Centria SecuLabin tietoturva-podcast. Vieraana Kimmo Rousku 19.5.2023

Digitaalinen turvallisuus ja digiirohkeus

Tom Tuunainen
Centria SecuLab esittää tietoturva- podcast osa 10 digitaalinen turvallisuus ja digirohkeus.

Laura Palovuori
Meillä on täällä Centria SecuLabissa haastattelijoina Laura Palovuori ja Tom Tuunainen.
Ja tällä kertaa meillä on vieraana Kimmo Rousku. Tervetuloa esitteletkö itsesi?

Rousku Kimmo (DVV)
Kiitos ensinnäkin kutsusta, ilo olla täällä. Toimin digi- ja väestötietovirastossa, vuonna 2020 aloittaneessa uudessa virastossa, jossa väestörekisterikeskus ja maistraatit yhdistyivät uudeksi virastoksi. Siellä minulla on kaksi tehtävää. Ensimmäinen on, että toimin julkisen hallinnon digitaalisen turvallisuuden johtoryhmässä, eli Vahtin. Vahti on perustettu 1990- luvulla valtionhallinnon tietoturvallisuuden johtoryhmäksi, mutta on nyt laajentunut julkiseen hallintoon ja tietoturvan ohella laajemmin koko digiturvan kaikkiin osa alueisiin. Vahti-verkostossa meillä on hieman yli 500 asiantuntijaa, johdon edustajaa, kehittämässä yhdessä julkiselle hallinnolle turvallisia palveluita. Eli se on oikeastaan tämän Vahti-toiminnan merkitys, edistämme ja autamme julkisen hallinnon organisaatiota tuottamaan turvallisempia palveluita, mutta samalla myös kaikki muutkin, eli myös yritykset ja elinkeinoelämä pystyy hyödyntämään näitä meidän kehittämiämme tuotteita ja palveluita. Tämä on ensimmäinen tehtäväni. Toinen on sitten se, että olen meidän monivuotisessa hankkeessamme toiminut myös projektipäällikkönä ja siinä tehtäväni on ollut kehittää alan asiantuntijoiden osaamista ja tietoisuutta näistä asioista ja tämä on konkretiassa tapahtunut muun muassa kuukausittaisilla verkko-ohjelmilla, lähetyksillä sekä muilla vuosittaisilla, myös fyysisessä maailmassa toteutettavilla seminaareilla. Tämän ohella on vielä pakko kolmantena nostaa esille vapaa- ajan toimintani. Eli harrastan myös näitä samoja asioita eri roolissa. Olen Tietoturva ry:n hallituksen varapuheenjohtajana tänä vuonna ja siellä me tuotamme myös tilaisuuksia ja meillä on koko päivän seminaareja pari kappaletta vuosittain ja tämän tyyppistä toimintaa. Olen siis aika monessa mukana. Voisi sanoa, että aikanaan nuoruuden harrastuksesta tuli ammatti ja ammatista on tullut osin intohimo.

Tom Tuunainen
Mitä Digi-ja väestötietovirasto tekee?

Rousku Kimmo (DVV)
Digi- ja väestötietovirasto tuottaa palveluita sekä henkilö- että organisaatioasiakkaille. Tietysti kansalaisille näkyy enemmänkin nämä meidän henkilöpalvelumme. Oikeastaan kaikista tärkein asia, jota ei aina välttämättä huomata eikä ymmärretä, on että Suomessa tehtiin kuusikymmentäluvun puolivälissä todella merkittävä päätös luoda yhtenäinen tapa tunnistaa käyttäjiä eli silloin luotiin sosiaaliturvatunnus eli sotu, joka kyllä seitsemänkymmentäluvulla vaihtui sitten henkilötunnuksesi. Henkilötunnus on ollut oikeastaan meidän koko digitalisaation ehkä kaikkein tärkein päätös silloin aikanaan. Meidän tehtävänämme on vastata tästä väestötietojärjestelmästä, joka sitten vastaa

meidän väestötietojen liittyvästä tiedosta ja muun muassa tähän henkilötunnukseen liittyvistä asioista. No, sitten me huolehdimme nimiasioista, aina kun joka vuosi julkaistaan suosituimmat lasten nimet ynnä muut, ne poimitaan meidän tiedoistamme.

Vihkimiset hoituvat meidän kauttamme, eli yksi meidän sivunimemme onkin rakkausvirasto. Tervetuloa, meillä saa hyvää ja mielenkiintoista palvelua myös tuolta osin.

Ehkä yksi entistä tärkeämpi osa-alue on edunvalvonta ja toisen asioiden hoitaminen antamalla edunvalvontavaltuutus. Tämä on palvelu ja toiminto, jota kannattaa kyllä jokaisen tutkia ennemmin liian aikaisin kuin liian myöhään, eli siinä vaiheessa, kun ei enää itse kykene hoitamaan niitä asioitaan. Läheisen kuolemaan liittyvät tehtävät ja asiat ja niiden digitalisointi on erittäin tärkeä asia. Vaalit ja äänioikeus kuuluvat meille. Meillä on ollut tänä vuonna yhdet vaalit, seuraavaksi tulee tammikuussa presidentinvaalit, eli meillä on muun muassa äänioikeusrekisteri, kansalaisvarmenne ja sähköinen henkilöllisyys. Näitä asioita kehitetään eli käytännössä suomi.fi -palvelu on se, jota kautta valtaosa näistä meidän palveluistamme näyttäytyy. Eli nämä ovat muun muassa niitä tehtäviä, mitä DVV:ssä toteutetaan.

Tom Tuunainen
Teidän verkkosivuillanne mainitaan myös Taisto- harjoitukset. Mitä ne ovat ja pääseekö kuka tahansa niihin mukaan?

Rousku Kimmo (DVV)
Tämä on yksi osa meidän digiturvapalveluistamme. Taisto on harjoitus, joka toteutetaan tämän vuoden marraskuussa jo kuudennen kerran. Tämä oli yhden hankkeen lopputulos, kun yleinen tietosuoja asetus, GDPR, oli hyvin ajankohtainen silloin kuusi vuotta sitten. Harjoitellaan sitä, että miten ilmoitukset eri viranomaisille sujuvat, kun tapahtuu henkilötietojen tietoturvaloukkaus. Ensimmäinen taisto oli valtava menestys, kaksisataakolmekymmentäviisi organisaatiota osallistui. Tämän jälkeen harjoitus on vuosittain kasvanut niin, että viime vuonna meillä oli kolmesataaseitsemänkymmentäviisi organisaatiota harjoittelemassa.

