristön monimutkaisuus hämärtää poikkeaman ja sen seurausten välistä yhteyttä. Monet ihmiset ovat esimerkiksi tietoisia tietokoneelleen tulevan virustartunnan mahdollisuudesta, mutta he eivät välttämättä pysty käsittämään sen mahdollisia seurauksia kuten identiteettivarkaus, taloudellinen petos tai liikesalaisuuksien anastus. Vielä vähemmän näkyviä ovat toisille aiheutuvat seuraukset, esimerkiksi silloin, kun kaapattu tietokone liitetään osaksi palvelunestohyökkäyksissä käytettyä bottiverkkoa. Näin ollen tietoisuuden lisäämisessä tulisi keskittyä uhkien, haavoittuvuuksien ja poikkeamien mahdollisiin taloudellisiin ja yhteiskunnallisiin seurauksiin (ts. riskeihin) pikemminkin kuin vain riskitekijöihin itseensä. Toimilla tulisi myös kannustaa sidosryhmiä hankkimaan tarvittava riskienhallinnan osaaminen, jotta he voisivat nauttia digitaalisen ympäristön taloudellisista ja yhteiskunnallisia eduista sen sijaan, että riskit saisivat heidät luopumaan sen käytöstä.

Digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan yleisen kulttuurin kehittäminen on niin ikään eri asia kuin se tietoisuus ja osaaminen, joka jokaisella osapuolella tulisi olla riskien arvioimiseksi ja hallitsemiseksi oman roolinsa, toimintakykynsä ja toimintakenttänsä mukaisesti. On tarpeen ottaa huomioon riskien, riskitekijöiden, digitaalisen ympäristön käytön sekä kyseessä olevan taloudellisen ja yhteiskunnallisen toiminnan dynaaminen luonne. Tietoisuuden lisäämisen ja osaamisen kehittämisen tulee olla jatkuvaa prosessimaista toimintaa, joka on integroitu osaksi riskienhallintaprosessia.

Tämä periaate koskee kaikkia sidosryhmiä; hallitukset, julkiset ja yksityiset organisaatiot ja jopa yksilöt voivat lisätä tietoisuuttaan digitaaliseen turvallisuuteen kohdistuvien riskien hallinnasta ja antaa panoksensa osaamistason nostamiseen. Julkiset ja yksityiset organisaatiot kehittävät asiakkailleen ja sidosryhmilleen kohdistettuja hankkeita oman riskienhallintakehyksensä tueksi. Jotkut organisaatiot, erityisesti ICT-alalla toimivat yritykset sekä voittoa tavoittelemattomat yhteisöt, ovat merkittävässä roolissa tukiessaan tietoisuutta lisääviä hankkeita, jotka on kohdennettu joko suurelle yleisölle tai nimenomaisille ryhmille kuten lapsille, teineille, opiskelijoille, vanhuksille jne. Hankkeet voivat olla monimuotoisia ja hyödyntää kaikenlaisia medioita, kursseja, paikan päällä tapahtuvaa koulutusta jne. Suosituksenkin kannalta olennainen kohderyhmä ovat johtajat ja päättäjät itse. Heillä on parhaat edellytykset ohjata organisaatiotaan kohti kulttuurillista ja organisatorista muutosta. Yleisten linjausten osalta viimeksi kuluneen kymmenen vuoden aikana niin hallitukset kuin yksityinenkin sektori ovat tehneet merkittäviä panostuksia yleisen tietoisuuden lisäämiseksi.[34] Näitä panostuksia tulisi jatkaa kaikkien talouden ja yhteiskunnan toimijoiden eri ryhmien tavoittamiseksi sekä heidän osaamisensa kehittämiseksi.

Asianmukaisen tietoiset ja osaavat sidosryhmät, joilla on mahdollisuus vaikuttaa, ovat kykeneviä ottamaan vastuuta (periaate 2).

2. Vastuullisuus

Yhteiskunnan kantavia periaatteita on se, että teoista tulee kantaa niin itseen kuin toisiinkin kohdistuvat seuraukset. Näin ollen kaikkien sidosryhmien tulisi ottaa vastuu digitaaliseen turvallisuuteen kohdistuvien riskien hallinnasta oman roolinsa, toiminta-alueensa ja toimintakykynsä mukaan kuten yllä on esitetty.

Tämä periaate ei koske vastuuta sanan juridisessa merkityksessä, ts. oikeudellisia seurauksia, jotka vaihtelevat oikeusjärjestyksen ja toiminta-alueen mukaan. Vastuullisuusperiaatteessa sen sijaan ilmennetään suosituksen johdantoa, jonka mukaan ”hallitukset, julkiset ja yksityiset organisaatiot sekä yksilöt jakavat asiayhteyteen ja rooliinsa perustuen vastuun digitaaliseen turvallisuuteen kohdistuvien riskien hallinnasta sekä digitaalisen ympäristön suojelemisesta”. On käynyt mahdottomaksi turvautua johonkin ulkopuoliseen tahoon kaikissa digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan osatekijöissä. Vastuu on jaettua vastuuta; jokainen on tietyssä määrin vastuussa. Kaikkien sidosryhmien tulisi pohtia rooliaan, toiminta-aluettaan ja toimintakykyään, ja määritellä näiden perusteella mitä vastuuta niiden tulisi ottaa.

Vastuullisuuden ajatus korostaa digitaalisen ympäristön samankaltaisuutta muiden ympäristöjen kanssa; taloudellisten ja yhteiskunnallisten tavoitteiden saavuttamiseksi on hyväksyttävä tietty digitaaliseen turvallisuuteen kohdistuva riskitaso.

Tilannetta voi verrata liikenneturvallisuuteen. Kaikki sidosryhmät ovat vastuussa siitä roolinsa, toiminta-alueensa ja toimintakykynsä puitteissa. Kuljettajien tulee osata ajaa ja heidän tulee noudattaa perustavanlaatuisia turvallisuussääntöjä; päihtyneenä ei saa ajaa, nopeusrajoituksia täytyy noudattaa, turvavyötä pitää käyttää, muu liikenne tulee huomioida jne. Autonvalmistajien tulee suunnitella autot siten, että suunnittelusta tai mekaanisista häiriöistä johtuva onnettomuuksien mahdollisuus minimoidaan (ts. välttää haavoittuvuuksia kuten esimerkiksi puutteellisia jarruja) ja sisällyttää autoihin suojamekanismeja (ts. turvaominaisuuksia kuten turvatyynyjä, taustapeilejä jne.). Tienpitäjien tulee myös huomioida onnettomuuksien mahdollisuus teiden suunnittelussa; suojakaiteet, kiertoliittymät, liikennevalot, liikennemerkit jne. Hallitusten tulee määritellä autoilua, autonvalmistusta ja liikennettä koskevat säännöt sekä huolehtia niiden täytäntöönpanosta. Hallitusten tulee myös tarjota pelastuspalveluja (ts. huolehtia varautumisesta). Jos jokin näistä osatekijöistä jää puutteelliseksi, se lisää kaikkiin kohdistuvan riskin tasoa.

Digitaalista ympäristöä taloudellisten ja yhteiskunnallisten tavoitteiden saavuttamiseksi käyttävät sidosryhmät (kuljettajat) hyväksyvät tietyn digitaaliseen turvallisuuteen kohdistuvan riskitason eli mahdolliset kielteiset seuraukset. Heidän tulisi hallita tätä riskiä, ts. pienentää se hyväksyttävälle tasolle, alempana esitettyjen neljän toimintaperiaatteen perusteella. Heidän tulisi myös pystyä selittämään toimiensa tai laiminlyöntiensä syyt (vastuuvelvollisuus).

Kaikki tahot eivät kuitenkaan ole tasavertaisessa asemassa vastuun ja vastuuvelvollisuuden suhteen. Heidän tulee kyetä riskienhallintaan mm. informaation, tietojen, osaamisen, resurssien, työkalujen ja määräysvallan sekä myös tekniikan osalta. Eri tahojen kyky tunnistaa, arvioida ja hallita riskejä vaihtelee merkittävästi, eikä joidenkin (esim. yksilöiden ja pk-yritysten) voida kohtuudella odottaa tunnistavan, arvioivan ja hallitsevan riskejä samalla tavalla kuin esim. tahot, joilla on käytössään merkittävästi laajemmat resurssit. Kuten edellä

on todettu, jatkotyöskentely tämän periaatteen täytäntöönpanon edistämiseksi yksilöiden ja pk-yritysten keskuudessa, sekä tähän liittyvien haasteiden ja mahdollisten edistämiskeinojen parissa olisi erittäin tervetullutta.

Digitaalisen ympäristön komponentteja kuten ohjelmistoja ja laitteita sekä verkkoinfrastruktuuria kehittävien, ylläpitävien tai hallinnoivien sidosryhmien (aiemman vertauksen autonvalmistajat ja tienpitäjät) tulisi luoda edellytykset käyttäjien vastuullisten riskienhallintapäätösten tekemiselle. Tämä käsittää mm. normien ja hyvien käytäntöjen käyttöönoton, asianmukaisten turvatoimenpiteiden sisällyttämisen itse teknisiin komponentteihin, sekä käyttäjien vaikutusmahdollisuuksien lisäämisen tarvittavan tiedon ja avun tarjoamisen kautta, ottaen huomioon riskien dynaamisen luonteen.

