Verkkokelmit eivät keinoja kaihda

Suomen tie kohti parempaa tietoverkkoturvallisuutta

Theo Herold

AGENDA

Ajatushautomo Agenda 2024
ISBN 978-952-7273-50-0 (pdf)
Suomenkielinen käännös: Anu Huusko / TranslatiOm
Graafinen suunnittelu ja taitto: Linnéa Sjöholm
Kuvituskuvat: Sebastian Dahlström

Verkkokelmit eivät keinoja kaihda

Suomen tie kohti parempaa tietoverkkoturvallisuutta

Ajatushautomo Agenda
Theo Herold
2024

Sisällysluettelo

Kirjoittajasta

Kuva: Tom Samuelsson

Theo Herold on väitellyt kauppatieteiden tohtoriksi Hankenista ja Helsingin kauppakorkeakoulusta. Hän on apulaistutkija Tukholman Ratio-tutkimuslaitoksessa ja Liberal Debatt -lehden tutkimusosaston päätoimittaja. Aiemmin hän on työskennellyt Tukholman kauppakamarissa muun muassa tietoverkkoturvallisuuteen ja -valmiuteen liittyvien kysymysten parissa.

Esipuhe

Nettihuijauksen kohteeksi joutuminen on normaalia – et ole yksin

Kuva: Anders Wikström

Minulta on huijattu rahaa verkossa kahdesti. Summa ei ollut suuri, mutta tunsin itseni jälkeenpäin äärimmäisen tyhmäksi, nöyryytetyksi ja huijatuksi. Ensimmäisen kerran jälkeen lupasin itselleni, ettei niin enää koskaan tapahtuisi. Toisen kerran jälkeen tajusin, kuinka se tapahtui. Kolmatta kertaa sitä ei ole tapahtunut.

Näemme otsikoissa säännöllisesti sanoja kuten tietovarkaus, salasanojen louhinta ja verkkopetos, mutta myös GPS-häirintä, palvelunestohyökkäykset ja hybridisodankäynti. Yksittäisten toimijoiden, rikollisverkostojen ja hallitusten tekemä tietoverkkorikollisuus – joskus kaikkien kolmen yhdistelmänä – on valitettavasti tullut jäädäkseen

Kun elämämme on siirtynyt verkkoon, rikollisuus on seurannut sitä. Sanotaan, että tilaisuus tekee varkaan, ja internet on täynnä sekä tilaisuuksia että varkaita. Sanotaan myös, että pitää huolehtia omista asioistaan. Fyysisen maailman osalta tiedämme, että on tärkeää lukita ulko-ovi ja polkupyörä sekä olla jättämättä lompakkoa kahvipöydälle.

Digitaalisen viestinnän osalta tilanne on kuitenkin hankalampi. Digitaalinen maailma muuttuu jatkuvasti, koska uusia teknologioita ja mahdollisuuksia syntyy jatkuvasti. On tärkeää olla valmistautunut.

Siksi Agenda julkaisee nyt aihetta koskevan raportin. Taloustieteilijä Theo Herold (Swedish School of Economics) kertoo, mitä tietoverkkorikollisuus on ja kuinka paljon se maksaa Suomelle (vastaus on paljon!), mitä voimme tehdä tietoverkkoturvallisuuden parantamiseksi (sekä kansakunnan että yksilön kannalta) ja mitä voisimme oppia Virosta, joka on edelläkävijä monissa digitaalisen alan asioissa.

Raportissa esitellään myös konkreettisia toimenpiteitä tietoverkkoturvallisuuden parantamiseksi sekä Huoltovarmuuskeskuksen kommentti, kuinka yksityishenkilöt ja hallitukset voivat vahvistaa tietoverkkoturvallisuutta.

Kaksivaiheinen todentaminen ja vahva varmennus eivät yksin riitä. On myös tärkeää tunnistaa yritykset päästä käsiksi tietoihin, salasanoihin tai henkilöllisyyteen suoran yhteydenoton kautta.

Helsinki, marraskuu 2024

Ted Urho
Toiminnanjohtaja
Ajatushautomo Agenda

1. Tietoverkkoihin yhdistynyt maailma

Yhteiskunta elää nykyään monin tavoin internetissä, eli tietoverkossa. Tietoverkot käsittävät viestintä-yhteydet, jotka toteutetaan sähköisillä laitteilla, kuten tietokoneilla, tableteilla ja matkapuhelimilla, mutta myös valvontakameroilla ja tallentimilla sekä muilla vastaavilla laitteilla. Yksityishenkilöt suorittavat maksuja digitaalisilla lompakoilla, viranomaiset käyttävät digitaalisia postilaatikoita ja matkustajat mobiilimatkalippuja. Koko yhteiskunnan infrastruktuuri edellyttää täydellistä tai osittaista yhteyttä tietoverkkoon aina sähkö-verkosta liikennevaloihin ja Itämeren ylittäviin liikennejärjestelmiin.

Kun ihmiset ovat yhä tiiviimmin yhteydessä internetiin, myös tietoverkkorikollisuus lisääntyy. Tieto-verkkorikollisuus tarkoittaa laitonta toimintaa, jossa rikoksentekijä tekee rikoksia sähköisiä laitteita käyttäen ja niiden välityksellä. Rikokset voivat olla arkaluonteisten tietojen luvatonta käyttöä, kiristystä, pelon ja disinformaation levittämistä sekä keskeisten yhteiskunnallisten toimintojen häirintää. Rikoksentekijät voivat toimia yksin tai osana laajempia verkostoja, ja hallitusten osallistuminen tällaiseen toimintaan on yhä yleisempää. Verkkohyökkäykset voivat kohdistua yksilöihin, ryhmiin ja kokonaisiin yhteiskuntiin. Siksi tieto-verkkoturvallisuuden varmistaminen on tärkeää yksilötasolla aina viranomaisiin ja suurempiin instituutioihin saakka.

Laadukas viestintäinfrastruktuuri ja tietoverkkoturvallisuus ovat keskeisiä tekijöitä nykyaikaisen yhteis-kunnan toiminnalle. Suomen maantieteellinen sijainti Venäjän vieressä lisää hyvän tietoverkkoturvallisuuden tarvetta. Venäjän tietoverkkorikollisuushistoria on pitkä, ja se on suurin yksittäinen turvallisuusuhka Euroopalle. Venäläiset verkkorikollisjärjestöt, kuten Avalanche ja NoName, ovat vuosien varrella tehneet Suomessa useita suuria hyökkäyksiä yksityishenkilöitä, yrityksiä ja viranomaisia vastaan. On hyvin toden-näköistä, että nämä järjestöt toimivat usein Venäjän valtion käskystä.

Merkittävä este tietoverkkoturvallisuuden parantamiselle yhteiskunnassa on digitaalisen kehityksen nopea vauhti. Se tarkoittaa, että tietoverkkohyökkäysten luonne muuttuu ajan myötä. Lisäksi jokaista hyökkäys-tyyppiä vastaan, jota vastaan onnistumme puolustautumaan, näyttää syntyvän kymmeniä uusia.

Onko täydellinen suojautuminen edes mahdollista? Suorasanainen vastaus on ei – ei oikeastaan – mutta tämä on myös totuus, johon liittyy muutoksia.

Voimme yhteistyötä tekemällä yhteisönä minimoida vahinkojen laajuuden ja altistumisriskin. Meidän täytyisi yksilöinä pitää itsemme ajan tasalla ja kehittää ymmärrystämme erityyppisten verkkohyökkäysten toiminta-tavoista. Paikallisen ja kansallisen tason päättäjien on varmistettava, että viranomaisten ja yritysten välinen vuoropuhelu sujuu kitkattomasti. Sekä yksityisen että julkisen sektorin on huolehdittava tarvittavien viestintä-infrastruktuuri-investointien hankintamahdollisuus. Hallituksen, yritysten ja yksityishenkilöiden välisen tiedonkulun on oltava vapaata, ja sen vastuunjaon on oltava selkeää.

Suomen Nato-jäsenyyden myötä on myös tärkeää lisätä yhteistyötämme muiden Pohjoismaiden ja Euroopan kanssa. Naapurimaista Baltiassa ja ehkä erityisesti Virosta voidaan ottaa paljon mallia. Viro on maailman johtava maa sekä tietoverkkoturvallisuuden että digitalisaation alalla, mikä johtuu varhaisista koulutus-mahdollisuuksista, vahvoista julkisen ja yksityisen sektorin kumppanuuksista ja (valitettavasti) myös maan laajasta tietoverkkohyökkäyskokemuksesta.

