KYMENLAAKSOLAISTEN YRITYSTEN KYBER- JA TIETO-TURVATASON NOSTAMINEN PARANTAA KOKO ALUEEN KYBERVALMIUKSIA

Jenna Ruuska

Yhä useampi asia siirtyy verkkoon, kun maailma digitalisoituu. Samalla on tärkeää muistaa pitää huolta turvallisuudesta. Turvallisuus muodostuu monista eri tekijöistä, ja laitteiden ja palveluiden käyttäjällä on monia keinoja vaikuttaa siihen. Tutkimusten mukaan suurin osa kyberhyökkäyksistä mahdollistuu käyttäjän tekemien virheiden vuoksi. Näistä virheistä ei koskaan tulla täysin pääsemään eroon, mutta kouluttamalla ihmisiä virheiden määrää voidaan pienentää. Ymmärrys turvallisesta laitteiden käytöstä ja verkossa työskentelystä korostuu etenkin silloin, kun kyseessä on yrittäjä tai työntekijä, joka käsittelee omien tietojen lisäksi yrityksen ja sen asiakkaiden tietoja. Juuri tästä syystä Kyberturvan abc yrittäjille ja KyberReact Kymi22 – Last Call -hankkeissa pyrittiin parantamaan kymenlaaksolaisten yritysten kyberturvan tilaa ja kyberresilienssiä muuttuvassa maailmassa.

Ruuska, J. 2024. Kymenlaaksolaisten yritysten kyber- ja tietoturvatason nostaminen parantaa koko alueen kybervalmiuksia. Teoksessa Rajahonka, M. & Haapaniemi, H. (toim.) Luovia menetelmiä ja älykkäitä ratkaisuja. Digitaalisen talouden vahvuusalajulkaisu 2023. Mikkeli: Kaakkois-Suomen ammattikorkeakoulu, 178–186. https://urn.fi/URN:ISBN:978-952-344-568-0

Kuva 1. Tutkimusten mukaan suurin osa kyberhyökkäyksistä mahdollistuu käyttäjän tekemien virheiden vuoksi. (Kuva: Gettyimages)

Viime vuodet ovat tuoneet mukanaan monia muutoksia

Vuosi 2020 toi mukanaan koronapandemian, joka vaikutti merkittävästi esimerkiksi siihen, kuinka paljon yrityksissä tehdään etätyötä. Yritysten valmiudet siirtyä etätöihin vaihtelivat suuresti. Koska tilanne kehittyi verrattain nopeasti, ei kaikilla ollut mahdollisuuksia tarpeeksi kattavaan turvallisuuden huomioimiseen.

Pandemia ei vienyt verkkoon pelkästään työntekijöitä. Myös monet palvelut ja esimerkiksi opetus siirtyivät verkon kautta toteutettaviksi. Vaikka osittain on palattu pandemiaa edeltäviin toimintatapoihin, pandemian vaikutukset näkyvät yhä esimerkiksi etätyön tekijöiden määrässä.

Samana vuonna 2020 uutisoitiin Vastaamoon kohdistuneesta tietomurrosta. Tapaus oli merkittävä. Poliisin julkaisemien tietojen mukaan noin 33 000 henkilöä joutui tapauksen uhriksi. Tapaus herätteli tärkeää keskustelua yritysten kyber- ja tietoturvan tilasta.

Keväällä 2022 alkanut Venäjän hyökkäyssota Ukrainassa ja sitä seurannut Suomen Nato-prosessi herättelivät puolestaan keskustelua häiriönsietokyvystä ja valtiollisesta vaikuttamisesta. Nato-prosessin vaikutukset näkyivät verkossa. Kyberturvallisuuskeskuksen mukaan esimer-

kiksi suomalaisiin yrityksiin kohdistuneiden kiristyshaittaohjelmien määrä nelinkertaistui liittymisprosessin alkamisen jälkeen. Myös palvelunestohyökkäysten määrä nousi selkeästi. (Martin 2023.)