Hallitusten tulisi osaltaan kehittää kansallisia strategioita ja ottaa käyttöön hankkeita sekä toimenpiteitä digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan edistämiseksi kaikkien sidosryhmien parissa. Useimmilla OECD-hallituksilla on jo olemassa monia tarvittavista osatekijöistä kuten sääntely, lainsäädäntö (esim. tietoverkkorikollisuuteen ja yksityisyydensuojaan liittyen), reagointivalmiudet (CSIRT-yksiköiden kautta), opetus ja koulutus, julkisen ja yksityisen sektorin väliset kumppanuudet jne. Politiikkaa alettiin muotoilla strategisemmin ja lähestymistapaa yhdenmukaistaa jo useita vuosia sitten[35] esimerkiksi ottamalla käyttöön uusia tai parempia koordinointimekanismeja kuten erillisvirastoja. Kuten osassa 2 todetaan, digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa koskevat linjaukset ovat lähtökohtaisesti horisontaalisia ja edellyttävät yhteistyötä, ei vain hallituksen sisällä, vaan myös kaikkien sidosryhmien kanssa niin kansallisella, alueellisella kuin kansainväliselläkin tasolla. Kyseessä ovat pitkän tähtäimen strategiset linjaukset.

Toisin kuin liikenneturvallisuudessa, digitaalisessa ympäristössä sidosryhmät ovat paljon enemmän yhteydessä toisiinsa ja riippuvaisia toisistaan. Näin ollen vastuullisuusperiaatteessa todetaan, että sidosryhmien tulisi huomioida päätöstensä mahdolliset vaikutukset toisiin. Tämä koskee esim. i) kolmansia osapuolia, joiden henkilötietoja käsitellään, ii) digitaalista ekosysteemiä kokonaisuutena, jonka suojeleminen on kaikkien sidosryhmien yhteisen edun mukaista[36] ja jonka suojelua tai heikentymistä heidän omat toimensa tai laiminlyöntinsä voivat edesauttaa, ja iii) talouden ja yhteiskunnan toimivuutta kaiken kaikkiaan, koska digitaalista ympäristöä käytetään elintärkeiden infrastruktuurien ja palvelujen osana. Parhaiden käytäntöjen käyttöönoton ja toisten etujen huomioimisen lisäksi on lukuisia muitakin keinoja kantaa yhteistä vastuuta; standardien ja parhaiden käytäntöjen noudattaminen, osallistuminen standardeja käsitteleviin elimiin, yhteistyö toisten sidosryhmien kanssa myös maantieteellisten ja tieteenalojen rajojen yli jne.

Kaikkien sidosryhmien tulisi myös ottaa vastuuta ihmisoikeuksien ja perusarvojen huomioimisesta digitaaliseen turvallisuuteen kohdistuvien riskien hallinnassa (periaate 3) sekä tehdä yhteistyötä (periaate 4).

3. Ihmisoikeudet ja perusarvot

Yhteiskunnan perussäännöt pätevät myös digitaalisessa ympäristössä. Näin ollen ihmisoikeudet ja perusarvot ulottuvat myös sinne ja niitä tulee suojella sielläkin. Näitä oikeuksia ja arvoja käsittelevät lukuisat kansainväliset säädökset, joissa niihin saatetaan viitata muillakin termeillä kuten ”ydinarvot”, ”perusvapaudet” jne. Tärkeitä kansainvälisiä säädöksiä tässä suhteessa ovat mm. ihmisoikeuksien yleismaailmallinen julistus [Universal Declaration of Human Rights], kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus [International Covenant on Civil and Political Rights] sekä taloudellisia, sosiaalisia ja kulttuurisia oikeuksia koskeva yleissopimus [International Covenant on Economic, Social and Cultural Rights].[37]

Digitaaliseen turvallisuuteen kohdistuvien riskien hallintaan liittyvillä turvatoimenpiteillä[38] voi olla ihmisoikeuksia ja perusarvoja vahvistava tai heikentävä vaikutus käyttötavasta riippuen. Ne voivat vaikuttaa ilmaisunvapauteen, vapaaseen tiedonkulkuun, tietojen ja viestinnän luottamuksellisuuteen, yksityisyyden ja henkilötietojen suojaan, avoimuuteen ja menettelyjen oikeudenmukaisuuteen.[39] Turvatoimenpiteet voivat esimerkiksi vahvistaa yksityisyydensuojaa tai mahdollistaa nimettömyyden väärinkäytösten ilmiantajille ja ihmisoikeusaktivisteille. Niiden avulla voidaan myös mahdollistaa kansalaisten laiton valvonta tai estää pääsy aktivistien tarjoamaan sisältöön. Ne voivat vaikuttaa sellaisiin oikeuksiin ja arvoihin, joita periaatteessa ei ole lueteltu. Näin ollen vastuullisuus edellyttää digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa koskevien päätösten tekemistä näihin oikeuksiin ja arvoihin kohdistuvien seurausten valossa.

Periaate koskee kaikkia sidosryhmiä. Organisaatioiden tulisi tiedostaa, että ihmisoikeuksia ja perusarvoja heikentävien digitaaliseen turvallisuuteen kohdistuvien toimien käyttöönotto on riski niiden imagolle ja uskottavuudelle, ja saattaa johtaa oikeudelliseen vastuuseen. Niiden tulisi hyödyntää digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan prosessin systemaattista luonnetta arvioidakseen riskienhallintapäätöstensä vaikutuksia ihmisoikeuksiin ja perusarvoihin sekä tehdä tarvittavat muutokset. OECD:n yksityisyydensuojaa koskevissa ohjeissa edellytettyjen yksityisyydenhallintaohjelmien täytäntöönpanoa hyödyttäisi niiden sisällyttäminen olemassa oleviin riskienhallintakehyksiin ja hallintorakenteisiin.[40]

Digitaalista ympäristöä suunnittelevien, ylläpitävien tai hallinnoivien sidosryhmien (esim. ICT-alan ammattilaisten) tulisi pohtia, onko heidän ICT-alan tuotteisiin ja palveluihin sisällyttämiään turvaominaisuuksia mahdollista käyttää ihmisoikeuksien heikentämiseen, ja ryhtyä tarvittaviin toimiin. Toisinaan mahdollinen vaikutus ihmisoikeuksiin riippuu ICT-alan tuotteiden ja palvelujen käyttötavasta eikä vaikutusta ole ehkä mahdollista estää suunnittelutoimin. Tällaisissa tapauksissa ICT-alan ammattilaisten tulisi harkita mahdollisen ihmisoikeuksiin kohdistuvan kielteisen vaikutuksen tiedottamista näiden tuotteiden ja palveluiden käyttäjille sekä neuvoa heitä, miten se voidaan estää. Hallitusten tulisi myös varmistaa, että niiden digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan edistämistä koskevat linjaukset tukevat ja kunnioittavat lakeja ja säännöksiä ja ovat hallitusten tällä alueella olevien kansainvälisten velvoitteiden mukaisia (vrt. osa 2. A. 2).

Ns. kultaista sääntöä tai vastavuoroisuuden etiikkaa heijastaen (”kohtele toisia niin kuin haluaisit itseäsi kohdeltavan”) sidosryhmien tulisi myös tunnustaa, että niiden toimet tai lai-

minlyönnit voivat vahingoittaa toisia ja vaikuttaa myös digitaaliseen ympäristöön itseensä. Näin ollen niiden tulisi toimia eettisesti kestävällä tavalla, toisin sanoen kunnioittaa toisten ja koko yhteiskunnan oikeutettuja etuja. Eettinen toiminta on erityisesti tärkeätä koska digitaalisen ympäristön avoin, globaali ja verkottunut luonne voi vahvistaa sidosryhmien toimien tai laiminlyöntien vaikutusta.

Digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan käytäntöjen ja menettelytapojen osalta organisaatioiden yleisenä linjana tulisi olla avoimuus. Ohjeet tämän yleisen linjauksen toimeenpanon yksityiskohtien osalta vaativat kuitenkin jatkotyöskentelyä, jossa kiinnitetään erityistä huomiota tapauksiin, joissa liiallinen avoimuus saattaisi heikentää turvallisuutta, sekä pohditaan mahdollisia valvontamekanismeja.

4. Yhteistyö

Kuten edellä on jo esitetty, digitaalisen ympäristön globaali verkottuneisuus luo sidosryhmien välille keskinäistä riippuvuutta. Tällä on myönteisiä puolia, kuten kaikkien osapuolten yhteiseen voimaan perustuvien taloudellisten ja yhteiskunnallisten hyötyjen mahdollistaminen kullekin osapuolelle. Sillä on myös kielteisiä puolia, kuten lisääntynyt monimutkaisuus, uhkien ja haavoittuvuuksien leviämisen helpottuminen, ja mahdollisesti kasvava kollektiivinen riski. Yhteistyö on välttämätöntä, koska sidosryhmät ovat riippuvaisia sekä toisistaan että digitaalisesta ympäristöstä.