Meillä on aina marraskuussa torstaipäivät Taistoa täynnä, eli siellä on mahdollisuus tänä vuonna viitenä eri päivänä osallistua tähän saman sisältöiseen harjoitukseen, jossa harjoitellaan käytännössä jotain ikävää digimaailman ilmiötä. Se voi olla sähköjen katkeaminen tai se voi olla verkkorikollisten hyökkäys, jossa he ovat päässeet organisaation sisälle ja kiristävät rahaa. Se voi olla mustamaalauskampanja. Se voi olla melkein mitä tahansa ja nämä ovat saaneet aivan loistavaa palautetta. Vaikka tässä pääasiallinen kohderyhmä on julkishallinnon organisaatiot, meillä on ollut niin pörssiyrityksiä kuin huoltovarmuuskriittisiä yrityksiä elinkeinoelämän puolelta. Taisto on tarkoitettu kaikille sen takia, että myös meidän julkinen maailmamme pyörii elinkeinoelämän ja yritysten tuottamien digipalvelujen varassa. Joten sen takia mahdollistamme tämän kenelle tahansa. Tuolta DVV .fi /taisto -sivulta löytyy lisää tietoa.

Tom Tuunainen
Erittäin mielenkiintoista. Onko teillä myös jotain muita turvallisen digiympäristön palveluita, jotka haluaisit nostaa esiin tässä?

Rousku Kimmo (DVV)

No, joo niin kuin sanoin, me tuotamme palveluita ensisijaisesti julkiseen hallintoon. Mutta koska maailma on nyt muuttunut niin, että se mitä julkisen hallinnon organisaatio voi hyödyntää, sitä voivat myös yritykset käyttää. Ja taas samalla tavalla, kun me kehitämme julkisen hallinnon henkilöstön digiturvaosaamista, niin monet näistä vinkeistä ja asioista ovat ihan samoja myös vapaa-ajalla. Muutenkin, kun vapaa-aika ja työelämä yhä enemmän nivoutuvat toisiinsa, on hankala enää erotella, että tämä asia koskee minua vain, kun teen töitä. Päinvastoin ne ovat yhä enemmän sidoksissa toisiinsa. Suosittelisin tutustumaan sivustoon digiturvallinenelama.fi, koska sen takaa löytyy meidän kaikki keskeiset henkilöstön osaamisen kehittämiseen liittyvät palvelut.

Olemme nyt luoneet digiturvallinen elämä -mobiilipelin, joka löytyy tuolla nimellä. Yleensä meidän koulutuksiimme liittyvät asiat löytyvät suomen ohella ruotsiksi ja englanniksi. Esimerkiksi tämä peli löytyy englannin kielellä ja tiedän, että sitä on myös pelattu aika eksoottisissa maissa. Sitä on kaksi kautta tällä hetkellä ja siinä seikkaillaan kuvitteellisessa Tyrskylän kunnassa. Siellä sitten tehdään digimaailmassa vastaan tulevia ilmiöitä, asioita ja uhkia ja katsotaan, kuinka hyvin niissä sitten menestyy. Tästä pelistä meillä tulee nyt syksyllä kolmas tuotantokausi, jossa sitten pääseekin seikkailemaan Tyrskylän kunnan tietoturva- ja ehkä myös tietosuojavastaavan roolissa, eli miettimässä, miten eri tilanteissa tulisi toimia. Ja tähän samaan liittyy myös sitten meidän verkkolähetyksemme tai webinaarit, eli meillä on joka kuukausi keskimäärin vähintään yksi puolenpäivän tilaisuus, jossa kerromme ajankohtaisista uhkakuvista henkilöstölle. Nämä ovat myös kansalaisille suunnattuja. Ne uhkakuvat ovat ihan samanlaisia nykyään henkilöstölle organisaatiossa kuin meille kansalaisille. Toisaalta meillä on myös sitten alan asiantuntijoille tarkoitettu Vahti-verkosto.

Vahti-verkosto tarkoittaa yli 500 alan ammattilaisen ja osin johdon edustajan verkostoa, joka sitten jakaantuu käytännössä kuuteen erilaiseen ryhmään. Eli meillä on työryhmiä. Siellä on yksi työryhmä, joka keskittyy riskienhallintaan, toinen, joka keskittyy toiminnan jatkuvuuteen, kolmas työryhmä, joka keskittyy ICT palveluiden turvallisuuteen, neljäs keskittyy tietosuojaan ja viides ryhmä on tarkoitettu alan osaamisen kehittymisestä kiinnostuneille. Tämän lisäksi meillä on valtionhallinnon tietoturvavastaavien, voisi sanoa, suljettu verkosto, eli siihen pääsee vain näiden virastojen vastuuhenkilöt. Erikseen meillä on vielä johtoryhmä, jossa on vajaan neljänkymmenen, pääasiassa julkisen hallinnon organisaation, digitaalisen turvallisuuden ja ylimmän johdon edustajaa keskustelemassa ja yhdessä miettimässä näitä asioita. Nämä ovat meidän keskeisiä asioitamme. Meidän sivultamme DVV.fi/digiturvani löytyy paljon muutakin. Siellä on materiaaleja, meillä on videokoulutuksia ja tietoiskuja saatavilla. Ne löytyvät kaikki sieltä.

Laura Palovuori
Digitaalinen turvallisuus on yhtä tärkeää kuin fyysinen turvallisuus. Ja kun yritykset digitalisoivat palveluitaan, niin mitä pitäisi ensimmäiseksi huomioida?

Rousku Kimmo (DVV)
Lähtisin aina liikkeelle siitä, mikä on yrityksen toiminnalle kriittistä. Jos se on fyysinen maailma, eli jos yrityksellä on toimitiloja, niin sitten siihen liittyvät tekijät ja asiat. Eli riippuu hyvin paljon yrityksen toimialasta ja tehtävistä, tuotannosta, tuotteista ja palveluista. Mutta nimenomaan lähestytään tätä riskienhallinnan näkökulmasta, tunnistetaan ne kriittiset tuotannontekijät, on ne sitten digimaailmaa tai fyysistä maailmaa. Ja siellä vielä priorisoidaan kaikista tärkeimmät asiat, koska emme voi suojella kaikkea. On mahdotonta toteuttaa sellaista ratkaisua, että kaikki asiat olisivat yhtä tärkeitä ja yhtä kriittisiä ja sen takia tässä pitäisi tunnistaa juuri nimenomaan ne, jotka

oikeasti, jos niihin tulee jotain häiriöitä lamauttaa yrityksen toimintaa. Tuo on se ensimmäinen asia, eli riskienhallinta ja sitä kautta palveluiden toiminnan kriittisyyden tunnistaminen. Sitten mietitään niitä keinoja, joilla vältetään näiden uhkien ja tarkemmin tunnistettujen riskien toteutumista. Ja tässä me tarvitsemme välttämättä jatkuvuuden hallintaa, varautumista ja mahdollisesti jonkin näköisiä toipumissuunnitelmia siltä varalta, että jos tai, kuten nykyaikana yhä useammin on pakko sanoa, kun jotain ikävää tapahtuu.