Tekoäly nousi erityisen suosituksi puheenaiheeksi loppuvuodesta 2022, kun OpenAI:n ChatGPT julkaistiin yleisesti kokeiltavaksi. Samaan aikaan kun keskustellaan tekoälyn mahdollisuuksista, ovat ymmärrettävästi esiin nousseet tekoälyn tuomat uhkat ja sen käytöstä nousevat eettiset kysymykset.

Tekoälyssä on kyberturvallisuuden kannalta sekä hyvät että huonot puolet. Tekoälyä voidaan käyttää entistä tehokkaampien hyökkäysten tekemiseen. Se nopeuttaa esimerkiksi tiedonkeruuta, mikä auttaa tekemään kohdennetumpia hyökkäyksiä. Se voi myös auttaa laajentamaan hyökkäyksiä suuremmille määrille kohteita automatisoinnin avulla, tai sen avulla voidaan luoda aidolta vaikuttavaa ääntä ja kuvaa.

Samaan aikaan tekoäly kuitenkin auttaa havaitsemaan haavoittuvuuksia ja hyökkäyksiä sekä puolustautumaan niiltä. Kehitys on jatkuvaa ja ammattilaiset pyrkivät minimoimaan sen tuomia uhkia. Myös tekoälyyn liittyvää sääntelyä pyritään kehittämään.

Kyberturvallisuuskeskus ja suojelupoliisi pitivät keväällä 2023 tiedotustilaisuuden, jossa ne kertoivat kyberturvallisuuden uhkatason olevan Suomessa edelleen kohonnut. Valtionhallintoon ja huoltovarmuuskriittisiin toimijoihin kohdistettuja hyökkäyksiä oli enemmän kuin aiemmin ja hyökkäykset olivat aiempaa kohdennetumpia. Myös verkossa tapahtuvan yhteiskunnallisen vaikuttamisen määrä oli selvästi nousussa. (Traficom 2023.)

Suuren, yhteiskunnan toimintaa lamauttavan hyökkäyksen riskin kerrottiin kuitenkin olevan pieni. Tähän vaikuttaa eri toimijoiden tekemä yhteistyö ja varautuminen. Varautumisen ja suojautumisen tarve korostuu etenkin viranomaisisten ja huoltovarmuuskriittisten toimijoiden osalta, mutta se on tärkeää myös muille.

”Miksi kukaan haluaisi ottaa minun pienen yritykseni kohteeksi?”

Helposti ajatellaan, ettei kyberturvallisuuden huomioiminen ole niin suuressa roolissa, kun yritys on pieni. Kukapa haluaisi pienen paikallisen yrityksen kimppuun hyökätä, kun verkosta löytyy houkuttelevampiakin kohteita?

Kyber- ja tietoturvallisuuteen pitää kuitenkin kiinnittää huomiota kaikenkokoisissa yrityksissä. Sen lisäksi että lait ja säädökset tuovat mukanaan velvollisuuksia, voi näiden asioiden laiminlyöminen johtaa esimerkiksi mainehaittoihin, taloudellisiin tappioihin tai jopa yritystoiminnan lakkaamiseen.

Se että yritys on pieni eikä se ole suuren yleisön tietoisuudessa, saattaa suojata yritystä kohdennetulta hyökkäykseltä. Se ei kuitenkaan suojaa yritystä esimerkiksi niiltä hyökkäyksiltä, joita toteutetaan automatisoidusti ja joissa keskitytään enemmän kohteiden määrään kuin tyyppiin. Esimerkiksi kalastelusähköpostia voidaan lähettää mahdollisimman monelle siinä toivossa, että edes joku menee lankaan. Sähköpostiosoitteet voivat tällöin olla verkosta automatisoidusti kerättyjä ja listat pitkiä.

Lopulta on kuitenkin tärkeää miettiä mahdollisia riskejä yrityksen asiakkaan näkökulmasta. Esimerkiksi yleinen tietosuoja-asetus (GDPR) painottaa riskiperusteista lähestymistapaa henkilötietojen käsittelyssä. Tämä tarkoittaa sitä, että tietojen suojatoimet pitää suunnitella sen mukaan, kuinka suuri riski käsittelystä syntyy sille henkilölle, jonka tietoja käsitellään. Ei ole asiakkaan näkökulmasta juurikaan väliä, vuotaako esimerkiksi henkilötunnus suuren yrityksen tiedoista vai pienen – vaikutus on molemmissa tilanteissa asiakkaalle suuri.