Monet digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan osatekijät edellyttävät jossain määrin yhteistyötä[41] eikä yhden tahon ole yksinään mahdollista hoitaa niitä. Näin ollen yhteistyö läpäisee kaikki suosituksessa esitetyt periaatteet. Esimerkkeinä: i) tietoisuus ja osaaminen edellyttävät sitä, että tiedostavammat ja osaavammat valistavat, opettavat ja kouluttavat toisia, joiden on tarpeen ymmärtää tietoisuuden ja vaikutusmahdollisuuksien lisääntymisen olevan heidän etujensa mukaista, ii) vastuu jakautuu kaikkien sidosryhmien kesken niiden roolien, toimintakyvyn ja toiminta-alueen mukaisesti ja sidosryhmien yhteistyö on näin ollen välttämätöntä, jotta toisiaan täydentävissä rooleissa olevat sidosryhmät voivat kantaa vastuunsa yhdenmukaisesti, ja iii) vaikka ne on yleensä kodifioitu laeissa, ihmisoikeudet ja perusarvot voidaan ilmaista myös etiikan kautta ja niiden asianmukainen ymmärtäminen ja kunnioittaminen edellyttävät osapuolten välistä dialogia ja keskustelua. Yhteistyö on myös avainasemassa toimintaperiaatteiden suhteen, sillä niiden täytäntöönpano edellyttää laajamittaista yhteistyötä niiden sidosryhmien välillä, jotka vastaavat taloudellisen ja yhteiskunnallisen toiminnan harjoittamisesta ja niiden, jotka vastaavat toiminnan alustana olevan digitaalisen ympäristön tarjoamisesta. Yhteistyö on myös välttämätöntä turvatoimenpiteiden, innovaatiotoiminnan ja varautumistoimien täysimittaiseksi toimeenpanemiseksi. Tämä koskee myös ei-teknisiä näkökulmia, joiden osalta ihmisten on tarpeen muuttaa käyttäytymistään. Digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan tueksi on lisäksi otettava käyttöön hallintaprosesseja.

Kaikkien sidosryhmien tulisi osallistua digitaaliseen turvallisuuteen kohdistuvien riskien parempaan hallintaan tähtäävään yhteistyöhön ja tässä yhteistyössä tulisi huomioida heidän eri roolinsa. Yhteistyötä tulisi tapahtua myös organisaatioiden sisällä mahdollisten siilojenkin yli. Ylimmän tason johdolla voi olla olennainen rooli varmistettaessa, että sisäi-

set riskienhallinnan politiikat ja kehykset luovat edellytykset toimivalle yhteistyölle. Olennaista on yhteistyö niiden organisaation osien välillä, jotka käyttävät digitaalista ympäristöä taloudellisessa toiminnassa (bisnespuoli), niiden, jotka tarjoavat kyseisen ympäristön (ICT-puoli), sekä niiden, jotka varmistavat lakien ja säännösten noudattamisen.

Yhteistyötä voi tapahtua monella eri tavalla. Siinä osapuolina voivat olla mm. seuraavat:

- Organisaation eri osat eli organisaation sisäinen yhteistyö esim. uhkien ja haavoittuvuuksien mahdollisen leviämisen estämiseksi eri yrityksiin ja tuotantoketjun eri osapuoliin. Myös hallituksen eri osat kuten ministeriöt ja virastot sekä hallinnon eri tasot (kunnallinen/maakunnallinen/kansallinen) sekä alihankkijat voivat niin ikään tehdä yhteistyötä vastaavasti;

- Samalla talouden sektorilla toimivat organisaatiot, joihin kohdistuu yhteisiä uhkia. Joissakin tapauksissa, kuten esimerkiksi elintärkeiden infrastruktuurien osalta, hallitukset saattavat kannustaa tällaiseen yhteistyöhön;

- Julkinen ja yksityinen sektori, esimerkkinä yksityisen sektorin yhteistyö lainvalvontaviranomaisten, koulutuslaitosten ja muiden julkisten tahojen kanssa;

- Organisaatiot sekä niiden kuluttajat ja käyttäjät, ja laajemmin katsoen kansalaisyhteiskunta kokonaisuudessaan.

Yleisissä menettelyissä on tarpeen ottaa mukaan useita sidosryhmiä, jotta voidaan luoda edellytykset laajemmalle osallistumiselle ja parempien linjausten kehittämiselle (osa 2. A. 4). Käytännössä yhteistyön muotoja voivat olla esim. julkisen ja yksityisen sektorin kumppanuudet ja hankkeet eri aloilla kuten tietoisuus ja osaaminen, tietoverkkorikollisuus (esim. yhteistyö lainvalvontaviranomaisten kanssa), CSIRT/CERT-yksiköt[42], tietojen vaihtaminen ja jakaminen[43] jne. Osassa 2 ja erityisesti sen kohdissa B. 3 ja B. 4 annetaan useita esimerkkejä alueista, joilla julkinen ja yksityinen sektori[44] voivat tehdä yhteistyötä.

Yhteistyön tulisi tarvittaessa ulottua myös rajojen yli.

Toimintaperiaatteet

Digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan prosessi esiteltiin tämän asiakirjan osiossa "Avainkäsitteet". Alla esitetyt elementit keskittyvät kuhunkin periaatteeseen. Yleisesti ottaen on kuitenkin tärkeätä mieltää digitaaliseen turvallisuuteen kohdistuvien riskien hallinta luovaksi ja ketteräksi päätöksentekoprosessiksi, joka voi luoda mahdollisuuksia hyötyjen lisäämiseen pitämällä toiminnan mahdollisimman herkkänä reagoimaan sen jatkuvassa muutostilassa olevaan ja näin ollen epävarmaan asiayhteyteen. Se edustaa **dynaamista reaktiota dynaamiseen haasteeseen**, joka tarjoaa sidosryhmille onnistumisen todennäköisyyttä lisäävää joustavuutta ja sopeutumiskykyä. Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta on siten luonteeltaan:

- ***Toistuvaa***: taloudellinen ja yhteiskunnallinen toiminta, digitaalinen ympäristö, jossa toiminta tapahtuu ja digitaaliseen turvallisuuteen kohdistuvat riskit ovat jatkuvassa muutostilassa. Muutosten tahdissa pysyminen vaatisi ihannetapauksessa riskien jatkuvaa tarkastelua. Käytännössä olisi suotavaa luoda toiminnan ohjaama yleinen prosessi sekä tarkennettu malli, jota ohjaavat tapahtumat kuten uusien uhkien ja haavoittuvuuksien esiinnousu, tapahtuneet uudet poikkeamat ja kehitys toiminta-alueen muissa osatekijöissä. Riskienhallinnan toistuvaa luonnetta edustavat Kaaviossa 1 nuolet, jotka palaavat kierroksen lopusta riskienarviointivaiheeseen sekä toimintaan liittyvän innovaatiotoiminnan osalta myös suunnitteluvaiheeseen.

- ***Kokonaisvaltaista***: koska digitaalinen ympäristö on verkottunut, riskienhallinnassa tulisi olla käytössä kattava lähestymistapa. Riskienhallinnan tulisi esimerkiksi kattaa kyseessä olevan toiminnan koko arvoketju, sillä yhden ketjun osan haavoittuvuuksia saatetaan käyttää hyväksi ketjun toisesta osassa lähtöisin olevaan uhkaan ja näin aiheuttaa seurauksia kolmanteen ketjun osaan. Sen tulisi myös käsittää elementtejä, jotka liittyvät arvoketjussa mukana oleviin ihmisiin (henkilöihin), prosesseihin (ts. sääntöihin ja menettelytapoihin) ja tekniikoihin. Näin ollen sitä tulisi hallita muiden riskiluokkien rinnalla sen sijaan, että kehitettäisiin päällekkäisiä prosesseja tai menetelmiä.

- ***Systemaattista***: monimutkaisuuden asteeltaan kokonaisvaltainen riskienhallintaprosessi todennäköisesti vastaa kyseessä olevaa organisaatiota ja toimintaa. Systemaattinen lähestymistapa on paras keino hallita kasvava monimutkaisuus. Eri osatekijät tulee eritellä ja niitä käsitellä erikseen kokonaisuuden puitteissa.

Kehittämällä digitaaliseen turvallisuuteen kohdistuvien riskien hallintaan jatkuva, kokonaisvaltainen ja systemaattinen lähestymistapa luodaan edellytykset sille, että riskejä voidaan hallita mahdollisuuksien rinnalla kuten jäljempänä esitetään (innovaatiotoimintaperiaate). Se on myös kattavampi ja soveliaampi lähestymistapa ihmisoikeuksien ja perusarvojen sekä muiden oikeutettujen etujen huomioimiseen, samoin kuin turvatoimenpiteiden mahdollisten ihmisoikeuksiin ja perusarvoihin sekä digitaaliseen ympäristöön kohdistuvien vaikutusten huomioimiseen.

Riskienhallintaa voidaan toteuttaa erilaisten menetelmien, standardien ja parhaiden käytäntöjen avulla. Niistä voi olla hyötyä usealla eri tasolla kokonaisprosessissa, kuin myös sen eri osissa, kuten turvatoimenpiteissä tai jatkuvuuden hallinnassa ja varautumisessa.