Verkkorikollisuus on kasvanut merkittävästi viimeisten vuosien aikana, se kasvaa, eikä ole nähtävissä, että se millään lailla tulisi laantumaan. No, jotta näiden tietojen turvallisuus, jota yritys käsittelee, on varmasti toteutettu oikein, me tarvitsemme ihan perinteistä tietoturvallisuutta, jolla varmistetaan, että tiedot ovat vain niiden henkilöiden käsiteltävissä, joille on annettu käsittelyoikeudet.

Eli tämä on ehkä näistä turvallisuuteen liittyvistä perusperiaatteista, pilareista, yksi niistä vanhemmista. Tuossa kaksikymmentä vuotta sitten, kun puhuin näistä asioista, oli kyse hyvin pitkälle pelkästä tietoturvasta, puhuttiin virustorjunnasta ja palomuureista. Niitä tarvitaan edelleenkin mutta niiden lisäksi tarvitaan paljon muutakin. Sen rinnalle on noussut viimeisen viiden vuoden aikana todella paljon henkilötietojen käsittelyä, eli tietosuojaa. Itse asiassa EU:n yleinen tietosuoja- asetus täyttää nyt 25. toukokuuta viisi vuotta, eli sitä on sovellettu jo näin kauan. Tietosuojan eräs iso merkitys on ollut myös, että se ei ole pelkästään kehittänyt tätä henkilötietojen turvallista käsittelyä tai vaatimusten mukaista käsittelyä, vaan se on samalla edellyttänyt myös tietoturvallisuuden kehittämistä. Jotta tietosuoja toteutuisi, tietoturvan pitää olla myös ajan tasalla ja oikeastaan kaikki edellä olevat ovat niitä tekijöitä, joilla me myös kansallista kyberturvallisuutta kehitämme. Eli huolehdimme siitä, että digimaailma tai kybermaailma on turvallinen niin, että voimme luottaa siellä oleviin palveluihin ja varmistaa myös niiden toiminta erilaisissa häiriötilanteissa.

Nuo ovat ne osa-alueet, joihin kannattaa kiinnittää huomiota. Eli ei ole olemassa yhtä asiaa vaan tarvitaan hyvin laaja- alaisesti koko kokonaisuuden avaamista ja tarkistamista, olemmehan huolehtineet kaikista asioista

Laura Palovuori
Onko tavallisella kuluttajalla valmiuksia arvioida palvelun luotettavuutta, eli mitä pitää tarkkailla, kun menee vaikka nettikaupan sivuille?

Rousku Kimmo (DVV)
Voisin tästä kertoa hyvän, huonon, opettavan esimerkin siitä, miten itse melkein mokasin tai en edes vielä tiedä mokasinko, toivottavasti en.

Reilu kuukausi sitten olin hankkinut ilmanpuhdistimen, koska keväällä tulee siitepölyä sisälle. Hankin semmoiseen vähän uudempaa tekniikkaa hyödyntävän ilmanpuhdistimen ja sen mukana tuli ilmansuodattimet, joita se käyttää. Ajattelin, että ennakoivasti tilaan lisää näitä ilmansuodattimia tulevia kuukausia ja vuosia varten. Googletin netistä ja löysinkin kauppapaikan, joka tarjosi edullisesti näitä ilmansuodatinpaketteja ja laitoin ne sitten tilaukseen. Sitten sieltä tuli ilmoitus, että kyllä tässä ovat tiedot ja tilaus on lähtenyt liikkeelle, ilmoitamme, kun varastostamme löytyy näitä. Kului jokunen päivä, ei kuulunut mitään. Odotin vielä muutaman päivän ja sitten kysyin, että jokos on löytynyt? Silloin tulikin ilmoitus, että nyt ei vielä löydykään, tässä voi mennä vähän aikaa. Siinä vaiheessa huolestuin, yleensähän tuotteen pitäisi lähteä liikkeelle aika nopeasti.

Tämä kyseinen kauppapaikka oli minulle uusi outlet- tyyppinen kauppa, jolla on kyllä toimintaa, sivujen mukaan, ympäri maailmaa ja se vaikutti hyvin aidolta. Sitten alkoikin netistä löytyä aika

huolestuttavia tarinoita siitä, että kauppa ottaa kyllä tilauksia vastaan ja myös rahat vastaan, tietysti, mutta sitten sieltä tulee ilmoitus, että tätä tuotetta ei löydykään varastosta ja sen saaminen kestää. No, tarinat olivat aika samanlaiset kuin minun, joten aloin vähän huolestua siitä.

Laitoin sitten viestin sinne, että nyt jos sen saa kahteen päivään varmistusta, että tämä tuote lähetetään minulle, peruutan tämän tilauksen, sopiihan näin. Sain ilmoituksen, että kyllä sopii. Kun tuotetta ei tosiaan alkanut tulla, kaupalta tuli ilmoitus, että he peruuttavat tilauksen ja hyvittävät maksuni. En tajunnut siinä vaiheessa, että he hyvittävät sen vain heidän omaan järjestelmäänsä, eli eivät palautakaan rahoja luottokortille, vaan raha on ikään kuin heillä piikissä minulle, jos haluan ostaa jotain muuta. Tässä on kulunut yli 30 päivää, heidän aikarajansa, jonka jälkeen rahat palautetaan. En ole saanut mitään ilmoitusta siitä.

Tänään tulen soittamaan luottokorttiyhtiöön ja sanoa, että nyt olen joutunut tämmöiseen tilanteeseen, joten käynnistäkää siellä sitten perintätoimet, jotta saan rahani takaisin. Normaalisti aina katson etukäteen huolella mistä mitäkin ostan. Kiireessä, kun oli aidolta näyttävä sivusto, en tehnyt perusteellista selvitystä. Todennäköisesti en menetä rahojani vaan saan ne luottokorttiyhtiön kautta takaisin, mutta enpä saa niitä suodattimia.