Kyberturvan abc yrittäjille -hankkeessa keskityttiin nimenomaan yksinyrittäjien ja mikroyrittäjien kyber- ja tietoturvan parantamiseen. Koulutukset ja materiaalit tehtiin huomioiden se, ettei yrityksessä ole erikseen henkilöä, kenen osaamisalaa aiheet ovat.

Hankkeessa toteutettiin kolme koulutuskokonaisuutta, joista kahdessa keskityttiin yleisesti kyber- ja tietoturvaan yrityksissä. Yksi kokonaisuus oli kohdennettu sosiaali- ja terveysalan yrityksille, sillä alan yrityksissä tapahtuva tietojen käsittelyn luonne ja laajuus ovat johtaneet siihen, että alalla on näiden yleisten asioiden lisäksi erityisiä vaatimuksia.

Keskeistä koulutuksissa oli se, ettei niiden ymmärtäminen vaatinut aikaisempaa kyber- tai tietoturvaosaamista, vaan perustasoiset tietokoneenkäyttötaidot riittivät. Koulutuksissa huomioitiin myös se, ettei yrittäjä välttämättä pääse osallistumaan koulutuksiin paikan päällä johonkin tiettyyn aikaan. Tästä syystä koulutuksiin oli mahdollista osallistua etänä. Koulutuksia pystyi halutessaan katsomaan jälkikäteen juuri sellaisissa pätkissä kuin se parhaiten sopi.

Kuva 2. Yksi Kyberturvan abc yrittäjille -hankkeen koulutuskokonaisuuksista oli kohdennettu sote-alalle. (Kuva: Gettyimages)

Pienillä asioilla on suuri merkitys

Jo perusasioista huolehtiminen parantaa yrityksen kyber- ja tietoturvan tilaa. Kyberturvan abc yrittäjille -hankkeessa käytiin käytännönläheisesti läpi asioita alkeista lähtien.

Esimerkiksi haittaohjelmilta suojautumisessa merkittävässä roolissa on virustorjuntaohjelman käyttö ja laitteiden päivitysten ajantasaisuudesta huolehtiminen. Myös ymmärrys yleisistä haittaohjelmien levitystavoista on tärkeää. On hyvä ymmärtää, ettei työlaitteille kannata esimerkiksi ladata mitä vain sovelluksia, että kaikki verkot eivät ole turvallisia ja ettei epäilyttävältä vaikuttavia linkkejä kannata klikata.

Muita pieniä asioita, joilla käyttäjä voi parantaa omaa ja yrityksen turvallisuuden tilaa, ovat tarpeeksi vahvat salasanat ja muut salasanoihin liittyvät turvalliset toimintatavat, kuten se, ettei salasanoja kirjoiteta muistilapulle ylös tai ettei samoja salasanoja käytetä useissa palveluissa. Myös monivaiheinen tunnistautuminen sekä laitteiden lukitseminen niiden ääreltä poistuttaessa ovat yksinkertaisia mutta tärkeitä asioita.

Yleisten koulutusten aiheisiin kuului edellä mainittujen asioiden lisäksi muun muassa yritysten tavallisimmat kyberuhat, niiltä suojautuminen ja se, miksi kyberturvallisuudesta huolehtiminen on jopa kilpailuetu. Myös artikkelissa aiemmin mainitusta etätyöstä ja sen riskeistä puhuttiin. Muita koulutuksissa käytyjä aiheita olivat esimerkiksi tietoturvallinen työskentely, verkon turvallisuus, sosiaalinen media, pilvipalvelut sekä verkkosivut

ja kaupat. Ensimmäinen koulutuskokonaisuus toteutettiin syksyllä 2022 ja toinen kevään ja kesän 2023 aikana.