5. Riskien arviointi- ja käsittelyprosessi

Jatkuva riskien arviointi ja käsittely on tarpeen sen varmistamiseksi, että turvallisuuteen liittyvät päätökset ovat soveltuvia ja oikeasuhteisia riskiin sekä kyseessä olevaan taloudelliseen ja yhteiskunnalliseen toimintaan nähden.

Riskien arviointi on analyyttinen prosessi, joka voidaan jakaa useaan alaprosessiin. Niissä riskit i) tunnistetaan; riskitekijät selvitetään menettelyssä, jossa usein hyödynnetään kokemuksia, historiallisia tietoja, teoreettisia analyyseja, asiantuntijoiden näkemyksiä jne. ii) analysoidaan; ts. riskit ymmärretään ja niiden taso määritellään. Kuten yllä on todettu, tämä taso ilmaistaan usein todennäköisyyden sekä kyseessä olevaan taloudelliseen ja yhteiskunnalliseen toimintaan kohdistuvan vaikutuksen kautta, ja iii) arvioidaan; ts. riskiä verrataan hyväksyttävään riskin tasoon suhteessa toimintaan sekä siltä odotettuihin taloudellisiin ja yhteiskunnallisiin tavoitteisiin ja hyötyihin.

Vaikka riskien arvioinnissa tulisi pääasiassa keskittyä epävarmuuden mahdollisiin seurauksiin omille tavoitteille, siinä tulisi tarvittaessa ottaa huomioon myös mahdolliset seuraukset toisille siltä osin kuin toiset ovat osallisina asiassa tai vaikutukset saattavat ulottua toisiin (esim. yksityisyydensuoja, Laatikko 4). Riskien arvioinnissa tulisi myös ottaa huomioon epävarmuuden mahdolliset vaikutukset digitaaliseen ekosysteemiin kokonaisuutena (kollektiivinen riski).

Riskien käsittely[45] on prosessi, jossa riskien arvioinnin tulosten perusteella päätetään, miten riskejä muokataan niiden pienentämiseksi hyväksyttävälle tasolle suhteessa toiminnasta odotettuihin taloudellisiin ja yhteiskunnallisiin hyötyihin, huomioiden samalla mahdolliset vaikutukset toisten oikeutettuihin etuihin (”hyväksyttävä riskin taso”). Tällaisia oikeutettuja etuja ovat myös ihmisoikeudet ja perusarvot (periaate 3) sekä digitaalisen ympäristön toimivuus.

Riskien käsittelyyn on yleensä neljä eri mahdollisuutta (ks. Kaavio 1) ja niitä voidaan myös yhdistellä:

- Riskin hyväksyminen: “otetaan riski” ja hyväksytään epävarmuuden vaikutus tavoitteisiin aina osittaiseen tai täydelliseen epäonnistumiseen asti. Jos toimintaan ryhdytään, riskiä ei voida täysin poistaa ja näin ollen tietty ”jäännösriski” täytyy aina hyväksyä (vrt. periaate 2, Vastuullisuus). Yleisesti ottaen riskienhallinta on taloudellisesti tehokasta, kun toiminnan harjoittamisesta saadut hyödyt ovat jäännösriskiä suuremmat.

- Riskin pienentäminen hyväksyttävälle tasolle. Keinoja tässä ovat i) riskiarvioinnissa tunnistettuja haavoittuvuuksia hyväksi käyttäviltä mahdollisilta uhkilta suojaavien turvatoimenpiteiden valinta ja käyttö (periaate 6), ii) toiminnan muuttaminen esimerkiksi suunnittelemalla tai toteuttamalla se eri tavalla, mikä saattaa johtaa innovaatioihin (periaate 7), ja iii) toiminnallisten varautumistoimien määrittäminen ja tarvittaessa käyttö poikkeamista selviämiseksi (periaate 8).

- Riskin siirtäminen: epävarmuuden ei-toivottujen toiminnan tavoitteisiin kohdistuvien vaikutusten siirtäminen toiselle taholle esimerkiksi sopimusteitse, kuten vakuutuksen kautta. Vakuuttaminen digitaaliseen turvallisuuteen kohdistuvien riskien varalta saattaisi olla hyödyllinen jatkotyöskentelyn aihepiiri.

- Riskin välttäminen: riskin poistaminen jättämällä toiminta harjoittamatta tai harjoittamalla sitä ilman digitaalista elementtiä.

”Hyväksyttävän riskin tason” määrittelee se sidosryhmä, joka harjoittaa toimintaa ja jolle riski aiheutuu. Riskinottohalukkuus on termi, jota käytetään kuvaamaan, miten paljon riskiä sidosryhmä on valmis hyväksymään voidakseen harjoittaa tiettyä toimintaa. Riskinottohalukkuuteen vaikuttavat useat toimintaan ja sen tavoitteisiin, samoin kuin organisaation kulttuuriin ja tyyliin, markkinaolosuhteisiin ja tekniseen ympäristöön jne. liittyvät tekijät. Lainsäädännölliset ja sääntelylliset puitteet saattavat joskus asettaa rajoja riskinottohalukkuudelle. Mikäli riskiä ei voida hyväksyä tai välttää täysin, on tarpeen päättää, miten riskiä voidaan pienentää hyväksyttävälle tasolle tai miten riski voidaan siirtää.

6. Turvatoimenpiteet

Vaikka turvatoimenpiteet ovat ehdottoman välttämättömiä taloudellisen ja yhteiskunnallisen toiminnan suojelemiseksi, niillä voi olla myös kielteisiä vaikutuksia toimintaan. Periaate korostaa, että paras keino varmistaa turvatoimenpiteiden soveltuvuus ja oikeasuhteisuus kyseessä olevaan taloudelliseen ja yhteiskunnalliseen toimintaan nähden on valita, toteuttaa ja kehittää turvatoimenpiteitä riskien arvioinnin ja käsittelyn perusteella (ks. yllä, digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan määritelmä).

Turvatoimenpiteet voivat esimerkiksi kasvattaa toiminnan kustannuksia sekä vaikuttaa sen käytettävyyteen, toimivuuteen ja kehitysmahdollisuuksiin. Moniin teknisiin turvatoimenpiteisiin saattaa liittyä jonkinasteista tietovirtojen vähenemistä (esim. palomuurit) tai ne saattavat lisätä menettelyssä tarvittavien vaiheiden määrä (esim. tunnistautuminen). Jotkut lisäävät monimutkaisuutta (esim. salausmenetelmät) ja edellyttävät toimivuuteen liittyviä kompromisseja pysyäkseen hallittavina. Esimerkkejä ihmisoikeuksiin ja perusarvoihin mahdollisesti vaikuttavista turvatoimenpiteistä ovat mm. sellaiset, jotka edellyttävät pääsyä henkilötietoihin, kuten liikennevirtojen seuranta ja analysointi turvallisuusuhkien havaitsemiseksi (esim. pakettien syvätarkastusteknologiaa eli deep packet inspection, DPI). Turvallisuusalan ammattilaisilla on usein pääsy henkilötietoihin työnsä puitteissa. Heidän saattaa olla tarpeen esimerkiksi päästä käsiksi henkilökohtaisiin käyttäjätileihin poikkeaman selvittämistä varten. He saattavat myös joutua siirtämään poikkeamaan liittyviä henkilötietoja kolmansille osapuolille jatkoanalyysia tai teknisiä tutkimuksia varten. Kriisinhallinta voi myös synnyttää tilanteita, joissa palvelu joudutaan sulkemaan, jotta uhka ei leviäisi. Tällöin heikennetään käyttäjien oikeuksia. Digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan prosessi tarjoaa systemaattisen lähestymistavan sen varmistamiseksi, että turvatoimenpiteiden mahdolliset kielteiset vaikutukset otetaan huomioon ja että niihin puututaan asianmukaisin välinein ja käytännöin.

Turvatoimenpiteitä on luonteeltaan monenlaisia. Ne voivat olla digitaalisia (esim. tietoturvaohjelmistot), fyysisiä (esim. lukitukset, kamerat ja aidat) tai sekoitus molempia (esim. älykortit). Ne voivat liittyä ihmisiin (esim. koulutus), prosesseihin (esim. organisaation säännöt ja käytännöt) tai tekniikkaan (esim. salausmenetelmät). Turvatoimenpiteet voivat myös olla luonteeltaan oikeudellisia (esim. sopimukset) tai liittyä menettelytapoihin (esim. standardit) tai johtamiseen jne. Tässä on vain joitakin esimerkkejä mahdollisista luokituksista.

Turvatoimenpiteillä puututaan myös haavoittuvuuksiin. Samoin kuin digitaalisen ympäristön uhkat niin myös sen haavoittuvuudet ovat jatkuvassa muutostilassa. Organisaatioiden tulisi näin ollen jatkuvasti selvittää ja arvioida haavoittuvuuksia ja puuttua niihin mahdollisimman nopeasti. Vain näin on mahdollista pysyä uusien ja vasta esiin nousevien uhkien edellä.