Ukrainaa vastaan käyty häikäilemätön hyökkäyssota osoittaa myös, miten valtio, tässä tapauksessa Venäjä, voi osallistua tietoverkkorikollisuuteen. Hyökkäystä edeltävänä päivänä, 23. helmikuuta, tehtiin hyökkäyksiä pankkeja ja viranomaisia vastaan palvelunestohyökkäysten ja haittaohjelmien levittämisen muodossa. Vahvat viitteet osoittavat, että koodia kehitettiin jo vuonna 2021, mikä saattaa tarkoittaa, että hyökkäystä suunniteltiin vuosia etukäteen.[1] Ennen tätä hyökkäystä Venäjä teki useita samankaltaisia hyökkäyksiä hallituksen verkkosivuja, muun muassa Ukrainan hallituksen virastoa ja ulkoasiainministeriötä vastaan. Jotkut saattavat muistaa Ukrainan hallituksen verkkosivustoilla levinneen tekstin ”pelkää ja valmistaudu pahimpaan”.[2] Sodan aikana Venäjä on jatkanut hybridisodankäyntiään.

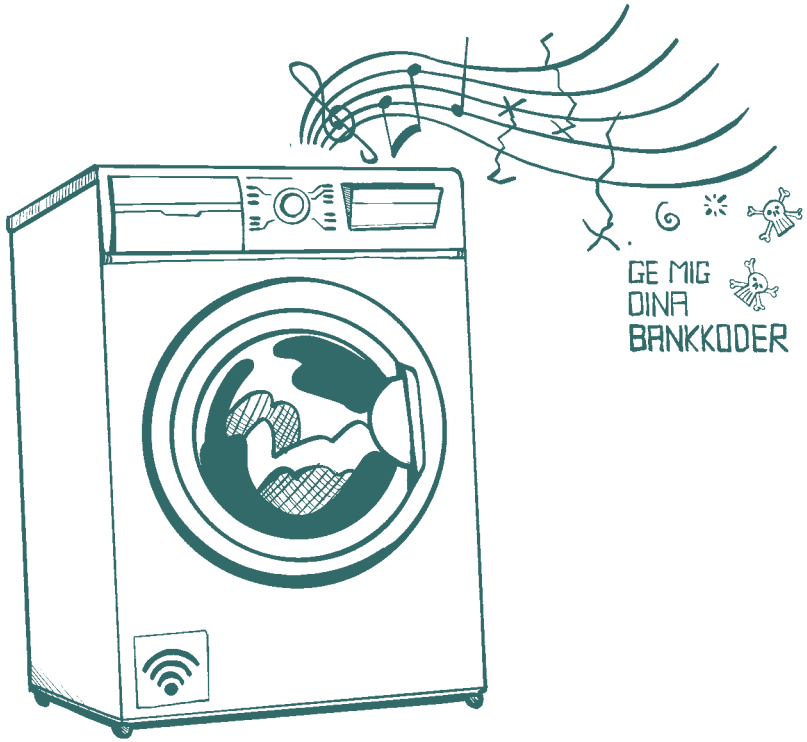
Venäjä on tehnyt Suomessa vuosien varrella useita niin sanottuja palvelunestohyökkäyksiä (DDoS-hyökkäyksiä), jotka ovat kohdistuneet Verohallintoon, Traficomiin, Expressbusiin, eduskuntaan ja useisiin muihin viranomaisiin. Vuonna 2024 useat matkustajalentokoneisiin ja -lauttoihin kohdistuneet GPS-häirintä-hyökkäykset ovat häirinneet Itämeren liikennettä sekä ilmassa

1 ESET Research, ”IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine”, We Live Security, 2022.

2 Andrew Kramer/The New York Times, ”Hackers Bring Down Government Sites in Ukraine”, 2022.

että merellä, ja vaikuttaa siltä, että hyökkäysten takana on Venäjä.[3] Yksittäisten toimijoiden, rikollisverkostojen ja hallitusten tekemä tietoverkkorikollisuus – joskus kaikkien kolmen yhdistelmänä – on valitettavasti tullut jäädäkseen.

Luet raporttia, jonka tavoite on lisätä yleistä ymmärrystä tietoverkkorikollisuudesta, sen muodoista ja tavoista, joilla me suomalaisessa yhteiskunnassa voimme lisätä vastustuskykyämme sitä vastaan. Raportissa esitetään ensin lyhyt historiallinen katsaus ja tietoverkkorikollisuuden kustannusarviot (luku 2). Sen jälkeen käsitellään tietoverkkoturvallisuuden kehitystä Suomessa ja sen toimivuutta nykyään (luku 3). Sen jälkeen tarkastelemme lähemmin virolaista huippuosaamista, joka on tehnyt Virosta maailman kärkeä sekä digitalisaatiossa että tietoverkkoturvallisuudessa. Lisäksi tarkastelemme, mitä me Suomessa voimme oppia Itämeren-naapuriltamme (luku 4). Raportin lopussa esitetään konkreettisia ehdotuksia, kuinka Suomi voisi kehittää tietoverkkoturvallisuuttaan (luku 5).



3 Dann Pettersson/Hufvudstadsbladet, ”Finnair pausar flyg efter gps-störningar”, 2024.

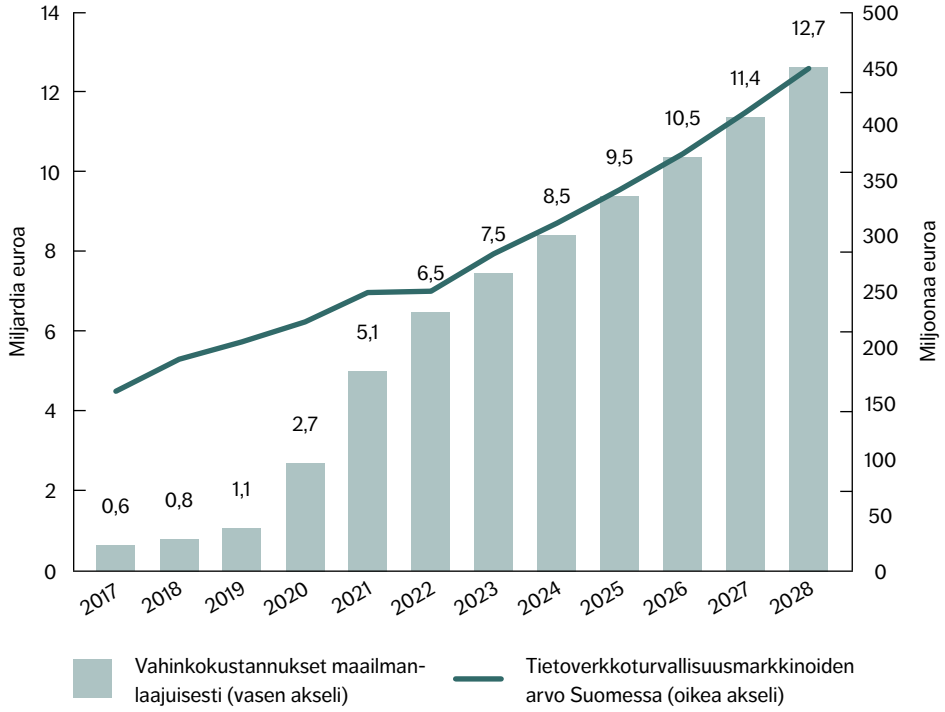
2. Tietoverkkorikollisuus – miljoonakustannukset Suomen valtiolle

Tietoverkkorikollisuus lähti kunnolla liikkeelle 1990-luvulla digitalisaation nopean kehityksen ja henkilö-kohtaisten tietokoneiden yleistymisen myötä. Jälkikäteen on vaikea arvioida rahamäärää, jonka hyökkääjät ansaitsivat tänä aikana, puhumattakaan aiheuttamiensa vahinkojen määrästä. Kuten kuvasta 1 käy ilmi, voimme kuitenkin päätellä, että maailmanlaajuisen tietoverkkorikollisuuden aiheuttamat vahingot ovat nykyään tähtitieteellisiä. Vuoteen 2028 mennessä niiden odotetaan nousevan 12,7 biljoonaan euroon (biljoona b:llä!) – kirjoitamme tämän luvun esiin järjettömyyden havainnollistamiseksi: 12 700 000 000 000 euroa. Jos tietoverkkorikollisuus olisi maa, se olisi maailman kolmanneksi suurin talous Yhdysvaltojen ja Kiinan jälkeen.[4] Vertailun vuoksi mainittakoon, että Suomen bruttokansantuote, Suomen taloudellisen toiminnan arvo, oli vuonna 2022 noin 280 miljardia euroa – eli ”vain” 280 000 000 000 euroa. Tietoverkkorikollisuuden aiheuttamat vahingot ylittävät tiettynä vuonna kaikkien maailman luonnonkatastrofien taloudelliset kustannukset yhteensä tai koko maailmanlaajuisen huumekaupan suorat kustannukset.[5] Tämän seurauksena myös erilaiset tietoverkkoturvallisuusratkaisumarkkinat ovat kasvaneet nopeasti. Kuten kuvasta 1 käy ilmi, Suomen markkinoiden liikevaihdon odotetaan kasvavan 180 prosenttia 450 miljoonaan euroon vuosina 2017–2028.