Tämän olisin välttänyt siten, että olisin vain googlettanut tätä kyseistä yritystä tai sen nettisivua ja hakenut vaikka hakusanalla “kokemuksia”. Usein käytän myös sivustoa scamadviser.com, josta löytyy näiden erilaisten huijaussivustojen paljastamistietoja. Sinne voi laittaa jonkun palvelun tai nettisivun osoitteen niin se kertoo, löytyykö näiltä sivuilta paljon käyttäjien kommentteja kyseisestä palvelusta tai muuta huolestuttavaa. Nyt kun sieltä katsoin tätä käyttämääni palvelua, niin siellähän oli todella paljon, kymmenittäin tai sadoittain, ilmoituksia ja kaikki olivat yleensä saman mallin mukaisia. Tuotetta on mutta kestää vähän aikaa ja sitten aletaan rahoja palauttamaan. Kaikki eivät ole välttämättä rahojaan saaneet takaisin. Eli kysymykseesi, että onko valmiuksia arvioida: Kyllä on, kunhan huolehtii siitä etukäteen ja nimenomaan käyttää näitä hakupalveluita vähän selvittääkseen, millaisia kokemuksia käyttäjillä on. Itse pitäydyn yleensä aina näissä tunnetuissa joko kotimaisissa tai sitten kansainvälisissä isoissa ketjuissa. Pitkästä aikaa kokeilin jotain muuta ja heti kävi näin. Toivottavasti tästä on oppia myös muille

Laura Palovuori
Olen ollut huomaavinani, että digi- ja väestötietovirastolla on meneillään uuden termin käyttöönotto. Kimmo Rousku, kerro mitä on digirohkeus?

Rousku Kimmo (DVV)
Digirohkeuden oikeastaan voi määritellä monella lailla ja jokaisella on siihen vähän erilaisia näkökulmia. Mielestäni digirohkeus on sitä, että sen sijaan että pelkää, mitä digimaailmaa tarjoaa, vaikka on keskusteltukin aika ikävistä asioista, niin siitä huolimatta toteaa, että totta kai kaikkiin asioihin liittyy aina ikäviä asioita. Emmehän me koskaan ottaisi mitään uusia asioita käyttöön, jos koko ajan pelkäisimme. Digirohkeus minulle on sitä, että kokeilen aktiivisesti, toki varovasti ja erilaiset uhat tunnistaen, näitä digimaailman palveluita ja ilmiöitä ja hyödynnän niitä sen jälkeen, kun olen uuden palvelun ottanut käyttöön. Tarkoittaa juuri sitä, että kun meillä on koko ajan tulossa uusia digilaitteita ja uudenlaisia palveluita kiihtyvällä vauhdilla, nyt varsinkin tekoälyn aikakausi tulee vauhdittamaan uusien palveluiden markkinoille tuloa valtavasti, niin kokeilen näitä vapaa- ajallani käyttäen vapaa- aikaani liittyviä tunnuksia. Jos totean, että joku palvelu on hyvä ja koen sen turvalliseksi, niin pyrin ottamaan sen aktiivisesti käyttöön. Tässä tietysti on se huono puoli, että jos tulee vaikkapa digihuijatuksi niin se varmasti aiheuttaa itsetuntoon kolahduksen ja vähän pelkää sen jälkeen.

Meillä oli tuossa toissa päivänä yksi näistä meidän kuukausiverkkolähetyksistämme, siellä keskusteltiin romanssihuijauksista ja romanssipetoksista. Ne ovat ehkä verkkorikollisuuden ikävin puoli, koska siinä henkilö ei pelkästään menetä rahaa vaan myös monesti luottamuksen muihin ihmisiin. Mutta kannustan kuitenkin miettimään niitä positiivisia asioita, jota digimaailmaa meille mahdollistaa ja tulee jatkossa mahdollistamaan entistä enemmän. Mielestäni digirohkeus on juuri nimenomaan yhdistelmä teknologiaa, eli laitteita ja palveluita ja toisaalta myös meidän ihmisten toimintaa. Myös ympäristö, jossa toimimme kotona ja vapaa- ajalla, kavereiden ja perheen kesken sekä työpaikalla on osa tätä yhdistelmää. Kun nämä kaikki yhdistetään, saamme tätä digirohkeutta.

Tom Tuunainen
Mainitsit tuossa vastauksessasi äsken tekoälyn. Centria SecuLab on siis ammattikorkeakoulun tietoturvalaboratorio ja olemme paljon tekemisissä sekä asiantuntijoiden ja yritysten että opiskelijoiden kanssa. Mitä lisäneuvoja antaisit näille kohderyhmille tekoälyn käyttöön liittyen?

Rousku Kimmo (DVV)
Ensinnäkin kannattaa opiskella, miten tekoäly periaatteessa ideana toimii.
Jos ei ollenkaan tiedä, miten tekoäly toimii, ajattelee, että se toimii vähän kuten ihmisen aivot. Tosin siinä on se teko siinä välissä. Käytännössähän uusi, nopeasti edennyt ChatGPT ja siihen pohjautuva laaja kielimalli tarkoittaa sanojen arviointia ja sen ennustamista, mitä pitäisi seuraavaksi tähän kysymykseen vastata. Tämä pohjautuu huikeaan määrään analysoitua tietoa. Voisi sanoa, että se on kuin älylaitteissa käytettävä ennakoiva tekstinsyöttöjärjestelmä. Joten nyt voisi sitten kevennyksenä sanoa, että se on eräänlainen vähän kehittyneempi versio tekstinsyöttöjärjestelmästä. Se ei pelkästään tunnista sitä sillä hetkellä käytettävää sanaa, vaan virkkeitä. Se siis ennustaakin vähän pitemmälle, mitä nyt aiot tai mitä haluat saada vastauksena tähän kysymykseesi. Eli sen ymmärtäminen, mistä se lähtee liikkeelle ja miten se toimii, on tärkeää, koska sen jälkeen ymmärtää paremmin miksi se tekee virheitä.

Olen aika aktiivinen Twitterin käyttäjä ja alkuviikolla laitoinkin tämmöisen mielenkiintoisen twiitin liikkeelle, jossa kyselin yhdeltä testaamaltani OpenAI- pohjaiselta tekoälypalvelulta, onko Kimmo Rousku syyllistynyt minkälaisiin rikoksiin?

Tietysti etukäteen mietin, että no saa nähdä mitä sieltä tulee. Sieltähän tuli todella pitkät syytelistat siitä, minkälainen verkkorikollinen, kiristäjä ja tietovuotaja olen ja kuinka olen parhaillaan odottamassa tuomiota näistä rikoksistani. Nyt jos joku ulkopuolinen henkilö, joka ei tunne minua, tekisi tämän saman kyselyn, niin hän kuvittelisi, että ahaa onpas tuossa todella mielenkiintoinen henkilö. Hän puhuu positiivisesti näistä digiturva- asioista, mutta sitten siinä aivan kuin oikealla kädellään näköjään toimii aktiivisena verkkorikollisena.