Koska riski on luonteeltaan dynaamista, turvatoimenpiteet tulisi valita toiminnan suunnitteluvaiheessa ja niitä tulisi päivittää toiminnan koko elinkaaren ajan noudattaen yllä esitettyä prosessimaista, kokonaisvaltaista ja systemaattista lähestymistapaa. Jotkut toimenpiteet on syytä sisällyttää toimintaan ”sisäänrakennettuina” eli ydinkomponenttina. Syitä tähän voi olla se, että turvatoimenpiteet ovat välttämättömät tai se, ettei kyseistä toiminnan osaa ole mahdollista muokata jälkikäteen. Koska riski kuitenkin on luonteeltaan dynaamista, jatkuvan riskien arvioinnin ja hallinnan prosessin osana tulisi harkintaan ottaa myös muita turvatoimenpiteitä.

Digitaalisen ympäristön suunnittelussa, hallinnoinnissa ja hoidossa mukana olevien sidosryhmien tulisi aina noudattaa hyviä käytäntöjä ja toimia turvatoimenpiteiden toteuttamisessa standardien mukaisesti. Turvatoimenpiteisiin voidaan soveltaa monia yleisiä ja sektorikohtaisia standardeja ja hyviä käytäntöjä. Tällaisten standardien mukainen toiminta yleensä auttaa turvallisuuteen kohdistuvien riskien hallinnan yleisimpien osatekijöiden käsittelyssä ja sallii näin kohdentaa enemmän aikaa ja resursseja organisaatiolle tai toiminnalle ominaisiin erityispiirteisiin ja niiden ongelmiin.

ICT-alan tuotteita ja palveluja kehittävien ja ylläpitävien sidosryhmien tulisi sisällyttää niihin turvatoimenpiteitä sekä tarjota niiden käyttäjille tietoja ja tarvittaessa myös apua käyttöön liittyvien riskien arviointiin ja käsittelyyn.

7. Innovaatiotoiminta

Turvatoimenpiteiden käyttöönoton lisäksi sidosryhmät voivat vähentää altistumistaan digitaaliseen turvallisuuteen kohdistuville riskeille toimintaan sekä turvatoimenpiteisiin liittyvän innovaatiotoiminnan kautta. Innovaation määritellään yleensä olevan markkinoille tuotu uusi tai olennaisesti parannettu tuote (tuote tai palvelu), käyttöön otettu uusi tai olennaisesti parannettu prosessi, käyttöön otettu uusi markkinointimenetelmä tai käyttöön otettu uusi organisatorinen menetelmä liiketoimintakäytännöissä, työorganisaatiossa tai ulkoisissa suhteissa.[46]

Digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan yhteydessä riskejä pienentävä innovaatiotoiminta voi saada monia muotoja, jotka eivät välttämättä liity digitaalisuuteen. Se voi esimerkiksi vaikuttaa organisaation taloudelliseen tai liiketoimintamalliin, prosesseihin kuten maksutapoihin, tai jopa tuotteen fyysisten, juridisten tai muiden

ei-digitaalisten elementtien uudelleensuunnitteluun. Epävarmuuden toimintaan kohdistuvien mahdollisten vaikutusten pienentämiseksi käyttöön otettu innovaatio saattaa itsessään luoda toiminnan muihin osa-alueisiin liittyvää epävarmuutta. Sen tulisi näin ollen käynnistää riskien uudelleenarvioinnin ja uudelleen käsittelyn prosessi.

Digitaaliseen turvallisuuteen kohdistuvien riskien hallinnasta voi näin tulla innovaatiotoiminnan ajuri. Tämä edellyttää, että asiaa lähestytään olennaisena osana toimintaan liittyviä taloudellisia ja yhteiskunnallisia päätöksentekoprosesseja. Jos digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa koskevat päätökset eristetään taloudellisten ja yhteiskunnallisten päätösten tekemisen ydinprosessista, niitä on vaikeampi käsittää mahdollisiksi innovaatiotoiminnan ajureiksi ja niitä voidaan pikemminkin pitää esteinä tai rajoitteina kuin kannusteina kilpailuedun saamiselle.

Riski, innovaatiotoiminta sekä taloudellinen ja yhteiskunnallinen kehitys liittyvät itse asiassa hyvin läheisesti toisiinsa. Esimerkiksi monet keksinnöt ja edistysaskeleet kautta historian voidaan jäljittää haluun tai tarpeeseen hallita epävarmuutta; säätilaan liittyvät epävarmuudet esimerkiksi mitä suurimmassa määrin johtivat sateenvarjon keksimiseen, mutta myös merkittäviin edistysaskeliin maataloudessa sekä ruoka-aineiden säilytyksessä, jalostuksessa ja jakelussa nälänhädän riskin pienentämiseksi. Jatkotyöskentely riskin ja innovaatiotoiminnan suhteen laajemmaksi ymmärtämiseksi digitaalisessa ympäristössä olisi suotavaa.

Tästä näkökulmasta katsoen periaatteelle voidaan myös antaa laajempi tulkinta kuin vain toteamus, että riskienhallinnan voidaan katsoa olevan yleinen lähestymistapa niin arvon säilyttämiseen kuin luomiseenkin. Riskienhallinnan avulla organisaatiot voivat systemaattisesti reagoida epävarmuuteen lisätäkseen onnistumisen todennäköisyyttään alati muuttuvassa ympäristössä. Kuten yllä on todettu, epävarmuuden ei tarvitse vaikuttaa toimintaan yksinomaan haitallisesti. Riskissä on hyvät ja huonot puolensa; epävarmuus voi luoda mahdollisuuksia toiminnan parantamiseen yhtä lailla kuin heikentää tällaisia mahdollisuuksia. Jos riskejä ja mahdollisuuksia katsotaan saman päätöksenteon kolikon kahtena eri puolena, riskienhallinta voidaan ymmärtää prosessiksi, jossa i) arvioidaan yhtä aikaa sekä ”negatiivinen riski” että ”positiivinen riski” (ts. mahdollisuudet) ja ii) riskien käsittelyssä päätetään, miten pienentää negatiivinen riski hyväksyttävälle tasolle ja miten hyödyntää positiivinen riski – eli tarttua mahdollisuuksiin – niin, että tavoitteet voidaan saavuttaa parhaalla mahdollisella tavalla. Molempien puolten integrointi ainutlaatuiseen jatkuvaan, kokonaisvaltaiseen ja systemaattiseen kehykseen voi lisätä organisaatioiden ketteryyttä ja kykyä vastata tilanteisiin, mikä puolestaan edistää niiden kilpailukykyä ja helpottaa innovaatiotoimintaa.

Kyseessä on varsin uusi lähestymistapa riskienhallintaan[47] ja jatkotyöskentely olisi tarpeen myös sen mahdollisten hyötyjen ja yleistymisen esteiden selvittämiseksi erityisesti digitaaliseen turvallisuuteen kohdistuvien riskien osalta. Näin ollen suosituksessa käsitellään riskien haitallisia vaikutuksia, kuten riskitekijöiden kuvailussa käytetyistä termeistä (esim. uhkat, haavoittuvuudet ja poikkeamat) sekä turvallisuuteen liittyvästä ja suojelun maailmasta peräisin olevasta terminologiasta (esim. saatavuus, eheys, luottamuksellisuus) ilmenee. Innovaatiotoimintaperiaatteessa kuitenkin korostetaan, että digitaaliseen turvallisuuteen kohdistuvien riskien hallinta voidaan nähdä myös mahdollisuuksien hyödyntämisen ja innovaatioiden edistämisen ajurina.

8. Varautuminen ja jatkuvuus

Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta perustuu sen tosiasian tunnustamiseen, että on mahdotonta tarjota ehdottoman "varmaa ja turvallista" digitaalista ympäristöä, jossa ei koskaan esiintyisi poikkeamia. Poikkeamia voi esiintyä ja niillä voi olla vaikutuksia taloudelliseen ja yhteiskunnalliseen toimintaan tehokkaista turvatoimenpiteistä huolimatta. Näin ollen digitaaliseen turvallisuuteen kohdistuvien riskien hallinta ei rajoitu turvatoimenpiteiden käyttöönottoon ja innovaatiotoimintaan, vaan sen tulisi käsittää myös varautumis- ja jatkuvuussuunnittelu. Suunnitelmissa määritellään etukäteen mekanismit, joilla riskejä pienennetään poikkeamatilanteissa pienentämällä riskien haittavaikutuksia taloudelliseen ja yhteiskunnalliseen toimintaan sekä mahdollistamalla toiminnan jatkuvuus ja häiriönsietokyky.

Varautumis- ja jatkuvuussuunnitelmissa tulisi huomioida se nopeus, jolla poikkeamat voivat levitä ja eskaloitua digitaalisessa ympäristössä. Eskalaation vaiheet erotellaan yleensä kyseessä olevaan taloudelliseen ja yhteiskunnalliseen toimintaan sekä kyseessä oleviin tavoitteisiin kohdistuvien seurausten vaikutusalan ja mittakaavan mukaan. Tilanteeseen voidaan soveltaa eri asteikkoja kuten "hälytys" (ei vaikutusta), "poikkeama" (vain IT-vaikutuksia), "hätätilanne" (rajoitetusti taloudellisia ja yhteiskunnallisia vaikutuksia" ja "kriisi" (organisaation olemassaoloa uhkaava vaikutus). Muitakin termejä ja asteikkoja voidaan käyttää asiayhteydestä riippuen. Yleisissä linjauksissa voidaan esimerkiksi huomioida vaikutukset yksittäiseen organisaatioon, organisaation toimintasektoriin, kansantalouteen kokonaisuudessaan, ja kansainvälisesti. Vastuun tulisi jakautua eri tavalla kussakin eskalaation vaiheessa, jotta voidaan varmistaa riskin asianmukainen hallinta poikkeaman kestäessä. Tässä yhteistyö on jälleen avainasemassa erityisesti sen varmistamiseksi, että päättäjät ymmärtävät niin poikkeaman taloudelliset ja yhteiskunnalliset vaikutukset kuin myös siihen liittyvät tekniset näkökohdat.