4 Steve Morgan/Cybercrime Magazine, ”Cybercrime to cost the world $10.5 trillion annually by 2025”, 2020.

5 Mai Periman7/Cisco, ”How to prevent the bank robbery no one can see”, 2017.

KUVA 1 Maailmanlaajuiset tietoverkkorikollisuuden aiheuttamien vahinkojen kustannukset ja tietoverkkoturvamarkkinoiden tulot Suomessa 2017–2028



Huom: Huomaa, että vasemmanpuoleinen akseli esittää vahinkokustannukset triljoonina euroina ja oikeanpuoleinen akseli osoittaa tietoverkkoturvallisuuden markkina-arvon Suomessa miljoonina euroina. Lähde: Statista Technology Market Insights

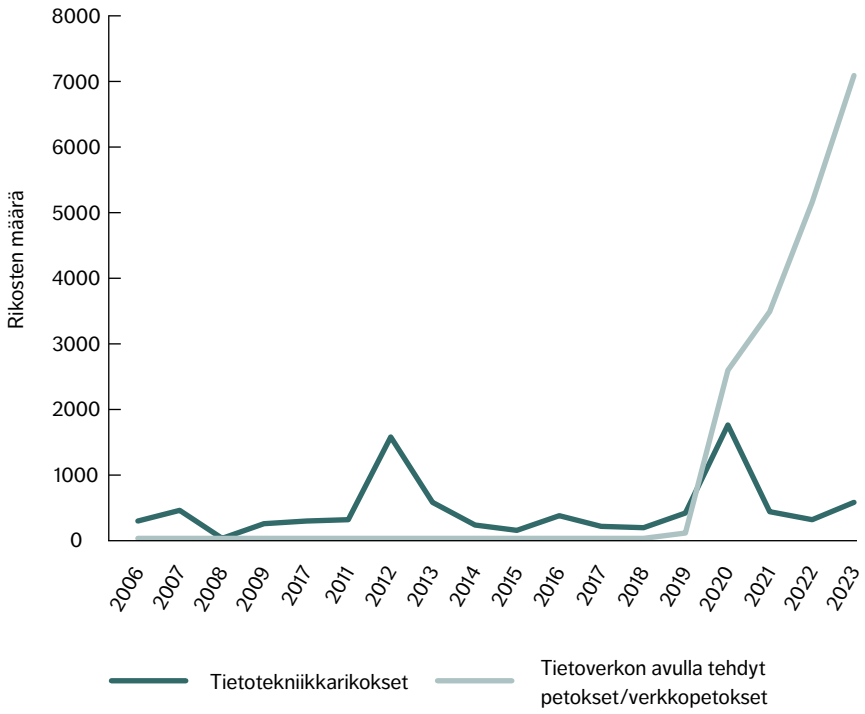
Yksityishenkilöihin kohdistuvat tietovarkaudet ja petokset ovat yleisimpiä, ja ne tehdään usein salasanojen louhinnan avulla. Tämä ei ole yllättävää, kun otetaan huomioon, miten aktiivisesti Suomessa käytetään internetiä – vuonna 2023 94 prosenttia ilmoitti käyttäneensä internetiä vähintään kerran viimeisten kolmen kuukauden aikana, ja 73 prosenttia käytti internetiä useita kertoja päivässä.[6] Valitettavasti internetin yleinen käyttö heijastuu myös internetpetosten määrään, sillä poliisin tietoon tuli yli 7 000 tällaista rikosta vuonna 2023 (ks. kuva 2).[7] Verkkopetokset ovat lisääntyneet räjähdysmäisesti vuodesta 2019 läh-

6 Tilastokeskus, ”Befolkningens användning av informations- och kommunikationsteknik”.

7 Finanssiala Ry, ”Varo, varmista ja varoita: Nettihuijaukset ja tietojenkalastelu muuttavat muotoaan, mutta niiltä on mahdollista suojautua”, 2022.

tien, ja kaikki merkit viittaavat tämän jatkumiseen. Vuonna 2023 suomalaisilta arvioidaan huijatun yli 40 miljoonaa euroa.[8] Erilaiset rakkaushuijaukset ovat myös yleistymässä. Tekoälyn avulla usein uhria lähellä olevan henkilön on helpompi jäljitellä tekstiä, ääntä ja kuvaa, mikä lisää myös todennäköisyyttä joutua salasanojen louhinnan ja muiden huijausten uhriksi.[9]

KUVA 2 Poliisin tietoon tulleet tietotekniikkarikokset ja verkkopetokset 2006–2023



Lähde: Poliisi, Tilastokeskus

8 Markku Korhonen/Cryptonews, ”Valtavaa kasvua: Digihuijaukset Suomessa lisääntyivät”, 2024.

9 Niklas Fagerström/Yle, ”Finländare har lurats på rekordmycket pengar på nätet – det handlar om tiotals miljoner euro på ett halvår”, 2023.

Mitkä ovat siis erilaisten hakkerointihyökkäysten ja petosten kustannukset? Tämän arvioimiseksi tarkastelemme ensin poliisin tietoon tulleiden tietojen tuhoamisen, tietoturvaloukkausten ja tietosuoja-rikkomusten määrää, joihin on osallistunut viranomaisia, yrityksiä ja yksityishenkilöitä. On tärkeää muistaa, että tietomurrot eivät ole samanlaisia – vahingonkorvauskustannukset voivat vaihdella suuresti tapaus-kohtaisesti. On myös tärkeää huomata, että luultavasti suuri määrä tapauksia jää ilmoittamatta, jos yritykset ja yksityishenkilöt eivät halua, pysty tai voi ilmoittaa hyökkäyksestä poliisille. Poliisin tietoon tulleiden tieto-turvaloukkausten, tietojen tuhoamisen ja tietosuojarikosten kokonaismäärä oli noin 17 000 vuonna 2023. Vakavien tietomurtojen määrä on kasvanut räjähdysmäisesti vuosien 2022 ja 2023 välillä, mikä johtuu toden-näköisesti hyökkäystiheyden tosiasiallisesta kasvusta ja yrityskohtaisen hyökkäyspinnan koon kasvusta. Lisäksi osa aiemmin tehdyistä tapauksista tuli poliisin tietoon vasta vuonna 2023.[10] Erityistä on, että useisiin sovelluksiin leviävät tietomurrot luokitellaan moninkertaisiksi rikoksiksi. Tämä tarkoittaa, että luku on korkeampi kuin jos sama hyökkäys luokitellaan yhdeksi hyökkäykseksi riippumatta siitä, kuinka moniin sovelluksiin se kohdistuu. Tämän vuoksi kehitämme matalan skenaarion, jossa oletamme, että yksittäiset vakavat tietoturvaloukkaukset edustavat viidennestä mitä poliisin tietoon todella tulleista tapauksista. Matalassa skenaariossa tapausten kokonaismäärä on noin 4 300.

Kun otetaan huomioon keskimääräiset kustannukset yrityksiin ja viranomaisiin kohdistuvaa verkko-hyökkäystä kohti Euroopassa, jotka olivat vuosina 2021–2023 noin 14 000 euroa, verkkorikollisuuden kokonaiskustannukset vuonna 2023 olisivat lähes 290 miljoonaa euroa.[11] Tämä vastaa noin 7 prosenttia kaikista valtion vuoden 2024 talousarvion määrärahoista. Se on enemmän kuin mitä ulkoasiain-, oikeus-, sisä- ja puolustusministeriölle on myönnetty – yhteensä! Verrattuna muihin maihin, kuten Ruotsiin, arvioidut kustannukset ovat suhteellisen matalat. Pelkästään ruotsalaisiin yrityksiin kohdistuneiden verkko-hyökkäysten kustannukset olivat noin 2 miljardia euroa jo vuonna 2021.[12] Edellä mainittujen piilolukujen vuoksi ei siis ole mahdotonta, että kustannukset olisivat Suomessa taulukossa 1 esitettyjä kustannuksia korkeammat. Joka tapauksessa kustannukset jarruttavat Suomen kilpailukykyä ja yritysten kasvua.

10 Poliisin rikostilastoja käsittelevän Tilastokeskuksen mukaan juuri nämä tekijät selittävät erityisesti vakavien tietomurtojen valtavan kasvun vuodesta 2022 vuoteen 2023.

11 Tietoverkkorikollisuuden keskimääräiset kustannukset ovat peräisin Statista Market Insight -tietokannasta ja edelleen Hiscoxilta ja Forrester Researchilta.