Tärkeä on ymmärtää, että nämä tekevät virheitä ja voivat tehdä hyvinkin vakavia virheitä ja siksi, etenkin, jos kyselee, keskustelee ja hakee sellaista tietoa, josta ei ole itsellä sataprosenttista varmuutta, niin medialukutaito on tärkeä. Vaikka yleensä ymmärtää, mikä tieto on varmasti oikein tai oikean olosta, niin tekoälyn alkuaikakaudella pitää olla sen suhteen entistä varovaisempi. Tämä on hyvin tärkeä oppi, jota kannattaa ehdottomasti harjoitella. Jokaisessa organisaatiossa kannattaisi nyt luoda periaatteet tämän testaamiseen.

Tässä on yksi esimerkki meidän vahtitoiminnastamme. Kun meillä on kesäkuun puolivälissä viidestoista kuudetta, tämmöinen kokopäivän verkko- ja fyysinen seminaari, jossa meidän iltapäivämme aiheena tulee olemaan juuri tekoäly, tulemme julkaisemaan siellä huoneentaulun siitä, miten voi lähteä turvallisesti näitä tekoälypalveluita hyödyntämään ja testaamaan. Eli se on tavallaan

loppukäyttäjille suunnattu, aika yksinkertainen huoneentaulu perusteluineen, mitä asioita ainakin kannattaa miettiä ja muistaa. Ehkä yksi perusperiaate on, että mitään organisaation tai yritykseen liittyvää salassa pidettävää tietoa tai mitään henkilötietoja ei tule tämäntyyppiseen palvelun viedä, ellei sitten jollain lailla ole varmistettu, että kyseessä on sellainen versio, joka ei käytä tietoja esimerkiksi palvelun opettamiseen.

Kerron erään, voisi ehkä sanoa ääriesimerkin. Kun kesällä opiskelen tätä lisää, aion kokeilla kuvitteellisen ihmissuvun tekemistä, jossa on henkilöitä ja heillä on henkilötunnus, osoite ja muita tietoja. Tällä testaan, saanko tämän lisättyä johonkin tunnettuun tekoälypalveluun niin, että sen jälkeen joku ulkopuolinen pystyy hänkin näitä tietoja sieltä kaivamaan. Eli vuotavatko tekoälypalvelut? Juuri tämän takia on nimenomaan tärkeätä käyttää tällaista testidataa, jos haluaa tuollaisia asioita testata ja muutenkin olla tosiaan huolellinen, millaisia kysymyksiä ja mitä asioita siitä palvelusta haluaa hyödyntää.

Tuohon vielä vinkkinä, että kannattaa, digirohkeuteen liittyen, tämmöistä tekoälyn rohkeutta harrastaa. Meillä tulee olemaan varmasti paljon keskustelua siitä, pitäisikö näitä asioita kieltää. Tämä on vähän sama juttu kuin aina, kun tulee uutta teknologiaa, alussa on aika paljonkin vastustusta, tämä on pelottava ja tämä on huolestuttavaa. On aina helpompi kieltää kuin lähteä hyödyntämään. Meillä oli myös tässä meidän eräässä verkko- ohjelmassa parin meidän kyberprofessorimme kanssa keskustelua tästä tekoälystä. Kysyin, että miten he näkevät tämän opetuskäytössä, niin kyllähän tämä on työkalu, vähän sama asia kuin silloin, kun taskulaskin tuli joskus 1970- luvulla. Olisiko silloin pitänyt sanoa, että taskulaskinta ei saa koskaan käyttää, se on pahasta? On kyse nimenomaan siitä, että otetaan uutta teknologiaa käyttöön, mutta sitä pitää oppia hyödyntämään oikealla tavalla. Tässä tapauksessa juuri tekoälyä, koska siitä tulee meille yksi työväline, työkalu, joka auttaa meitä tekemään tehokkaammin entistä kehittyneempiä asioita. Sen avulla varmasti taas luodaan uudenlaisia innovaatioita ja asioita, jotka tällä perinteisellä tekoälyttömällä aikakaudella olisi ollut joko kokonaan mahdotonta tai hyvin, hyvin haasteellista kehittää. Nämä ovat nyt ehkä ensimmäisiä vinkkejä, mitkä tulevat tässä mieleen.

Laura Palovuori
Mitkä ovat mielestäsi tällä hetkellä suurimmat kyberturvallisuusalan uhat ja liittyykö esimerkiksi tekoäly myös näihin?

Rousku Kimmo (DVV)
Jälleen erinomaisen hyvä kysymys. Itse olen oikeastaan viimeisen parin vuoden aikana keskittynyt aika pitkälle siihen, että meillä julkisessa hallinnossa, niin kuin varmasti myös yrityksissä ja kansalaisten ja kotikäyttäjien joukossa, verkkorikollisuus on se numero ykkönen, joka näkyy joka paikassa ja tuntuu koko ajan kasvavan. Me luemme mediasta siitä, miten nykyään kaikkien, tunnettujen viranomaisten, pankkien, posti- ja kuriiripalveluiden ja muiden tunnettujen yritysten nimissä lähetetään viestejä, joissa yritetään saada henkilö luovuttamaan jotain sellaista tietoa, josta tämä verkkorikollinen saa taloudellista hyötyä, kuten esimerkiksi pääsyn pankkiin, luottokorttitietoja, pankkikorttitietoja, pääsyjä käyttäjän sähköpostijärjestelmään, josta sitten päästään lähettämään viestejä tämän henkilön nimissä muille käyttäjille ja siellä yrittämään pääsyä heidän sähköpostiin tai muihin järjestelmiin. Tämä on koko ajan kehittynyt ja laajentunut ja tulee uudenlaisia hyökkäyksiä.

Verkkorikollisuus on omasta näkökulmastani se ikävin ilmiö digitalisaation muun kehityksen rinnalla. Syy tähän on, että kun teknologia tarjoaa uusia mahdollisuuksia, niin verkkorikollisilla on matalin kynnys ja mahdollisuus niitä hyödyntää. Heillä ei ole lainsäädäntöä tai muita velvoitteita ja vaatimuksia siellä millä mitäkin pitää toteuttaa. He voivat tuottaa omaa rikollista toimintaansa ihan

sillä tavalla, mitä he itse haluavat, joka on yleensä, totta kai, hyvin kevyt ja tehokas rakenne. Sitä voidaan hyvin ketterästi tarvittaessa muuttaa ja soveltaa. Eli me häviämme verkkorikollisille, juuri siinä, että heidän ei tarvitse noudattaa lakeja. Heillä ei ole mitään pelisääntöjä.