Varautumissuunnitelman tulisi kattaa digitaalisen turvallisuuden poikkeamien estäminen ja havaitseminen sekä niihin vastaaminen ja niistä toipuminen. Siinä tulisi myös määrätä niin yksittäisten toimijoiden kuin yhteistyössäkin tehtävistä toimista kuten asianmukainen tiedonvaihto toisten sidosryhmien kanssa myös julkisen ja yksityisen sektorin välillä sekä rajojen yli. Riskin dynaamisen luonteen huomioimiseksi suunnitelmaa tulisi testata, arvioida ja tarkastella jatkuvan kehittämisen mallilla. Tietoturvaloukkauksiin reagoivat ja niitä tutkivat yksiköt (Computer Security Incident Response Team, CSIRT), näistä käytetään myös nimeä Computer Emergency Response Team, CERT), voivat antaa merkittävän panoksen auttaakseen sidosryhmiä vastaamaan tiettyihin digitaalisen turvallisuuden poikkeamiin. Kansainvälisesti vertailukelpoiset CSIRT/CERT-yksiköiden toimintaa kuvaavat tilastolliset indikaattorit voisivat antaa päättäjille paremman käsityksen yleisestä riskitasosta.

Asianmukaisia ilmoitusmenettelyjä tulisi myös harkita osana suunnitelman toimeenpanoa. Ilmoitusmenettely voi joissakin tapauksissa perustua vapaaehtoisuuteen ja toisissa tapauksissa olla lakisääteinen.

Mahdollisia aihepiirejä jatkotyöskentelyä varten

Mahdollisiin aihepiireihin jatkotyöskentelyä varten kuuluvat mm.:

- Digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan hallinnointi organisaatioissa: siirtymä teknisestä asiasta johdon prioriteetiksi.
- Riskienhallinta yksityisyydensuojan edistämiseksi: digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan panos OECD:n yksityisyydensuojaa koskevien ohjeiden parempaan täytäntöönpanoon. Digitaaliseen turvallisuuteen ja yksityisyydensuojaan kohdistuvien riskien hallinnan yhteisten piirteiden, eroavaisuuksien ja synergioiden samoin kuin yhteisen kehyksen mahdollisuuden selvittäminen.
- Innovaatiotoiminnan ja digitaaliseen turvallisuuteen kohdistuvien riskien hallinnan välinen suhde sekä "riski ja mahdollisuus" -lähestymistavan soveltaminen digitaaliseen turvallisuuteen (ts. riskienhallinta arvon säilyttämiseksi ja luomiseksi) sekä sen käytettävyys, edut ja haasteet.
- Digitaaliseen turvallisuuteen kohdistuvien riskien varalta vakuuttamisen mahdollisuudet ja haasteet.
- Periaatteiden tulkinta pk-yritysten ja yksiköiden osalta.
- Digitaaliseen turvallisuuteen kohdistuvien riskien hallintaan liittyvä valvonta.
- Suosituksen osaan 2 sisältyvä yleisten linjausten ohjeistus.
- Kansainvälinen yhteistyö ja kehittyvät taloudet.
- Digitaaliseen turvallisuuteen kohdistuvia riskejä koskevan tietopohjan parantaminen.

Lähdeluettelo

ACMA (Australian Communications and Media Authority) (2011), An overview of international cyber-security awareness raising and educational initiatives, www.acma.gov.au/theACMA/an-overview-of-international-cyber-security-awareness-raising-and-educational-initiatives.

Angwin, J. (2015), The World's Email Encryption Software Relies on One Guy, Who is Going Broke, www.propublica.org/article/the-worlds-email-encryptionsoftware-relies-on-one-guy-who-is-going-broke.

App Promo (2013), "App Promo White Paper. Slow and steady win the race. App Developers That Stick it Out Come Out on Top", App Promo Developer Survey, heinäkuu 2013, http://app-promo.com/wp-content/uploads/2013/06/SlowSteady-AppPromo-WhitePaper2013.pdf (luettu 25.8.2015).

App Promo (2012), "Wake Up Call – If You Spend It, They Will Come", http://app-promo.com/wake-up-call-infographic/ (luettu 25.8.2015).

Ashford W. (2013), Targeted cyber espionage on the increase, McAfee warns, www.computerweekly.com/news/2240185167/Targeted-cyber-espionage-on-the-increase-McAfee-warns. Aven, T. (2012), "The risk concept - historical and recent development trends", teoksessa Reliability Engineering & System Safety, Volume 99, maaliskuu 2012, ss. 33–44, http://dx.doi.org/10.1016/j.ress.2011.11.006.

CBC News (2012), "Nortel collapse linked to Chinese hackers", www.cbc.ca/news/business/nortel-collapse-linked-to-chinese-hackers-1.1260591 (luettu 25.8.2015).

Choe, S. (2014), "Theft of Data Fuels Worries in South Korea", New York Times, www.nytimes.com/2014/01/21/business/international/theft-of-data-fuels-worries-in-south-korea.html (luettu 25.8.2015).

CIGI (Centre for International Governance Innovation) (2014), CIGI-Ipsos Global Survey on Internet Security and Trust, https://www.cigionline.org/internet-survey (luettu 25.8.2015).

CNIL (Commission Nationale de l'Informatique et des Libertés) (2012), Methodology for privacy risk management, www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf.

Council of Europe (2001), Convention on Cybercrime [Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus], http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

Dark Reading (2012), "4 Long-Term Hacks That Rocked 2012", www.darkreading.com/application-security/database-security/4-long-term-hacks-that-rocked-2012/d/d-id/1138643 (luettu 25.8.2015).

ENISA (European Union Agency for Network and Information Security) [Euroopan unionin verkko- ja tietoturvavirasto] (2013), National Cyber Security Strategies in the World, www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world (luettu 25.8.2015).

ENISA (n.d.), "Existing Taxonomies", www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/incident-taxonomy/existing-taxonomies
(luettu 25.8.2015).

Europol (2013), Notorious Botnet Infecting 2 Million Computers Disrupted,
www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted-0 (luettu 25.8.2015).

Fechner, B. (2014), Les entreprises françaises face au défi de l'espionnage industriel, http://lexpansion.lexpress.fr/actualite-economique/les-entreprises-francaises-peuvent-elles-relever-le-defi-de-l-espionnage-industriel_1633978.html (luettu 25.8.2015).

Gaudiosi, J. (2014), "Why Sony didn't learn from its 2011 hack", http://fortune.com/2014/12/24/why-sony-didnt-learn-from-its-2011-hack/ (luettu 25.8.2015).

ISOC (Internet Society) (2015), Collaborative Security: An approach to tackling Internet Security issues, www.internetsociety.org/collaborativesecurity.

Jackson, W. (2014), "Cyber Espionage Incidents Triple: Verizon Report",
www.informationweek.com/government/cybersecurity/cyber-espionage-incidents-triple-verizon-report/d/d-id/1204612 (luettu 25.8.2015).

Kim, Y. (2014), "Top executives resign over massive data leak", www.koreaherald.com/view.php?ud=20140120001002 (luettu 25.8.2015).

Kitten, T. (2014), "Chase's Cybersecurity Budget to Double", www.bankinfosecurity.com/chases-cybersecurity-budget-to-double-a-7427 (luettu 25.8.2015).

Lee, R., M. Assante ja T. Conway (2014), German Steel Mill Cyber Attack, https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility. pdf.

Leyden, J. (2013), "Biggest DDoS attack in history hammers Spamhaus", www.theregister.co.uk/2013/03/27/spamhaus_ddos_megaflood (luettu 25.8.2015).

Molla, R. (2012), "Most app developers make less than $500 a month", https://gigaom.com/2012/10/04/most-app-developers-make-less-than-500-a-month-chart/ (luettu 25.8.2015).

NACD (National Association of Corporate Directors) (2014), NACD Reports Directors Dissatisfied with Cyber and IT Risk Information, www.nacdonline.org/AboutUs/PressRelease.cfm?ItemNumber=12530 (luettu 25.8.2015).

NIST (2014), Framework for Improving Critical Infrastructure Cybersecurity, www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

NIST (National Institute of Standards and Technology) (2012), Guide for conducting risk assessment. Special publication 800-30, revision 1, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

O'Connor, C. (2014), "Target CEO Gregg Steinhafel Resigns in Data Breach Fallout", www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout (luettu 25.8.2015).

OECD (Organisation for Economic Co-operation and Development) (2014), Recommendation on Digital Government Strategies, www.oecd.org/gov/public-innovation/recommendation-on-digital-government -strategies.htm.