12 Tukholman kauppakamari, ”Cyberbrott mot svenska företag – hur bygger vi en säkrare framtid?”, 2022.

TAULUKKO 1 Skadekostnadsestimat för finska staten av samtliga cyberangrepp, 2023

Kuvaus	Arvio
Poliisin tietoon tulleet tapaukset	
Tietojen tuhoaminen, lukumäärä	80
Tietomurrot, lukumäärä	2 097
Vakavat tietomurrot, lukumäärä	14 171
Tietosuojarikkomukset, lukumäärä	697
Kaikki yhteensä, lukumäärä	**17 045**
Yhteensä vähäisesti vaikuttavat vakavat tietomurrot, lukumäärä	**4 291**
Muut muuttujat	
Keskimääräiset kustannukset hyökkäystä kohti Euroopassa, 2021–2023	14 636 €
Petosten kustannukset Suomessa, 2023	40 000 000 €
Kustannukset yhteensä, 2023	**289 470 620 €**
Kustannukset yhteensä, matalassa skenaariossa, 2023	**102 804 540 €**

Lähde: Tilastokeskus, Poliisi, Statista, Markku Korhonen/Cryptonews

3. Tietoverkkoturvallisuus-työ Suomessa

Toisen valtiovallan, erityisesti Venäjän, uhka on ajankohtaisempi kuin koskaan. Kuten alussa totesimme, tietoverkkoturvallisuuden on oltava laadukasta, jotta nykyaikainen yhteiskunta voisi toimia. Tätä vastuuta on nyt myös laajennettu entisestään osana Suomen Nato-jäsenyyttä. Suomi on ottanut viime vuosina merkittäviä askeleita.

Suomessa turvallisuuskomitea avustaa sekä hallitusta että ministeriöitä asioissa, jotka koskevat kokonaisvaltaista turvallisuutta. Turvallisuuskomitea koostuu puheenjohtajasta, joka on käytännössä puolustusministeriön pysyvä sihteeri, sekä ministeriöiden pysyvistä sihteereistä, poliisin pääjohtajasta, tullin pääjohtajasta jne. Turvallisuuskomitean tehtäviin kuuluu koordinointityö yhteiskunnan elintärkeiden toimintojen turvaamiseksi, huoltovarmuuden ylläpitämiseksi ja hyvän ennakkosuunnittelun varmistamiseksi. Vaikka turvallisuuskomitean vastuualueet eivät suoranaisesti liity tietoverkkoturvallisuuteen, sen työ liittyy suoraan tietoverkkoturvallisuuteen.

Turvallisuuskomitea julkaisi vuonna 2013 Suomen ensimmäisen tietoverkkoturvallisuusstrategian. Strategiassa esitettiin tietoverkkoturvallisuuden vastuunjako, jossa hallitus on ylimpänä, mutta jokainen ministeriö ”vastaa tietoverkkoturvallisuudesta ja siihen liittyvien vaaratilanteiden hallinnasta”.[13] Tätä tarkistettiin osittain vuoden 2019 uudella tietoverkkoturvallisuusstrategialla (joka on edelleen voimassa). Liikenne- ja viestintäministeriöön perustettiin muun muassa kyberturvallisuusjohtajan virka, jonka tehtävä on ”koordinoida tietoverkkoturvallisuuden kehittämistä, suunnittelua ja varautumista yhteiskunnan tasolla”.[14] Strategiassa kuitenkin huomautetaan, että uuden viran perustaminen ei muuta ”ministeriöiden ja toimivaltaisten viranomaisten vastuita ja toimivaltaa tietoverkkoturvallisuuden alalla”.[15] Nykyinen valtion kyberturvallisuusjohtaja on Rauli Paananen.

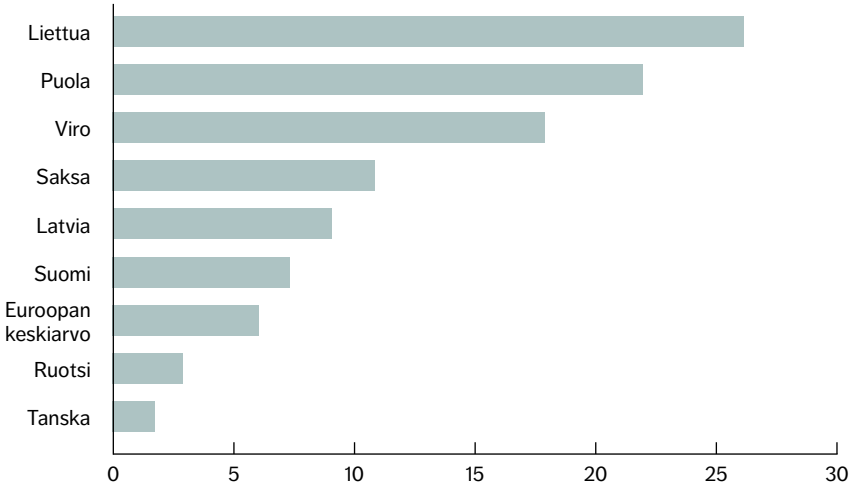
13 Turvallisuuskomitea, "Suomen kyberturvallisuusstrategia", 2013.

14 Turvallisuuskomitea, "Suomen kyberturvallisuusstrategia 2019”, 2019.

15 Ibid.

Yksi ensimmäisen tietoverkkoturvallisuusstrategian keskeisistä tavoitteista oli tehdä Suomesta vuoteen 2016 mennessä globaali edelläkävijä tietoverkkouhkiin varautumisessa. Jälkikäteen voimme sanoa, että emme ole onnistuneet. e-Governance Academy laatii kansallisen kyberturvallisuusindeksin ja digitaalisen kehityksen tason indeksin, jotka vähennetään toisistaan mittaamaan, kuinka hyvin maan kyberturvallisuus vastaa sen digitaalisen kehitystason vaatimuksia. Tämä esitetään kuvassa 3. Luvut on nähtävä suhteellisina siinä mielessä, että maa, jonka nettoluku on korkeampi, pystyy paremmin vastaamaan tietoverkkoturvallisuustarpeisiinsa. Lähialueillamme Baltian maat, Puola ja Saksa menestyvät Suomea paremmin. Suomi voi nähdä positiivisena puolena sen, että se on vain hieman EU:n keskiarvon yläpuolella, mutta tämä tuskin on kelvollinen tulos maalle, joka pyrkii olemaan tietoverkkovalmiuden edelläkävijä. Maa ei voi olla maailman johtava teknologia- ja tietotekniikkainfrastruktuurin alalla ilman, että on myös maailman johtava tietoverkkoturvallisuuden ja -valmiuden alalla.

KUVA 3 Indekseihin perustuva nettopistemäärä tietoverkkoturvallisuuden nykyisiä tarpeita vastaavuudesta

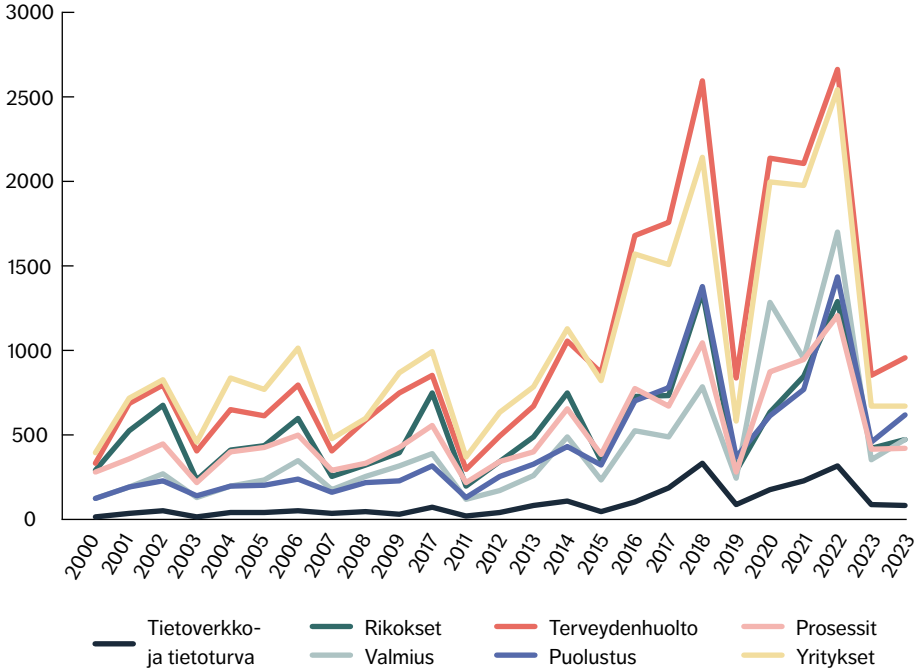


Huom: Indeksi perustuu painotettuun arviointiin lainsäädännöstä, poliittisista päätöksistä ja vuorovaikutuksesta asianomaisten yhteiskunnallisten toimijoiden välillä. Nollan suuruinen luku tarkoittaa, että tietoverkkoturvallisuuden vähimmäisvaatimus täyttyy, kun otetaan huomioon olemassa oleva digitaalinen infrastruktuuri. Tässä yhteydessä on huomattava, että nettoluku voi olla korkea, vaikka tietoverkkoturvallisuus absoluuttisesti mitattuna olisi heikompi. Tämä kuvaa hyvin tilannetta, jossa digitaalinen kehitys on yleisesti ottaen vähäistä.
Lähde: e-Governance Academy