No meidän hyvisten puolella on tietysti se, että meitä on aika paljon enemmän ja toisaalta emme keskity pelkästään ikävään puoleen, vaan me nimenomaan tuotamme paljon hyvää. Eli verkkorikolliset hakevat vain tuottoa ja taloudellista hyötyä itselleen. He keskittyvät siihen, me hyvikset taas sitten tuotamme paljon, oikeastaan vain, hyvää, eli miten näitä digimaailman palveluita ja tietoja oikealla tavalla hyödynnetään.

Verkkorikolliset ei ole ainoa ongelma. Toinen asia, jonka nostan aina tällaisissa kysymyksissä esille, on erilaiset valtiolliset toimijat. Verkkorikolliset hakevat nopeaa helppoa rahaa ja tämä onkin syy, miksi kehotan aina vain pikkuisen parantamaan, ei tarvitse kovin paljon parantaa sitä omaa turvallisuuttaan vaan pikkuisenkin riittää. Koska jos on vähän parannettu niin se on kuitenkin ehkä enemmän kuin jollain toisella. Kun verkkorikolliset hakevat niitä pikavoittoja ja he törmäävät organisaatioon, jossa huomaavat, että täällä perustemput eivät tunnukaan heti toimivan. Jos he lähettävät sähköpostiviestikampanjan ja organisaatiossa ei ole oikeastaan juurikaan reagoida siihen millään lailla, niin he toteavat, että okei, tuolla on semmoinen organisaatio ja sellaisia käyttäjiä, emme ehkä pääsekään sinne. Mennään jonnekin muualle. Tämän takia kannattaa pikkuhiljaa tätä tasoa pyrkiä aina nostamaan, eli ohjataan nämä verkkorikolliset muualle. Sama ei valitettavasti päde näihin valtiollisiin toimijoihin. Heidän tehtävänään on päästä sellaiseen tietoon käsiksi, johon kyseisellä valtiolla on suuri intressi. Heillä on yleensä aikaa. Heillä ei ole kiire. He eivät hae sitä helpointa kohdetta, vaan he hakevat tietoa, jota he oikeasti tarvitsevat. Heillä on siihen aikaa, heillä on siihen resursseja eli heillä on ammattilaisia ja työkaluja. Sellaisia, joita esimerkiksi tavallisella verkkorikollisella ei ole käytettävissä, heillä on siis kaikki nämä edut puolellaan.

Ja tämän takia sanonkin aina, että ei ole olemassa sata prosenttista turvallisuutta. Kaikki, mitä ihminen, tai tulevaisuudessa tekoäly, on laatinut ja kehittänyt, kaikki on murrettavissa. Verkkorikollisia vastaan me pystymme suojautumaan paremmin, mutta valtiollisia toimijoita, joilla on käytännössä äärettömät resurssit, vastaan suojautuminen on huomattavasti hankalampaa, osin mahdotonta. Sen takia ehkä se tärkein asia oikeastaan näissä molemmissa onkin se, että yhä enemmän organisaatioiden pitäisi kehittää kykyä tunnistaa, mitä heidän verkossansa ja palvelussaan tapahtuu. Onko sinne tullut, joku ulkopuolinen toimija, joka on saattanut viettää siellä jo jonkin verran aikaa? Esimerkiksi valtiolliset toimijat saattavat olla pitkiäkin aikoja piilossa siellä. Kyberturvallisuuskeskuksen hiljattaisessa kuukausi- ja taisi olla myös viikkoraportissa, kerrottiin yli 20 vuotta kestäneestä valtiollisesta hyökkäyskampanjasta, jossa kyseinen toimija on voinut viettää vuosia, jopa lähestulkoon vuosikymmeniä jonkun organisaation verkossa lymyämällä siellä ja keräämällä tietoa. Tuo on ehkä tähän mennessä julkisuuteen tulleista esimerkistä ikäviin.

Eli nämä ovat ne kaksi yleisintä: verkkorikolliset ja valtiolliset toimijat. Toki sitten on välissä, harmaalla alueella, erilaisia aktivisteja tai haktivisteja, jotka tekevät ikäviä temppuja ja ehkä haluavat vaikuttaa johonkin asiaan. Joissain asioissa toiminta saattaa olla osin laitonta. Mutta näiden määrä on jo merkittävästi pienempi kuin näiden kahden edelliseen. Nämä ovat keskeiset suurimmat kyberturvallisuusalan uhat ja menetelmät. Totta kai, kaikkia kiinnostaa nyt Venäjän hyökkäys Suomeen digitaalisessa maailmassa. Se on tapahtunut pro venäjämielisten verkkorikollisorganisaatioiden tai heille läheisten organisaatioiden kautta lähinnä palvelunestohyökkäyksinä. Tämä on siinä mielessä ollut hyvä esimerkki siitä, että siellä ei ole oikeastaan juuri muuhun tällä hetkellä kyetty tai haluttu. Esimerkiksi Ukrainaan on kohdistunut huikeasti enemmän erilaisia, huomattavan paljon vakavampia hyökkäyksiä kuin Suomeen ja muihin

länsimaihin. Tämmöinen palvelunestohyökkäys on vähän sama kuin, että joku menee kirjoittamaan graffitin jonnekin, vaikka sillan alla olevaan betoniin. Se on siellä vähän aikaa, sitten se pyyhitään pois. Palvelunestohyökkäykset ovat vähän samanlainen mielenosoitus digitaalisessa maailmassa. Ne voivat vähäksi aikaa pysäyttää palvelun, mutta mitään tietoa ei tyypillisesti häviä ja hetken kuluttua palvelu saadaan pystyyn.

Eli tässä ehkä jonkinlainen snapshot siitä, kuka ja ketkä ja millä keinoilla pyritään nyt tähän meidän digimaailmamme vaikuttamaan.

Laura Palovuori
Olemme keskustelleet siitä, miten tavalliset netin käyttäjät voivat suojautua tietoturvauhilta. Mutta jos mennään toiseen päähän, niin miten kyberrikollisuutta parhaiten ehkäistäisiin?

Rousku Kimmo (DVV)
Kunpa olisikin tähän joku semmoinen kaikenkattava, yksittäinen vastaus.