Koulutusten lisäksi hankkeessa tuotettiin oppaita, kuten yksinyrittäjän ja mikroyrityksen kyber- ja tietoturvaopas, jossa on kattavasti käyty läpi tärkeitä aiheita (Hölsä & Klauenbösch 2022). Opas sisältää kohta kohdalta eteneviä kuvallisia ohjeita, joiden avulla yrittäjä voi esimerkiksi ottaa kaksivaiheisen tunnistautumisen käyttöön sähköpostissa tai ottaa varmuuskopiot ulkoiselle kiintolevylle. Oppaiden lisäksi hankkeessa tuotettiin mallipohjia, artikkeleita ja videoita. Kyber- ja tietoturvan perusteita käytiin läpi myös Hyväksy kaikki evästeet -podcastissa.

Materiaalia löytyy kattavasti eri muodoissa, jotta mahdollisimman moni pystyy löytämään itselle parhaan keinon hyödyntää niitä ja parantaa yrityksensä kyber- ja tietoturvan tilaa. Materiaalit löytyvät hankkeen verkkosivuilta: https://www.xamk.fi/tutkimus-ja-kehitys/kyberturvallisuuden-abc-yrittajille/.

Sote-alalla tietoturvalle on omat vaatimukset

Kaikki aiemmin mainitut asiat ovat tietysti tärkeitä sosiaali- ja terveysalan yrityksissä, mutta niiden lisäksi alalla on myös erityisiä lakien tuomia velvoitteita. Tästä syystä yksi koulutuskokonaisuuksista oli kohdennettu sote-alalle. Kyseinen kokonaisuus toteutettiin syksystä 2022 kevääseen 2023.

Sosiaali- ja terveysalalla käsitellään paljon henkilötietoja, jolloin turvallisuuden merkitys korostuu entisestään. Vuonna 2021 voimaan tullut laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä eli asiakastietolaki (784/2021) on pyrkinyt parantamaan asiakastietojen käsittelyn tietoturvaa[4]. Yksi keskeinen keino tähän on tietoturvasuunnitelman laatiminen.

Tietoturvasuunnitelma on asiakirja, jossa kuvataan kaikki ne toimenpiteet, joilla palveluntarjoaja varmistaa asiakastietojen turvallisen kä-

[4] Sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annettu laki 784/2021 on kumottu säädöksellä 703/2023 (Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä), joka tulee voimaan 1.1.2024.

sittelyn. Asiakirja on kattava, ja sen laatimista edellytetään sote-alan yrityksiltä, jotka käsittelevät asiakas- tai potilastietoja. Suunnitelma on tärkeä osa sote-alan yrityksen tietoturvaa, ja sen laatiminen voi laajuutensa vuoksi vaikuttaa haastavalta, joten suunnitelmaan keskityttiin paljon hankkeen koulutuksissa ja muissa materiaaleissa.

Asiakastietolaki velvoittaa yhä useampia sote-alan palvelunantajia ottamaan valtakunnalliset tietojärjestelmäpalvelut eli Kanta-palvelut käyttöön. Hankkeen koulutuksissa annettiin ohjeita myös siihen.

Kyberturvan abc yrittäjille -hankkeessa valmistuneet sote-aiheiset materiaalit kasattiin yhteen tietopankkiin, joka on osoitteessa https://xamk.fi/kybersote. Materiaalia on monessa eri muodossa: niin kirjallisia oppaita ja mallipohjia kuin videoita, podcasteja sekä infograafeja. Esimerkiksi tietoturvasuunnitelman laatimisesta löytyy videosarja, jossa eri aiheita on jaettu omiin lyhyisiin videoihin. Kattavassa materiaalipankissa on vastauksia moneen sote-alan kyber- ja tietoturvaan liittyvään kysymykseen.

Varautumisessa on huomioitava myös kybernäkökulma

KyberReact Kymi22 – Last Call -hanke pyrki vahvistamaan kymenlaaksolaisten pk-yritysten kyberresilienssiä muuttuvassa maailmassa. Keskeisenä aiheena oli ulkopuolelta tulevaan verkkovaikuttamiseen varautuminen.