Erityisesti tietoverkkoturvallisuus on saanut suhteellisen vähän huomiota maan poliitikoilta. Kuvassa 4 esitetään parlamentin verkkosivuilta etsimieni eri termien esiintymistiheys – ”kyberturvallisuus”, ”sarjat”, ”liiketoiminta” ja ”terveydenhuolto”. Kuvassa esitetään siis yhteenveto hakusanaan liittyvien asiakirjojen määrästä vuosien 1991–2024 aikana. Toistuvien ongelmien taustalla on usein se, että hallitukset tehostavat toimintaansa toimikautensa lopussa, kun taas uusien hallitusten käynnistäminen vie aikaa. Olen tehnyt kaksi erillistä hakua ”kyber- ja tietoturvan” osalta, yhden ”kyberturvallisuuden” ja toisen ”tietoturvan” osalta, ja olen tehnyt niistä yhteenvedon.

Tietoverkko- ja tietoturvaa ei näytä priorisoitavan yhtä paljon kuin näitä aloja. Tietoverkko- ja tietoturvan osalta korkein luku kirjattiin vuonna 2022, jolloin parlamentaaristen tapausten määrä oli 314. Vertailun vuoksi mainittakoon, että kaikkia muita käsitteitä koskevien asiakirjojen määrä ylitti samana vuonna 1 000:n rajan. Myöskään tuleva suuntaus ei ole vahvasti nouseva. Vuodesta 2023 lähtien, Marinin hallituksen jälkeen, ero muihin käsitteisiin on pienentynyt huomattavasti, mutta on myös muistettava, että vuosi 2024 on Orpon hallituksen toinen hallitusvuosi. Historiallisen kehityksen perusteella tämä ero todennäköisesti kasvaa toimikauden edetessä.

KUVA 4 Tiettyjä avainsanoja sisältävien parlamentaaristen tapausten määrä vuosina 1991–2024



Huom: Kaikki käsitteet haettiin Eduskunnan verkkosivuilta 30.9.2024. Lähde: Suomen eduskunta

Eduskunnan verkkosivuilla on myös mahdollista nähdä, kuinka suuri osa eri hakusanoista liittyy myös muihin niin sanottuihin ”avainsanoihin”. Jos esimerkiksi haemme hakusanalla ”varautuminen”, voimme nähdä, kuinka moni näistä asiakirjoista liittyy myös ”kyberturvallisuuteen”. Tietoverkkoturvallisuuteen liittyvät myös seuraavat asiakirjat: 0,1 % ”yritys”, 0,13 % ”rikollisuus”, 0,38 % ”varautuminen” ja 0,42 % ”puolustus”. Matala prosenttiosuus voi tuntua oudolta, varsinkin kun nämä ovat aloja, joilla tietoverkkoturvallisuutta pidetään tärkeänä tai jotka liittyvät siihen läheisesti. Yhä useammat yritykset sanovat, että suurimmat tulevat haasteet ovat häiriöt arvoketjussa ja verkkohyökkäykset.[16] Lisäksi tietoverkko- ja tietoturva on olennainen osa rikollisuuden torjuntaa, ja se kulkee käsi kädessä valmiuden ja puolustuksen parantamisen kanssa.

Poliittiset päättäjät ovat kuitenkin lähiaikoina antaneet useita myönteisiä signaaleja kunnianhimoisuuden lisäämisestä tietoverkkoturvallisuuden alalla. Vuonna 2022 laadittiin Digitaalinen kompassi Suomelle vuoteen 2030, jonka yhdessä kulmassa on myös tietoverkkoturvallisuustavoitteet. Yksi merkittävistä tavoitteista on lisätä ihmisten yleistä osaamista digitaalisten välineiden ja tietoverkkoturvallisuuden alalla. Vuonna 2023 julkaistiin sisä- ja puolustusministeriön laatima raportti. Se sisältää toimenpiteitä, jotka voidaan toteuttaa lyhyellä ja pitkällä aikavälillä.[17] Yksi pitkän aikavälin toimenpide on puolustusvoimien, poliisin, Supon ja Traficomin mahdollisuus jakaa ja analysoida joitakin tietoja helpommin keskenään. Lyhyen aikavälin toimiin kuuluvat nykyisen tietoverkkoturvallisuusstrategian päivittäminen ja julkisen ja yksityisen sektorin toimijoiden välisen yhteistyön parantaminen. Tarkastelu on osittain kantanut hedelmää, sillä valtioneuvoston kanslia käynnisti 8.3.2024 valtioneuvoston turvallisuusjohtamisen toimintamallin kehittämistä koskevan tarkastelun, johon sisältyy myös Suomen tietoverkkoturvallisuusstrategian uudistaminen. tietoverkko-turvallisuusstrategian uudistustyötä valmistelee valtion kyberturvallisuusjohtajan johtama alaryhmä. Työryhmän toimikausi päättyy 31. lokakuuta 2024.

Nykyään on olemassa erilaisia yhteistyöpaikkoja, kuten Traficomin tietoverkkoturvallisuuskeskus, jonka tavoite on saattaa yhteen julkisen, yksityisen ja kolmannen sektorin toimijoita.[18] Keskuksen tehtävä on myös avustaa sidosryhmiä seurannassa ja vaaratilanteiden hallinnassa, tilannearvioinneissa ja

16 Allianz, ”Risk Barometer – Identifying the major business risks for 2023”, 2022.

17 Valtioneuvosto, ”Selvitys: Suomen kyberturvallisuutta tulee kehittää määrätietoisesti, viranomaisten yhteistyötä ja prosesseja pitää edelleen parantaa”, 2023.

18 Traficomin tietoturvakeskus, ”Kansallisen koordinointikeskuksen tehtävät”, 2023.

neuvonnassa. Vuonna 2023 myös Suomen kansallinen koordinointikeskus (NCC-FI) aloitti toimintansa Kyberturvallisuus-keskuksen tutkimus-, kehitys- ja innovaatiotoiminnan alaisuudessa. Kuten johdannossa mainittiin, tietoverkkoturvallisuus, liikenneinfrastruktuuri ja toimitusvarmuus liittyvät läheisesti toisiinsa. Se tarkoittaa, että kansallinen Huoltovarmuuskeskus on myös tietoverkkoturvallisuuden kannalta merkittävä toimija. Valtioneuvostolle raportoiva Huoltovarmuuskeskus on osittain vastuussa huoltovarmuuden kannalta tärkeiden toimijoiden yhteen kokoamisesta.

Vaikka jotkin toimenpiteet, kuten valtion kyberturvallisuusjohtajan perustaminen, osoittavat hyvää tarkoittavaa halua lisätä tietoverkkoturvallisuutta yhteiskunnassa, instituutioiden suuri määrä saattaa hämärtää vastuualueita. Yksittäisten viranomaisten suuri vastuu omista osa-alueistaan voi myös johtaa tiedonvaihdon puutteeseen ja rajusti vaihteleviin käytäntöihin eri viranomaisten välillä. Tämä voi korostua erityisesti vaalien yhteydessä, kun virkamiehet vaihtuvat ja uudet aloittavat työnsä ministeriöissä. Ilman selkeästi määriteltyjä vastuualueita yksityishenkilöiden, yritysten ja kolmannen sektorin toimijoiden on myös vaikea tietää, kenen puoleen voi kääntyä tietoverkkohyökkäyksen sattuessa.

4. Virolainen huippuosaaminen

Viro on toteuttanut merkittäviä digitalisaatiohankkeita Neuvostoliitosta vapautumisensa jälkeen vuodesta 1991 alkaen. Viron parlamentti hyväksyi jo vuonna 1994 periaateohjelman, jonka yhtenä tavoitteena oli varata yksi prosentti bruttokansantuotteesta informaatioteknologiainvestointeihin. Vuonna 1996 käynnistettiin ensimmäiset sähköiset pankkipalvelut, ja ajan myötä lähes kaikki julkiset palvelut on digitalisoitu ja siirretty niin sanottuun e-Estoniaan. e-Estonia Briefing Centren mukaan 99 prosenttia kaikista maan julkisista palveluista on saatavilla verkossa 24 tuntia vuorokaudessa seitsemänä päivänä viikossa. e-Estoniaan kuuluu muun muassa kansallinen pysäköintipalvelu, mahdollisuus rekisteröidä avioliitot digitaalisesti, poliittisten kokousten suoratoisto ja paljon muuta. e-Estonian tietovirroissa käytetään kehittynyttä salausta ja digitaalisia allekirjoituksia.