Meidän viimeisimmissä keskusteluissamme, mitä tuolla on näistä asioista juteltu, niin mielestäni yksi erittäin hyvä havainto oli se, että verkkorikollisuuden toteuttaminen on näille rikollisille joko kokonaan ilmaista tai erittäin halpaa. Eli se, että lähetetään miljoona sähköpostiviestiä, ei oikeastaan heille maksa juuri mitään. Eli jotenkin pitäisi saada verkkorikollisuuden toteuttamisen kalliimmaksi heille.

No sitten toinen, ehkä paljon pienempi kokonaisuus, mutta itseäni kovasti huolestuttava, on nuoret ja verkkorikollisuus. Keskusrikospoliisissa on käynnissä Cyber Crime Exit-hanke, monivuotinen kansainvälinen hanke, jossa pyritään nyt nimenomaan nuorille kertomaan verkkorikollisuuteen liittyvistä asioista. Eräässä tilaisuudessa, jossa kuultiin lisätietoja esimerkiksi siitä minkälaista verkkorikollisuutta nuorten osalta Suomessa on havaittu, ehkä huolestuttavin kuulemani tieto oli, että nuorin poliisin tietoon tullut henkilö, joka on tehnyt jotain laitonta, on ollut 8- vuotias.
Ja kun kaaviossa esiteltiin ikähaitari, niin siellä oli kymmeniä henkilöitä ikäjanalla kymmenestä neljääntoista vuoteen. On tietysti huolestuttavaa, että yhä nuoremmat syyllistyvät tämänkaltaisiin verkkorikoksiin, osa varmasti tietämättään, mutta varmasti osa tietää tai ainakin epäilee. Tämän takia nimenomaan nuorille tulisi tietysti suunnata ja kertoa näistä asioista. Oikeastaan kaikelle kansalle. Nimenomaan tätä rikollisuutta voidaan pienentää osaamistamme kehittämällä.
Voisi sanoa, että aikaisemmin ajateltiin, että meillä on tiettyjä kohderyhmiä iän, osaamiseen tai muun roolin näkökulmasta, jotka saattaisivat kiinnostaa jotain tiettyä verkkorikollisryhmittymää tai tyyppiä. Käytännössä nykyään voisi sanoa, että verkkorikollisuus koskee kaikkia, hyvin nuorista ikäihmisiin. Tämä on kaiken kattavaa, jolloin meidän myös täytyy kaikille näistä asioista kertoa. Mutta tapa, miten me kerromme pitääkin sovittaa kohderyhmään. Esimerkiksi nuorille toimii muun muassa podcastit ja sarjakuvat ja taas vastaavasti, meidän tutkimuksemme mukaan, mitä iäkkäämpi henkilö on kyseessä, sitä vähemmän tämän tyyppiset mallit toimivat. He haluavat esimerkiksi hyvin selkeitä tarkistuslistoja, miten pitää toimia.

Aina välillä kysytään myös, pitäisikö näiden rikosten tuomioita jotenkin koventaa? No siitä on aika monenlaisia mielipiteitä. Itse pyrin siihen, että saataisiin muilla keinoilla rikoksia ennaltaehkäisyä niin, että näitä rikollisia ei tulisi meille. Toisaalta rikollisuus on hyvinkin kansainvälistä.

Ja ehkä vielä yksi heitto tähän kohtaan liittyen on, että etenkin lunnashaittaohjelmien tai kiristämisen ollessa kyseessä (esimerkiksi uhkaus, että julkaisemme tietoa, voi olla kriittistäkin tietoa, teidän asiakkaistanne tai teidän henkilöstöstänne, kuten esimerkiksi Vastaamon tapauksessa), niin pitäisikö jotenkin tätä virtuaalivaluutan hyödyntämiseen liittyviä asioita miettiä uudelleen.

Yleensähän virtuaalivaluutta on toiminut näissä monessakin verkkorikollisuuden mallissa keskeisenä tapana kerätä verkkorikollisille rahaa.

Ehkä panostaisin ennen kaikkea siihen, että mitä paremmin ja enemmän me Suomessa keskustelemme ja kerromme näistä erilaisista tavoista, miten meitä vastaan hyökätään, sen parempi. Ihan siis perhepiirissä. Minun vahva vinkkini on, että aina kun saatte jonkun uuden tyyppisen digihuijausviestin, puhelinsoiton, tekstiviestin tai WhatsAppiin tulee jotain tai teidän nettisivuillenne ponnahtaa jokin huolestuttava ilmoitus, kertokaa niistä. Silloin muutkin tietävät eikä kukaan jää arvelemaan, miksiköhän minä sain tämmöisen, onkohan kukaan muu saanut. Itse olen myös kertonut, niistä kerroista, kun olen tullut huijatuksi. Tai kuten tässä aikaisemmin, kun kerroin esimerkin, jossa todennäköisesti en ole menettämässä rahaa, mutta ainakin läheltä piti- tapaus oli kyseessä. Mitä enemmän me näistä kerromme sitä enemmän osaamme varautua. Näin parannamme kansallista resilienssiämme sietää näitä asioita ja ilmiöitä. Ei ole mikään häpeä, että tulee digihuijatuksi. Minä olen tullut ja minulla on paljon kollegoita, jotka ovat tulleet huijatuiksi. Kuka tahansa voi tulla huijatuksi eli samalla tavalla kuin ei ole olemassa sataprosenttista turvallisuutta niin ei ole olemassa myöskään sataprosenttista henkilökohtaista suojautumista. Tässä nyt ehkä keskeisiä keinoja, joilla tätä suojautumista voisi parantaa.

Tom Tuunainen
Miten Suomi näyttäytyy digimaailmassa muihin valtioihin nähden?

Rousku Kimmo (DVV)
Positiivisesti siinä mielessä, että jos katsellaan näitä kansainvälisiä erilaisia tutkimuksia ja raportteja, niin Suomi on niissä yleensä kärkipäässä. Eli olemme yksi maailman digitalisoiduimpia eniten teknologiaa hyödyntäviä valtioita ja tämän taustalla on tietysti se, että meillä on Nokia ja meillä on monia muita teknologiatoimijoita ja meillä on loistavaa innovaatiokykyä, olemme tuottaneet ja kehittäneet erilaisia laitteita ja palveluita todella paljon. Tällä on pitkä historia, kymmeniä vuosia. Toisaalta varautumisen näkökulmasta olemme varautuneet erilaisiin uhkiin. Käytännössä varmasti toisen maailmansodan jälkeen olemme varautuneet ja kehittäneet näitä asioita. Se on yksi syy siihen, että pärjäämme näin hyvin.