OECD (2013a), ICTs and the Health Sector: Towards Smarter Health and Wellness Models, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264202863-en.

OECD (2013b), Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=114&InstrumentPID=312&Lang=en&Book=False.

OECD (2012a), Connected Minds: Technology and Today's Learners, Educational Research and Innovation, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264111011-en.

OECD (2012b), "ICT Applications for the Smart Grid: Opportunities and Policy Implications", OECD Digital Economy Papers, No. 190, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k9h2q8v9bln-en.

OECD (2012c), "Improving the Evidence Base for Information Security and Privacy Policies: Understanding the Opportunities and Challenges related to Measuring Information Security, Privacy and the Protection of Children Online", OECD Digital Economy Papers, No. 214, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k4dq3rkb19n-en.

OECD (2012d), "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy", OECD Digital Economy Papers, No. 211, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k8zq92vdgtl-en.

OECD (2011), Recommendation of the Council on Principles for Internet Policy Making, http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=270&InstrumentPID=275.

OECD (2008), Recommendation of the Council on the Protection of Critical Information Infrastructures, http://webnet.oecd.org/oecdacts/Instruments/ShowInstrumentView.aspx?InstrumentID=121&InstrumentPID=117.

OECD (2002), Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security, www.oecd.org/internet/ieconomy/15582260.pdf.

OECD ja Eurostat (2005), Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data, 3rd Edition, The Measurement of Scientific and Technological Activities, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264013100-en.

OSCE (Organisation for Security and Cooperation in Europe) [ETYJ, Euroopan turvallisuus- ja yhteistyöjärjestö], (2013), päätös nro 1106 "Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies", www.osce.org/pc/109168.

Peters, S. (2014), "Pharmaceuticals, Not Energy, May Have Been True Target of Dragonfly, Energetic Bear", www.darkreading.com/pharmaceuticals-not-energy-may-have-been-true-target-of-dragonfly-energetic-bear/d/d-id/1316869 (luettu 25.8.2015).

Piper, A. (2014), "Risk-informed innovation. Harnessing risk management in the service of innovation", www.economistinsights.com/technology-innovation/analysis/risk-informed-innovation (luettu 25.8.2015).

Prince, B. (2014), "Incident Response Plans Lacking in Many Organizations: Survey", www.securityweek.com/incident-response-plans-lacking-many-organizations-survey (luettu 25.8.2015).

Rawlinson, K. (2015), "Charlie Hebdo: 'Islamist cyber attacks' hit France", www.bbc.com/news/technology-30850702 (luettu 25.8.2015).

SecurEnvoy (2012), "The RSA Security breach – 12 months down the technology turnpike", www.securenvoy.com/blog/2012/04/27/the-rsa-security-breach-12-months-down-the-technology-turnpike/ (luettu 25.8.2015).

United Nations (2013) [Yhdistyneet kansakunnat, YK], Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

United Nations (2003), Creation of a global culture of cybersecurity, Resolution adopted by the General Assembly A/RES/57/239, www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/57/239.

United Nations (1966a), International Covenant on Civil and Political Rights, www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx.

United Nations (1966b), International Covenant on Economic, Social and Cultural Rights, www.ohchr. org/EN/ProfessionalInterest/Pages/CESCR.aspx.

United Nations (1948), Universal Declaration of Human Rights, www.un.org/en/documents/udhr/.

Westby, J. (2012), Governance of Enterprise Security: CyLab 2012 Report. How Boards & Senior Executives Are Managing Cyber Risks, http://globalcyberrisk.com/wp-content/uploads/2012/08/CMU-GOVERNANCE-RPT-2012-FINAL1.pdf.

Yadron, D. (2014), "Internet Security Relies on Very Few", www.wsj.com/news/articles/SB20001424052702303873604579495362672447986 (luettu 25.8.2015).

Viitteet

1. Kuten esimerkiksi energia, ks. OECD, 2012b, liikenne, teollisuus jne.

2. Ks. OECD, 2013a.

3. Ks. OECD, 2012a.

4. Ks. www.oecd.org/about/whodoeswhat.

5. Ks. www.oecd.org/sti/ieconomy.

6. Ks. www.oecd.org/legal/legal-instruments.htm.

7. Näitä edustavat OECD:n liike-elämän ja teollisuuden neuvoa-antava komitea (Business and Industry Advisory Committee BIAC), kansalais- ja tietoyhteiskuntaa käsittelevä toimikunta (Civil Society Information Society Advisory Council CSISAC) ja Internetin tekninen neuvoa-antava komitea (Internet Technical Advisory Committee ITAC).

8. Tämän suosituksen edeltäjään (vuoden 2002 turvallisuutta koskevat ohjeet) viitattiin ISO 27001:2002 -standardissa ja se innoitti Yhdistyneiden Kansakuntien päätöslauselman 57/239 (United Nations, 2003).

9. Council of Europe, 2001. Ks. myös Euroopan neuvoston tietoverkkorikollisuusohjelman toimisto (C-PROC) osoitteessa www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/default_en.asp.

10. Ks. www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

11. Ks. esim. United Nations, 2013.

12. Ks. OSCE, 2013.

13. Erityisesti tietoliikennettä ja tietoja käsittelevän työryhmänsä kautta (Telecommunications and Information Working Group, APEC TEL)

14. Esimerkiksi kunnallinen, alueellinen, maakunnallinen, liittovaltiotasoinen jne. Ks. tarkennukset kohdassa “Sidosryhmät ja niiden roolit”.

15. Ks. lisätietoja rooleista, toimintakyvystä ja kontekstista periaatteiden soveltamista koskevasta liiteasiakirjan osiosta.

16. CNIL, 2012, s. 13.

17. Ashford, 2013; Feshner, 2014; ja Jackson, 2014.

18. Ks. esim. Dark Reading, 2012, jossa annetaan esimerkkejä pitkäkestoisista Yhdysvaltain kauppakamariin, Norteliin, Coca-Colaan ja Japanin valtiovarainministeriöön kohdistuneista hyökkäyksistä. Nortelin konkurssin kerrotaan liittyneen digitaaliseen vakoiluun ja erityisesti kymmenen vuoden ajan vaikuttaneeseen vaivihkaiseen tunkeutumiseen yrityksen tietojärjestelmään. Ks. CBS News, 2012.

19. Ks. esim. Europol, 2013.

20. Ks. OECD, 2012d ja ENISA, 2013.

21. Vuonna 2012 tehdyssä kyselytutkimuksessa oli 108 vastaajaa Forbes Global 2000 -listalla olevista yrityksistä. Heistä 57 % ei analysoinut kybervakuutussuojan riittävyyttä eikä ryhtynyt olennaisiin kyberriskien hallintaan liittyviin toimiin, jotka auttaisivat hallitsemaan luottamuksellisen sekä teollis- ja tekijänoikeuden alaisten tietojen anastamiseen ja tietoturvaloukkauksiin liittyviä maineeseen kohdistuvia ja taloudellisia riskejä. Westby, 2012. Ks. myös NACD, 2014 ja Prince, 2014.

22. CIGI, 2014: Käyttäjistä 79 % on huolissaan pankkitilinsä hakkeroinnista, 77 % on huolissaan verkkotiliensä hakkeroinnista ja henkilötietojensa anastamisesta ja 72 % on huolissaan ulkomaisen valtion tai terroristijärjestön maansa instituutioihin kohdistamasta kyberhyökkäyksestä.

23. Niin valtiolliset kuin valtiosta riippumattomatkin kansalliset, alueelliset ja kansainväliset elimet ovat kehittäneet useita riskiperusteisia standardeja ja menetelmiä, joiden lähestymistapa on joko yleinen tai sektorikohtainen (esim. taloussektori, julkinen hallinto jne.). Euroopan verkko- ja tietoturvavirasto ENISA on esimerkiksi listannut 17 tällaista osoitteessa http://rm-inv.enisa.europa.eu/methods, ja niitä on myös muita, kuten esim. riskienarvioinnin opas US NIST 800-30 Rev. 1 Guide for conducting risk assessments (NIST, 2012) ja tuoreempana kyberturvallisuuskehys Cybersecurity framework (NIST, 2014). Standardit heijastavat usein eri näkökulmia, niillä on eri kohderyhmät ja niissä käytetään eri termejä ja määritelmiä, eivätkä ne silti ole välttämättä ristiriidassa tämän suosituksen kanssa.

24. Tässä kohtaa saattaa tapahtua myös risteämää, kun immateriaalioikeuksien loukkaus on seurausta turvallisuuspoikkeamasta (esim. organisaation tietojärjestelmään tunkeutuminen luottamuksellisten teollisuus- tai liikesalaisuuksien hankkimiseksi, tai laittoman sisällön (esim. vihapuheen) levittäminen verkkosivuston turmelemisen kautta.

25. Kun sanotaan: "Jos ylität kadun, sinulla on riski tulla yliajetuksi", riskillä viitataan tapahtumaan tai poikkeamaan; kun sanotaan: "autot muodostavat riskin tietä ylittäville jalankulkijoille", viitataan uhkaan tai vaaraan; ja kun sanotaan: "sinulla on riski kuolla, jos et ole tarkkana, kun ylität tietä", riski viittaa tapahtuman seuraukseen.