Viro perusti maailman ensimmäisen datasuurlähetystön Luxemburgiin vuonna 2015. Datasuurlähetystön tarkoitus on suojata ja ylläpitää turvaluokiteltua tietoa ja käsitellä kriittisten tietovirtojen varmuuskopioita. Datasuurlähetystön tallentamiin laajempiin tietokokonaisuuksiin kuuluvat muun muassa tuomioistuinten tiedostojärjestelmä, maarekisteri, yksittäisiä henkilöitä koskevat verotiedot ja väestörekisteri. Suur-lähetystöllä on niin sanottu Tier-4-turvasuojaus, joka on suurten tietokeskusten korkein turvallisuustaso. Suurlähetystöllä ja sen henkilökunnalla on diplomaattinen koskemattomuus, ja yksikköä johtaa Viron ulkoasiainministeriö.

Korkeatasoisen digitalisaation ohella Virossa on myös korkeatasoinen tietoverkkoturvallisuus. Kesti kuitenkin vuoteen 2007, ennen kuin Viro nosti tietoverkkoturvallisuuden samassa määrin etusijalle.

Viroon vuonna 2007 kohdistuneet palvelunestohyökkäykset ovat tähän mennessä edelleen yksi suurimmista palvelunestohyökkäyksistä. Ne seurasivat Viron ja Venäjän välistä pitkää kiistaa sen jälkeen kun virolaiset päättäjät olivat suostuneet siirtämään neuvostoliittolaisen ”Pronssisotilaan” pois Tallinnasta. Palvelunesto-hyökkäyksillä pyritään ylikuormittamaan verkkosivustoa

internetliikennettä ohjaamalla, jolloin kukaan muu ei pääse verkkosivustolle. Hyökkäykset vaikeuttavat palvelujen ja tietojen saantia. Hyökkäykset kohdistuivat pankkeihin, tiedotusvälineisiin ja viranomaisiin. Hyökkäyksen kohteeksi joutuneiden pankkien verkkopalvelut eivät toimineet, mediaorganisaatioilla oli vaikeuksia välittää uutisia ja hallituksen viestintäyhteydet olivat poikki. Hyökkäykset kestivät kolme viikkoa, ja monet venäläisryhmät ovat ilmoittautuneet iskujen tekijöiksi. On vahvoja viitteitä, että iskut tehtiin tiiviissä yhteistyössä Venäjän viranomaisten kanssa.

Nato käynnisti laajan tutkimuksen tapahtumien kulun kartoittamiseksi ja perusti vuonna 2008 Tallinnaan Naton yhteistoiminnallisen kyberpuolustuksen osaamiskeskuksen, joka tunnetaan myös nimellä CCDCOE. Se laati nopeasti niin sanotun Tallinnan käsikirjan kansainvälisen oikeuden soveltamisesta tietoverkko-konflikteihin liittyvissä asioissa. Nykyään CCDCOE on keskeinen toimija puolustusliiton kyberpuolustukseen liittyvässä työssä. Se tarjoaa foorumin yhteisten käytäntöjen kehittämiseksi, tutkimuksen tekemiseksi ja yhteisen tietoverkkoturvallisuuskoulutuksen lisäämiseksi. [19] Pian CCDCOE:n perustamisen jälkeen EU perusti Tallinnaan myös EU-Lisa-viraston, jonka tehtävä on koordinoida arkaluonteisia tietoja käsittelevien tietojärjestelmien sisäistä turvallisuutta.

Kansallisella tasolla hyökkäys sai Viron perustamaan kyberturvallisuusneuvoston suoraan valtion turvallisuus-komitean alaisuuteen. Kyberturvallisuusneuvoston tehtävä on toimia viranomaisten yhteyspisteenä ja varmistaa kansallisen tietoverkkoturvallisuusstrategian noudattaminen.[20] Viro oli yksi ensimmäisistä maista, joka laati kansallisen tietoverkkoturvallisuusstrategian, joka sisältää tavoitteet, uhat ja edellytykset. Viron tietoverkkoturvallisuusstrategiat ovat olleet kattavia. Niissä on yksilöity sekä ensisijaisia toimia että tiettyjä aihealueita, joilla tietoverkkoturvallisuutta voidaan parantaa. Viro kehittää järjestelmällisesti tarkistettua tietoverkkoturvallisuusstrategiaa neljän vuoden jaksoissa. Määrä ei aina tarkoita laatua, mutta määrä voi aina olla suuntaa-antava – Viron uusin tietoverkkoturvallisuusstrategia on 72 sivua pitkä, kun taas Suomen uusin tietoverkkoturvallisuusstrategia vuodelta 2019 on 12 sivua pitkä.

19 Virallisesti vapauden, turvallisuuden ja oikeuden alueen laaja-alaisten tietojärjestelmien operatiivisesta hallinnoinnista vastaava eurooppalainen virasto.

20 Republic of Estonia Ministry of Economic Affairs and Communications, ”Cybersecurity Strategy 2019–2022”.

Viro on laatinut oman digitaalisen asialistan vuoteen 2030, joka on samankaltainen kuin Suomen digitaalinen kompassi. Toisin kuin digitaalisessa kompassissa, jossa tietoverkkoturvallisuus on yhdessä kulmassa, tieto-verkkoturvallisuus on yksi Viron digitaalisen asialistan kolmesta pääkohdasta. Asiakirja sisältää myös useita konkreettisia tavoite-ehdotuksia. Ehdotuksiin kuuluu muun muassa tietoverkkoturvallisuuteen erikoistuneen ajatushautomon perustaminen, sekä tietoverkkoturvallisuustutkimuksen lisääminen ja parantaminen maan yliopistoissa ja tutkimuslaitoksissa. Siinä luvataan myös laatia kansallinen suunnitelma, jolla koordinoidaan kaikkea erityisesti tietoverkkoturvallisuuteen liittyvää kansallista tutkimus- ja kehitystyötä.[21]

Tärkeä osa Viron strategiaa on ollut lisätä yleistä tietoverkkoturvallisuuden ymmärtämistä yhteiskunnassa. Tämän ansiosta Virossa on nyt runsaasti osaajia, jotka ymmärtävät sekä digitalisaatiota että tietoverkko-turvallisuutta. Virossa järjestetään useita konferensseja, kuten vuosittainen *Digital Summit* ja *Nordic-Baltic Security Summit*. Nuorilla on mahdollisuus osallistua sekä koulutukseen että tietoverkkoturvallisuutta käsitteleviin tapahtumiin. Julkisella puolella TalTechin Centre for Digital Forensics and Cyber Security tarjoaa koulutusta ja opintoretkiä luokille ja nuorille. Arvioiden mukaan yli 150 000 vähintään 7-vuotiasta oppilasta ja opiskelijaa sekä yli 5 000 opettajaa on osallistunut erilaisiin ohjelmiin ja tapahtumiin vuosien 2017–2021 aikana. Erityisen kiinnostuneille on tarjolla sekä kandidaatin että maisterin tutkintoja tietoverkko-turvallisuuden alalla Tallinnan teknillisessä yliopistossa ja Tarton yliopistossa. Yksityisellä puolella CTF Tech -yritys on järjestänyt jo useiden vuosien ajan *Cyber Battlea*, joka on suunnattu 18–24-vuotiaille. Cyber Battle -kilpailussa joukkueet kilpailevat erilaisten tietoverkkohyökkäysskenaarioiden ratkaisemisesta ja saavat pisteitä suorituksestaan. Vuoden 2023 turnauksessa järjestettiin myös alueellinen turnaus muiden Baltian maiden ja Pohjoismaiden kanssa. CTF Tech järjestää myös erilaisia kursseja ja kehittää parhaillaan sekä opettajille että opiskelijoille suunnattua *e-learning*-alustaa.

21 Republic of Estonia Ministry of Economic Affairs and Communications, ”Estonia’s Digital Agenda 2030”, 2023.

5. Tie eteenpäin

On tärkeää tarkistaa nykyinen tietoverkkoturvallisuusstrategia, jotta voidaan määrittää, miten Suomi vahvistaa tietoverkkoturvallisuuttaan nyt ja tulevaisuudessa. Seuraavassa on kaksi tärkeintä Viron innoittamaa ehdotusta, jotka haluaisimme poliittisten päättäjiemme asettavan etusijalle.