Toisaalta kysymykseen olemmeko Suomessa helpommin digihuijattavia kuin muut kansalaiset olemme varmaan saamassa tutkimustietoa vielä tämän vuoden aikana. Minulla on jotenkin sellainen tunne, että olemme Suomessa vähän turhan sinisilmäisiä. Uskomme edelleenkin siihen, että tuo on todella hyvä tarjous tai tuo palvelu vaikuttaa aika luotettavalta, kun meidän pitäisi ehkä enemmän miettiä sitä, että jos jokin on liian hyvä ollakseen totta, tai nettipalvelussa, jos jokin on liian halpaa ollakseen totta, meidän pitäisi olla kriittisempiä ja nimenomaan näissä tilanteissa kysyä toista mielipidettä. Tämmöinen kuuluisa kilauta kaverille WhatsAppilla tyyppinen malli, jossa vähän enemmän varmistettaisiin näitä asioita.

Toinen on myös se, että kyllähän me aika helposti, koska käytämme paljon digiä, monesti ensin klikkaamme jotakin ja vasta sitten jälkikäteen mietitään, mitäköhän tästä nyt en oikein seuraa. Pitäisi käyttää mallia, mieti ensin ennen kuin klikkaat. Eli tämäkin on eräänlaista henkilökohtaista riskienhallintaa tai uhkien tunnistamista. Menemme monesti digi edellä kovaa vauhtia eteenpäin, miettimättä niitä seurauksia. En tiedä, veikkaan, että monessa muussa maassa on samoja ilmiöitä, mutta jotenkin tuntuu, että me Suomessa tosiaan olemme ehkä liian hanakoita kokeilemaan, ilman varautumista, että mitäköhän tästä voi seurata ja sitten siitä voi seurata jotain ikävää.

Mutta yhteenvetona voisi sanoa, että tosiaan olemme menestyneet tutkimuksissa hyvin. Se myös näkyy käytännössä, hyödynnämme digitaalisia palveluita ja laitteita valtavasti, pääosin myös

turvallisesti. Siinä mielessä, vaikka näitä ikäviä uutisia mediasta usein joutuu lukemaan ja jatkossa varmaan entistä useammin, valitettavasti aika harvoin kirjoitetaan siitä, kuinka paljon hyötyä näistä asioista meille on ollut ja kuinka paljon pystymme tekemään palveluiden avulla näitä hyviä asioita. Tätä asiaa pitäisi enemmän mediassakin tuoda esille, kuinka paljon ja miten me hyödymme näistä digipalveluista ja laitteista. Juuri se positiivinen näkökulma, mutta kun se ei välttämättä kiinnosta niin paljon niitä lukijoita, ellei niissä ole sitten hyviä esimerkkejä, joita jokainen voisi omaksua. Tämä onkin ehkä se suuntaus, jota meidän pitäisi digin hyödyntämisessä enemmän tuoda esille, miten tätä käytetään hyödyksi ja veikkaan että nämä uudet tekoälypalvelut tulee toimimaan tässä oivallisena esimerkkinä.

Laura Palovuori
Kiitos näistä mielenkiintoisista näkemyksistä. Kimmo Rousku, onko sinulla vielä jokin tulevaisuusvisio, jonka voisit tässä esittää lopuksi.?

Rousku Kimmo (DVV)
Tulevaisuuteen katsominen ja ennustaminen on aina hyvin haasteellista. Toisaalta olen tutkinut ja elänyt pitkään tätä digimaailmaa. Käytännössä ensimmäinen tietokoneeni, Commodore 64 taisi olla tuolla vuonna 1983 tai 1984 eli tässä voi katsoa 40 vuotta taaksepäin. Minun visioni on, että nyt jos mietimme 40 vuotta ja mitä kaikkea tänä aikana on tapahtunut ja jos mietimme kokonaisuutena seuraavat 40 vuotta, kukaan ei pysty sitä ennustamaan, mutta veikkaisin että tämä sama iso muutos tapahtuu nyt seuraavan 10 vuoden ajan. Eli neljänkymmenen vuoden oppiminen tuleekin tapahtumaan seuraavan 10 vuoden aikana.

Ja voi olla, että riippuen siitä, mitä tekoälyaikakausi tuo mukanaan ja toisaalta myös kvanttitietokoneet, jotka aikanaan voivat olla jopa vielä isompi myllerrys kuin tämä, voi olla, että kaikki tapahtuu jopa nopeammin.

Toisaalta aina on puhuttu näistä roboteista, että robotit tulevat ja meille tulee kotirobotteja. Olen aina vähän miettinyt, että minulla on toki siivousrobotti kotona ja se on itse asiassa yllättävänkin hyvä, kiitos hänelle, että kun yhdistämme nämä tekoälyrobotit, saamme nyt tekoälystä näihin kotona toimiviin robotteihin älykkyyttä. Eli juuri keskustelukykyä. Voisi sanoa, että tämä nyt käynnissä olevan tekoälymyllerryksen tärkein ominaisuus on, että nimenomaan tämmöinen keskusteleva tekoäly voidaan käyttää ja upottaa ties minne, vaikkapa juuri näihin kodinkoneisiin ja kodin laitteisiin. Näen jo itseni keskustelemassa kotona olevien kodinkoneiden kanssa. Ei välttämättä mene viittäkään vuotta, kun jo voin kertoa toiveitani kahvinkeittimelle, millaista kahvia haluan tänään ja antaa vinkin tuolle siivousrobotille, että käytkö pyyhkimässä tuolta, kun tuonne lattialle putosi jotakin. Menemme kyllä yhä automatisoidumpaa maailmaa kohden ja olen aina ihmetellyt, miksi meillä on edelleen näppäimistö käytössä. Miksi meillä on hiiri tai tämmöinen track paddyä vastaava laite, jota käytämme? Tulemme yhä enemmän siirtymään siihen, että kommunikoimme muilla tavoilla meille tärkeiden laitteiden kanssa. Mutta kyllä näppäimistö varmaan vielä kohtalaisen pitkään säilyy, mutta kuten sanoin, kymmenestä vuodesta on mahdoton sanoa muuta kuin, että tämä on todella iso muutos ja siihen meidän kannattaa varautua ja ehkä juuri digirohkeus on asia, jota kannattaa seuraavan kymmenen vuoden osalta sitten soveltaa.

Laura Palovuori
Centria SecuLabin tietoturva podcastin haastateltavana oli Kimmo Rousku digi- ja väestötietovirastosta.

Rousku Kimmo (DVV)
Kiitos tästä mahdollisuudesta kertoa näistä aina mielenkiintoisista ilmiöistä ja asioista

Laura Palovuori
Kiitos.