26. "ICT-ammattilaiset" saattaa käsittää myös yksilöitä, joille ICT-ala ei ole pääasiallinen ammatti, kuten on asianlaita esim. monien sovelluskehittäjien osalta.

27. Joskus asian tekninen monimutkaisuus saattaa tarkoittaa, että vaikka olisi mahdollista pienentää digitaaliseen turvallisuuteen kohdistuvia riskejä, tätä ei tehdä tavalla, joka antaisi yksilölle vaikutusmahdollisuuksia sen hallitsemiseen. Verkkopalvelut ja muut etäältä tuotettavat palvelut esimerkiksi toimeenpanevat turvallisuusratkaisunsa keskitetysti.

28. SecurEnvoy, 2012.

29. Kauppapaikka tulisi ymmärtää laajasti paikkana, missä tarjonta ja kysyntä kohtaavat. Se käsittää myös ilmaiset ja avoimeen lähdekoodiin perustuvat ohjelmistot.

30. Ks. Angwin, 2015, Yadron, 2014.

31. "Vastaajista 68 % ilmoitti, että heidän sovelluksensa oli tuottanut alle 1 000 $ julkaisustaan lähtien, kun taas vastaajista 29 % ei ollut vielä saanut mitään tuloja sovelluksestaan" (App Promo, 2013). "Useimmat sovelluskehittäjät ansaitsevat alle 500 $ kuukaudessa (Molla, 2012). Ks. myös App Promo, 2012.

32. Vrt. VI: [Neuvosto] "Toteaa, että periaatteet täydentävät toisiaan ja että niitä tulisi tarkastella kokonaisuutena…".

33. Saastunutta tietokonetta tai muuta laitetta voidaan esimerkiksi käyttää hyökkäyksessä toisen omaisuutta vastaan (esim. hajautettuun palvelunestohyökkäykseen) ja henkilötietojen julki tuleminen tietoturvahyökkäyksen seurauksena voi vaikuttaa ei vain tapahtuman kohteena olevan organisaation taloudellisiin intresseihin vaan myös niihin henkilöihin, joiden tiedot on anastettu.

34. Hankkeita koskeva kansainvälinen vertailuanalyysi, ks. ACMA, 2011.

35. OECD, 2012d.

36. Suosituksen johdannossa esiintyvä “Tiedostaa” -kohta (10. kohta) korostaa digitaalisen ympäristön suojelemisen vastuun jakautuvan sidosryhmien kesken. Lisätietoja ”kollektiivisen vastuun” käsitteestä, ks. ISOC, 2015.

37. United Nations, 1948, 1966a ja 1966b.

38. On aiheellista korostaa, että suosituksessa käytetään sanaa “turvatoimenpiteet” kattamaan turvatoimenpiteet digitaaliseen turvallisuuteen kohdistuvien riskien hallintaa varten. Muunlaiset turvatoimenpiteet eivät sisälly suosituksen soveltamisalaan.

39. Vuoden 2011 Internet-politiikan suunnittelun periaatteita koskevaan neuvoston suositukseen (OECD 2011) sisältyviä periaatteita avaavassa tiedonannossa todetaan, että: ”[…] On selvää, että Internetin avoimuutta ja saavutettavuutta on tuettava ilmaisunvapauden nimissä sekä edistämään laillista tiedon- ja tietämyksen jakamista sekä mielipiteiden vaihtoa käyttäjien kesken. Tämä käsittää myös tutkimus- ja kehitystoiminnan ja on tuottanut talouteen laajaa innovaatiotoimintaa […]”. Vuoden 2011 suosituksessa itsessään todetaan: ”Suosittelee, että Internet-talouden politiikoita kehittäessään tai tarkistaessaan jäsenmaat yhteistyössä kaikkien sidosryhmien kanssa ottavat huomioon seuraavat korkean tason periaatteet [:] […] Varmistavat avoimuuden, menettelyjen oikeudenmukaisuuden sekä vastuullisuuden”. Tältä osin tiedonannossa todetaan myös, että ”Internet-ympäristöön kohdistuvan yleisen luottamuksen rakentamiseksi olisi kannustettava poliittisiin päätöksentekoprosesseihin sekä käytännön periaatteisiin, jotka varmistavat avoimuuden, menettelyjen oikeudenmukaisuuden ja vastuullisuuden. Avoimuudella varmistetaan, että Internetin käyttäjille on saatavilla oikea-aikaista tietoa, johon perustaa toimensa ja joka on heidän oikeuksiensa ja intressiensä mukaista. Menettelyjen oikeudenmukaisuus tuottaa ennustettavissa olevia päätöksentekoprosesseja, jotka koskevat oikeuksienmäärittelemistä, niihin vetoamista ja niiden puolustamista. Vastuullisuuteen päästään noudattamalla toimintatapoja, jotka saattavat osapuolet tarvittaessa vastuuseen Internetissä tapahtuvista toimistaan.”

40. OECD 2013b, osa 3, kohta 15 a).

41. OECD:n vuoden 2002 turvallisuutta koskevissa ohjeissa korostettiin yhteistyön olevan hyödyllinen käsite. Siitä tehtiin periaate tässä suosituksessa, koska haluttiin korostaa sen kasvanutta merkitystä ja olennaista roolia muiden periaatteiden tukijana.

42. Mielenkiintoisena esimerkkinä toimii CONCERT, korealainen CERT-yksiköiden konsortio, joka luotiin vuonna 1996 yhteistä etua koskeviin turvallisuusasioihin liittyvien tietojen vaihtamiseen ja jakamiseen sekä osapuolten yhteistyöelimeksi. Konsortio koostuu yli 300 yritysten tietoturvayksiköstä, laitoksesta ja hallituksesta Koreassa. Ks. www.concert.or.kr.

43. Kuten esim. Yhdistyneiden Kuningaskuntien Cyber-security Information Sharing Partnership (CiSP), kyberturvallisuuteen liittyvää tietoa jakava yhteisö. Ks. www.cert.gov.uk/cisp.

44. Julkisten ja yksityisen sektorin kumppanuudesta puhuttaessa yksityinen sektori käsittää julkiseen sektoriin kuulumattomat sidosryhmät, joita ovat mm. yritykset, voittoa tavoittelemattomat yhteisöt, kansalaisyhteiskunta, tiedeyhteisö, tekninen yhteisö jne.

45. Riskien "käsittelystä" puhutaan joskus myös riskien "vähentämisenä". Ks. termien ja määritelmien osalta Laatikko 3. Esimerkkejä muista riskien käsittelyyn liittyvistä termeistä ovat mm. riskien hyväksyminen, ottaminen tai kantaminen, niiden vähentäminen tai minimointi, niiden siirtäminen tai uudelleenallokointi ja niiden välttäminen.

46. OECD/Eurostat, 2005.

47. Piper, 2014.

Taloudellisen yhteistyön ja kehityksen järjestö OECD

OECD on ainutlaatuinen foorumi, jossa hallitukset käsittelevät yhdessä globalisaatioon liittyviä taloudellisia, yhteiskunnallisia ja ekologisia haasteita. OECD myös johtaa toimia, joiden tarkoituksena on auttaa hallituksia ymmärtämään ja kohtaamaan uusia kehityssuuntauksia ja huolenaiheita kuten hyvään hallintotapaan, tietotalouteen ja väestön ikääntymiseen liittyviä haasteita. OECD tarjoaa ympäristön, jossa hallitukset voivat vertailla kokemuksiaan eri alojen politiikasta, etsiä vastauksia yhteisiin ongelmiin, jakaa hyviä käytäntöjä ja sovittaa yhteen kansallisia ja kansainvälisiä politiikkoja.

OECD:n jäsenmaat ovat: Alankomaat, Australia, Belgia, Chile, Espanja, Irlanti, Islanti, Israel, Italia, Itävalta, Japani, Kanada, Korea, Kreikka, Luxemburg, Meksiko, Norja, Portugali, Puola, Ranska, Ruotsi, Saksa, Slovakia, Slovenia, Suomi, Sveitsi, Tanska, Tšekki, Turkki, Unkari, Uusi-Seelanti, Viro, Yhdistyneet Kuningaskunnat ja Yhdysvallat. Euroopan unioni osallistuu OECD:n työskentelyyn.

OECD Publishing vastaa järjestön kokoamien tilastojen, sen laatimien talous-, yhteiskunta- ja ympäristötutkimusten sekä sen jäsenten hyväksymien sopimusten, ohjeiden ja standardien levityksestä.

Pysy ajan tasalla ja tilaa innovaatiotoimintaa, tiedettä, tekniikkaa ja teollisuutta käsittelevä uutiskirjeemme (englanniksi): OECD News on Innovation, Science, Technology and Industry: http://oe.cd/stinews

@OECDInnovation

http://oe.cd/dsrm

Meidät tavoittaa osoitteesta: STI.contact@oecd.org

OECD
BETTER POLICIES FOR BETTER LIVES

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin 0295 160 01
Telefaksi 09 160 33123
www.vm.fi

ISSN 1459-3394 (nid.)
ISBN 978-952-251-789-0 (nid.)
ISSN 1797-9714 (pdf)
ISBN 978-952-251-790-6 (pdf)

Syyskuu 2016