Seurataan Viron esimerkkiä ja investoidaan digitalisaatioon ja tietoverkkoturvallisuuteen

- **Varataan suurempi osuus BKT:sta tietotekniikkaan ja tietoverkkoturvallisuuteen tehtäviin investointeihin.** Viron varhaisvaiheen ponnistelujen tapaan Suomen olisi lisättävä investointeja tietoverkkoturvallisuuteen. Se auttaa myös hillitsemään tietoverkko-rikollisuuden kasvavia kustannuksia ja valmistautumaan tuleviin hyökkäyksiin. Hallituksen tulisi minimoida tietoverkkohyökkäysvahinkojen aiheuttamat kustannukset ja asettaa Suomelle raja, jonka ylittyessä kustannukset eivät saisi nousta.
- **Kartoitetaan tietoverkkohyökkäysten aiheuttamat todelliset vahinkokustannukset.** Tässä raportissa arvioimme tietoverkkohyökkäysten aiheuttamien vahinkojen kustannuksiksi Suomessa lähes 290 miljoonaa euroa, mikä on luultavasti aliarvioitu, koska raportoimattomien tapausten määrä on suurempi. Hallituksen tulisi käynnistää tutkimus, jossa selvitetään, paljonko tietoverkkohyökkäykset maksavat Suomelle – yksityiseltä ja julkiselta sektorilta.
- **Datasuurlähettilää ja turvallinen tietojen varastointi.** Tutkitaan mahdollisuutta perustaa Viron kaltainen datasuurlähetystö, jossa kriittisiä tietoja voidaan säilyttää ulkomailla erittäin turvallisesti. Tämä suojaisi hallituksen tärkeitä tietoja verkkohyökkäysten tai muiden uhkien varalta.

- **Vastuualueiden selventäminen.** Sidosryhmien on tiedettävä, minkä viranomaisen tai toimijan puoleen he voivat kääntyä, ja miten verkkohyökkäykselle altistuessa pitäisi reagoida. Selvitetään, kuinka Suomessa voidaan ottaa mallia Viron rakenteesta, joka vaikuttaa avoimemmalta ja helpommin ymmärrettävältä.

Seurataan Viron esimerkkiä ja keskitytään koulutukseen ja tutkimukseen

- **Tarjotaan koulutusmahdollisuuksia varhaisessa vaiheessa.** Konkretisoidaan, miten koulutusala voi osallistua tieto- ja tietoturvaa koskevien tietojen ja taitojen lisäämiseen. Tietoverkkoturvallisuuteen osallistumisen pitäisi olla trendikästä, ja hyvä tapa saavuttaa tämä on tarjota koulutusmahdollisuuksia jo varhaisessa vaiheessa.
- **Investoidaan tutkimukseen ja kehitykseen.** Opetus- ja kulttuuriministeriö myöntää yliopistoille 255 miljoonaa euroa lisärahoitusta kokeiluohjelmaan, jonka puitteissa otetaan noin 1 000 uutta tohtorikoulutettavaa vuosina 2024–2027. Pilottiohjelmassa ei keskitytä pelkästään tietoverkkoturvallisuuteen, vaikka muille digitalisaatioon liittyville kysymyksille onkin annettu lippulaiva-alueiden asema. Hallituksen tavoite käyttää neljä prosenttia BKT:sta tutkimukseen ja innovointiin luo hyvät mahdollisuudet integroida pilottiohjelmat osaksi tulevaisuuden korkeakoulutusta. Tietoverkkoturvallisuudesta olisi tehtävä lippulaiva-alue, ja osa rahoituksesta olisi suunnattava tietoverkkoturvallisuuden tohtorikoulutusohjelmiin.

Kommentti

Yritysten ja kansalaisten kyberturvallisuuden kehittäminen

Elämme kolmatta vallankumousta, jossa digitaalisuus muuttaa yhteiskuntien ja liiketoimintojen perusrakenteita – kaikki raha, data ja toiminnallisuus digitalisoituu. Samalla kaiken rahan, datan ja toiminnallisuuden suojaustavat muuttuvat. Tässä on kysymys kyberturvallisuudesta. Kun kaikkea ei voi suojata, valtionhallinnossa kuuluu priorisoida resurssien tehokkain kohdentamistapa yhteiskunnan keskeisimpien toimintojen suojaamiseksi, meidän kaikkien eduksi. Miten Suomi on onnistunut kyberturvallisuudessa ja onnistuu jatkossa?

Digitalisaatio koskee kaikkia yhteiskunnassamme, puhutaanpa sitten terveystiedoista terveydenhuollon järjestelmissä ja laitteiden ohjauksesta vanhustenhoidossa, yritysten ja kansalaisten rahojen käytöstä pankkitoiminnassa, teollisuuslaitoksen ostojen ja myyntien maksuliikenteestä, tehtaan tuotannon ohjauksesta tai vaikkapa ihmisten arjen ajankäytöstä sarjojen ja verkkopelien parissa. Kaikessa, missä ajankohtaiset uutiset ja viranomaisten antamat varoitukset välittyvät digitaalisten verkkojen ja sovellusten kautta tiedoksemme. Digitalisaatio siis koskee aivan kaikkea: jokainen yritys ja organisaatio on nykyään digiorganisaatio, tunnistipa sen tai ei. Ei ole yksittäistä tahoa, joka kykenisi määrittämään ja ymmärtämään kaikkien erilaisten liiketoiminnallisuuksien merkityksen ja siten päättämään kaikkein parhaasta suojauksesta. Yhteiskunnan perusrakenteisiin ulottuva digitalisaation muutos edellyttää vastaavaa osallisuutta.

Digitalisaatio on jo kaikkialla – niin on oltava myös kyberturvallisuuden

Digitalisaaton myötä sen suojauksen, kyberturvallisuuden, tulee olla kaikkien agendalla ja vastuulla – kaikkien perusrakenteissa. Tekniset valtiollisen suojauksen kyvykkyydet on sen sijaan perusteltua keskittää, jotta kaikki saisivat teknistä tukea tasapuolisesti. Tässä Liikenne- ja viestintäviraston kyberturvallisuuskeskus on digitaalisen maailman palokunta, ja ilmoitus sinne tuo ensiavun.

Kuten normaaleissa rikoksissa, poliisi on toimija, joka selvittää rikostutkinnassa tapahtumien kulun. Tähän on erikoistunut vakavampien kyberrikosten osalta Keskusrikospoliisin kyberkeskus. Puolustusvoimien rooli ulottuu sotatilanteisiin. Monin paikoin näiden rajat ovat hieman häilyvät, ja siellä toimijoiden yhteistyöllä on keskeinen merkitys – vahva suojaus vaatii kaikkien panosta.

Valtiolliset kyberkyvykkyydet suojaavat kansalaisten elintärkeitä toimintoja

Valtiollisten kyberkyvykkyyksien taito torjua ja suojata kyberhyökkäyksiä saa erityistä merkitystä tilanteessa, jossa yrityksestä tulee yhteiskunnan puolustaja. Kun valtiollinen taho tai rikollinen organisaatio pyrkii heikentämään kansalaisten kriisinsietokykyä rapauttamalla kriittisten palvelujen luotettavuutta tai ansaitsemaan kiristämällä niiden lamauttamisella, valtion kyvykkyydellä suojata yritysten tukena kansalaisten elintärkeitä toimintoja on keskeinen merkitys. Lisäksi valtion rooli korostuu, kun sen omaan toimintaan kohdistetaan haitantekoa tai jopa fyysisiä hyökkäyksiä, joissa hyödynnetään verkosta julkisilta toimijoilta tai kriittisiltä yrityksiltä saatavilla olevaa tietoa keskeisistä kriittisistä pullonkauloista. Tällaisissa tilanteissa on yhteiskunnan vastuulla yhdistää keskeisimmät toimijat, varmistaa saumaton tiedonkulku ja suojata toimintoja, mikä on kaikkien etu ja varmistaa kansalaisten sujuvan arjen.

Sektoriviranomaiset ymmärtävät suojattavat kriittiset palvelut

Kun puhutaan kansalaisten arjen kyberturvallisuudesta, jakaantuu vastuu sekä käyttäjään että palvelun tuottajaan. Käyttäjä voi käyttää palvelua digitaalisesti, tai palvelun taustalla voi olla järjestelmiä, jotka vaikuttavat palvelun tuottamiseen. Kansalainen ei voi vaikuttaa merkittävästi niiden toimintaan ja turvallisuuteen. Tavanomaisista palveluista puhuttaessa riskiarvio on normaalia liiketoimintaa: kuinka paljon yritys panostaa digitaalisten laitteiden toimivuuteen tai kyberuhkiin. Kun palvelu on yhteiskunnalle kriittinen, asiakas ei voi vaikuttaa käyttääkö hän palvelua vai ei, ja palvelu on normaalin arjen perusedellytys, on yhteiskunnalla yrityksen omien ratkaisujen lisäksi vastuu valvoa ja edesauttaa palvelun turvallisuutta.