Suuri osa hankkeen koulutuksista järjestettiin webinaarimuotoisina tietoiskuina. Tietoiskujen aiheita olivat muun muassa somekuplat ja niiltä suojautuminen, hyvät ja pahat hakkerit sekä informaatiovaikuttamisen monet muodot. Niissä pureuduttiin myös viestintään kyberkriisin koittaessa sekä siihen, miltä tietoturvan tulevaisuus näyttää. Viimeisessä tietoiskussa keskityttiin koulutuksiin osallistuneiden henkilöiden toiveesta tekoälyyn. Webinaarien lisäksi aiheita käsiteltiin myös infograafien ja artikkelin muodossa.

Hankkeessa järjestettiin keväällä 2023 kyber- ja tietoturvaan keskittyvä tapahtuma Kybertuskapäivä yhteistyössä Satamalogistiikan kyberhygienia -hankkeen kanssa. Tapahtuma järjestettiin hybridinä, ja siihen pääsi osallistumaan joko verkossa tai paikan päällä Xamkin Kotkan kampuksella. Puhujina tapahtumassa oli sekä kotimaisia että kansainvälisiä huippuasiantuntijoita, ja tapahtuma keräsi paljon positiivista palautetta osallistujilta.

Myös tietoiskuista pidettiin. Moni niistä herätti hyvää keskustelua koulutuksen aikana chatissa ja asiantuntijapuheenvuoron loppuun jätetyssä, kysymyksille ja keskustelulle varatussa ajassa.

Kuva 3. Keskeisenä aiheena KyberReact Kymi22 – Last Call -hankkeessa oli muun muassa ulkopuolelta tulevaan verkkovaikuttamiseen varautuminen. (Kuva: Gettyimages)

Pienten yritysten kyberturvan parantamisella on laajoja vaikutuksia

Tilastokeskuksen mukaan valtaosa suomalaisista yrityksistä on alle kymmenen työntekijän mikroyrityksiä (Tilastokeskus 2023). Monessa kohtaa esimerkiksi tietoturvaan liittyvät vaatimukset ovat kuitenkin samalla tasolla kuin suurissa yrityksissä, joilla on enemmän resursseja panostaa aiheeseen.

On tärkeää auttaa pienempiä yrityksiä pitämään huolta kyber- ja tietoturvasta. Se vaikuttaa yritysten kilpailukykyyn, jatkuvuuteen sekä asiakkaiden ja työntekijöiden tietoturvaan.

Kyberturvan abc yrittäjille ja KyberReact Kymi22 – Last Call -hankkeet tarjosivat ajankohtaista ja käytännönläheistä koulutusta aiheisiin liittyen. Etenkin Kyberturvan abc yrittäjille -hankkeessa tuotettiin jälkikäteenkin hyödynnettäviä materiaaleja niille, jotka haluavat parantaa oman yrityksensä kyber- ja tietoturvan tilaa.

LÄHTEET

Hölsä, M. & Klauenbösch, J. 2022. Yksinyrittäjän ja mikroyrityksen kyber- ja tietoturvaopas. Kyberturvan abc yrittäjille. PDF-dokumentti. Päivitetty 24.4.2023. Saatavissa: https://www.xamk.fi/wp-content/uploads/2023/04/kyber-ja-tietoturva-opas-24.4.2023.pdf [viitattu 6.10.2023].

Traficom 2023. Kyberturvallisuuden uhkataso pysynyt kohonneena – kohdistettujen hyökkäysten määrä noussut. WWW-dokumentti. Saatavissa: https://traficom.fi/fi/ajankohtaista/kyberturvallisuuden-uhkataso-pysynyt-kohonneena-kohdistettujen-hyokkaysten-maara [viitattu 6.10.2023].

Martin, A. 2023. Finland sees fourfold spike in ransomware attacks since joining NATO, senior cyber official says. *The Record* 3.8.2023. Verkkolehti. Saatavissa: https://therecord.media/finland-sees-fourfold-spike-in-rasomware-attacks-nato [viitattu 6.10.2023].

Tilastokeskus. 2023. Yritysten rakenne- ja tilinpäätöstilasto. WWW-dokumentti. Saatavissa: https://pxdata.stat.fi/PxWeb/pxweb/fi/StatFin/StatFin__yrti/statfin_yrti_pxt_13w1.px/table/tableViewLayout1/ [viitattu 6.10.2023].