Yhteiskunnan tarvitsema kyberturvallisuus voi toteutua lakisääteisin minimivaatimuksin tai yhteiskunnan tarjoamin palveluin, joilla yritys kykenee ylläpitämään palvelun hyvätasoista kyberturvallisuutta. Tässä sektoriviranomaiset ja huoltovarmuuskeskus verkostoinensa ovat parhaita määrittämään, mitkä ovat keskeisiä turvattavia palveluja ja niiden pullonkauloja. Sektoriviranomaisia ovat vaikkapa Valvira terveydenhuollossa ja Energiavirasto energiahuollossa. Kyberturvallisuuskeskus taas kykenee tuottamaan minkä tahansa alan teknisen suojaamisen tueksi kyberturvallisuuden tilannekuvaa ja havainnointipalveluja, joilla vaikkapa vakavat haittaohjelmat pidetään kurissa. Huoltovarmuuskeskus rahoittaa näiden yhteiskunnallisten palvelujen kehitystä yritysten käyttöön ja lopulta siis kansalaisten turvaksi. Näin kaikkien tahojen paras osaaminen, tiedot ja taidot ketjuuntuvat yhteiskunnan turvaksi.

Kyberturvallisuus on nykyajan kansalaistaisto

Kansalaisille, palvelujen asiakkaille, käyttäjille jää oma vastuu käyttää digitaalisia palveluja turvallisten periaatteiden mukaisesti. On palveluntarjoajankin etu, että asiakkaat eivät tule huijatuksi ja menetä rahaa tai tietoa, koska se ei ole eduksi kenenkään liiketoiminnalle. Siten palveluista pyritään tekemään myös mahdollisimman turvallisia. Lisäksi pyritään vähentämään riskiä tilanteista, joissa käyttäjä aiheuttaisi vahingossa tietoturvariskin itselleen tai palveluntarjoajalle, koska riski aiheuttaisi rahan tai tiedon menetyksen molemmille osapuolille. On edelleen mahdollista, ettei käyttäjä huolehtisi ohjeistusten mukaan oman laitteen suojauksesta, päivittäisi suositellusti tietoturvaa tai tulisi huijatuksi.

Valitettavasti rikolliset pyrkivät yleensä löytämään inhimillisiä keinoja saada käyttäjä tekemään virheitä. Kuten edeltävässä raportissa todetaan, kaikesta osuuden vieminen digitaalisella rikoksella on miljardibisnes, jossa rahavirtoja höylätään juustohöylällä erilaisten huijausten avulla. Taskuvarkaat ovat löytäneet verkosta uuden tavan putsata takataskuja. Viranomaiset ja yritykset pyrkivät estämään tällaiset keinot, mutta myös kansalaisten perusturvallisuustaidot uusissa digirakenteissa ovat tarpeen. Vastaavaa perusosaamista edellytetään jokaiselta liikenteessä, kun käytetään yhteisessä käytössä olevia teitä.

Suomen kyberturvallisuus on maailman kärkeä

Miten Suomessa on onnistuttu tässä? Tuoreimmassa ITU-T:n kyberindeksiraportissa[22] Suomi sai täydet pisteet 11 muun maan kanssa. Kyberhyökkäykset suomalaisiin yrityksiin ja kansalaisten huijaukset ovat arkipäivää, mutta olemme viime vuosina välttäneet erityisen vakavat yhteiskunnallisesti vaikuttavat tilanteet. Voisi sanoa, että periaatetasolla suomalainen verkottunut tapa toimia on osoittautunut edistykselliseksi ja turvallisuutta tuovaksi – olemme kyberturvallisuuden suuntaa näyttävä mallimaa Viron rinnalla. Mutta lopulta turvallisuus ratkaistaan arjessa: kuinka toimimme yhdessä, kun digitalisaation edistyminen jatkuu. Tekoäly ja kvanttilaskenta tuovat uudet kyberuhat laittamaan koetukselle järjestelmäämme, jossa meillä on vahva rakenteellisesti kattava pohja.

Keskinäisriippuvan yhteiskunnan turvaaminen ei ole yksinkertaista, sillä riippuvuudet muuntuvat ja hyökkääjät pyrkivät iskemään rahan tai datan ahneudessa epäkohtiin, jotka ovat jääneet ilman selkeää vastuuta ja suojausta. Yksi taho ei kykene hallitsemaan tietopääomaltaan kaikkea, jolloin yhteistyö on välttämätön edellytys. Turvaamisen kannalta rakenne on tapa organisoida, ja sen voi tehdä hyvin ja huonosti monella tavalla. Lopulta onnistumisen ratkaisee asenne: haluammeko onnistua yhdessä? Suoriutua parhaalla mahdollisella tavalla omasta vastuusta ja auttaa kumppania onnistumaan omassaan? Kun asenteet ovat kunnossa, on henkinen pääoma – vahva, digitaalinen sietokyky taattu. Kyberturvallisuus tukee henkistä kriisinsietokykyä – iskipä mikä vaan, mihin vaan. Me selviämme siitä yhdessä.

Jarna Hartikainen
Yksikön johtaja
Varautumisen suunnittelu
Huoltovarmuuskeskus

22 https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

Lähdeluettelo

Allianz, ”Risk Barometer – Identifying the major business risks for 2023”, 2022.

Andrew Kramer/The New York Times, ”Hackers Bring Down Government Sites in Ukraine”, 2022.

Dann Pettersson/Hufvudstadsbladet, ”Finnair pausar flyg efter gps-störningar”, 2024.

ESET Research, ”IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine”, We Live Security, 2022.

Finanssiala Ry, ”Varo, varmista ja varoita: Nettihuijaukset ja tietojenkalastelu muuttavat muotoaan, mutta niiltä on mahdollista suojautua”, 2022.

Mai Periman, ”How to prevent the bank robbery no one can see”, Cisco, 2017.

Markku Korhonen/Cryptonews, ”Valtavaa kasvua: Digihuijaukset Suomessa lisääntyivät”, 2024.

Niklas Fagerström, ”Finländare har lurats på rekordmycket pengar på nätet – det handlar om tiotals miljoner euro på ett halvår”, Yle, 2023.

Republic of Estonia Ministry of Economic Affairs and Communications, ”Estonia’s Digital Agenda 2030”, 2023.

Republic of Estonia Ministry of Economic Affairs and Communications, ”Cybersecurity Strategy 2019–2022”.

Statistikcentralen, ”Befolkningens användning av informations- och kommunikationsteknik”.

Valtioneuvosto, ”Selvitys: Suomen kyberturvallisuutta tulee kehittää määrätietoisesti, viranomaisten yhteistyötä ja prosesseja pitää edelleen parantaa”, 2023.

Steve Morgan/Cybercrime Magazine, ”Cybercrime to cost the world $10.5 trillion annually by 2025”, 2020.

Tukholman kauppakamari, ”Cyberbrott mot svenska företag – hur bygger vi en säkrare framtid?”, 2022.

Turvallisuuskomitea, ”Suomen kyberturvallisuusstrategia 2019”, 2019.

Turvallisuuskomitea, ”Suomen kyberturvallisuusstrategia”, 2013.

Traficomin verkkoturvakeskus, ”Kansallisen koordinointikeskuksen tehtävät”, 2023.

40 miljoonaa euroa – arvioitu summa, joka suomalaisilta huijattiin netissä viime vuonna. Vuodesta 2019 lähtien suomalaisiin kohdistuvien nettihuijausten määrä on kasvanut räjähdysmäisesti: vuonna 2023 poliisille ilmoitettiin yli 7000 tapausta.

Verkossa eivät vain rikolliset ja jengit aiheuta ongelmia kansalaisille. Yhä useammin myös yksittäiset valtiot ovat verkkorikollisuuden takana. Ja missä ei ole rajoja, kuka tahansa voi loukkaantua.

Taloustieteilijä **Theo Herold** (Svenska Handelshögskolan) kertoo, mitä tietoverkkorikollisuus on ja kuinka paljon se maksaa Suomelle, mitä tehdään tietoverkkoturvallisuuden parantamiseksi ja mitä voisimme oppia Virosta, joka on monissa digitaalisen alan asioissa edelläkävijä.

Raportissa esitellään myös konkreettisia toimenpiteitä kyberturvallisuuden parantamiseksi sekä Huoltovarmuuskeskuksen kommentti siitä, miten yksilöt ja valtio voivat vahvistaa kyberturvallisuutta.

AGENDA
TANKESMEDJAN • AJATUSHAUTOMO