Tietoturva podcast osa 9. Vieraana Helinä Turunen Kyberturvallisuuskeskuksesta.

Tom Tuunainen
Tietoturva podcast osa 9. Vieraana Helinä Turunen Kyberturvallisuuskeskuksesta.

Laura Palovuori.

Vieraana tämänkertaisessa podcastissa on Helinä Turunen. Esitteletkö itsesi?

Helinä Turunen
Heippa vaan kaikille. Olen Helinä Turunen kyberturvallisuuskeskuksesta ja toimin siellä erityisasiantuntijana. Tällä hetkellä seuraan ajankohtaisia tietoturvailmiötä, joihin kuuluu niin globaaleja ilmiöitä kuin myös kansalaisiin kohdistuneita tietoturvaloukkauksia.

Tom Tuunainen
Mitä kyberturvallisuuskeskus tekee?

Helinä Turunen
Kyberturvallisuuskeskus on Liikenne- ja viestintävirasto Traficomin alainen organisaatio ja siellä kehitetään ja valvotaan viestintäverkkojen ja palveluiden toimintavarmuutta ja turvallisuutta.Tämä näkyy esimerkiksi, meidän tuottamassa tilannekuvassa, joka julkaistaan viikoittain verkkosivuillamme. Tässä viikkokatsauksessa on kaikille luettavissa, mitä tapahtuu Suomessa ja tietoturvan saralla niin kotimaassa kuin kansainvälisestikin. Ja sen lisäksi meillä on sääntelyä ja valvontaa ja erilaista arviointitoimintaa. Myös kansallinen koordinointikeskus löytyy kyberturvallisuuskeskuksesta ja meillä myös on satelliittipaikannukseen liittyvä viranomainen meidän organisaatiossamme.

Laura Palovuori
Tänään ajattelimme puhua digitaalisesta turvallisuudesta. Digitalisaatiossa on kaksi puolta, on käyttäjän turvallisuus ja hyvinvointi sekä yritysten mahdollisuus uusiin liikeideoihin. Helinä Turunen, mitä me oikein suojelemme, kun puhumme digitaalisesta ympäristöstä?

Helinä Turunen
Näen sen niin, että kun me puhumme digitaalisesta ympäristöstä, tarkoitamme ympäristöä, joka ei ole enää fyysistä ja jota emme ehkä ymmärrä samalla tavalla kuin fyysistä ympäristöämme. Edessämme voi olla tietokone, tabletti, työkone tai jokin muu elektroninen laite, joka on liitetty erilaisiin verkon yli toimiviin järjestelmiin, joihin tallennetaan tietojamme ja joissa lähettelemme sähköposteja ja keskustellaan ihan arkisistakin asioista. Sen lisäksi tähän digitaaliseen ympäristöön kuuluu kaikki julkiset palvelut, joita saatamme käyttää joka päivä. Esimerkiksi erilaiset reittioppaat, kun yritetään päästä töihin tai kouluun tai lähteä matkalle. Voimme esimerkiksi seurata, millä tavalla lentokoneet lentelevät tänään ja tuleeko lentokone ajoissa. Tämä on digitaalisessa ympäristössä kulkeva tieto ja lentoyhtiöt käyttävät sitä päivittäin. Tässä meidän digitaalisessa ympäristössämme tänä päivänä on aika paljon ja emme ehkä ihan ymmärrä sen laajuutta ihan sellaisella tasolla kuin mitä meidän pitäisi. Ymmärrämme kuitenkin, että jos nämä asiat eivät toimi, niin meillä on ongelma. Digitaalinen ympäristö on siis osa meidän jokapäiväistä elämäämme nykyään.

Tom Tuunainen
Useinhan kuulee sanottavan, että minulla ei ole mitään salaisuuksia, mitä sanoisit tällaisille henkilöille?

Helinä Turunen
Tämä on hyvin tyypillinen kommentti, silloin kun aletaan miettimään, että eihän minulla ole mitään erityissuojattavaa asiaa, jonka takia minun pitäisi kiinnostua siitä, minkä mittainen salasanani on tai onko jääkaappini softa päivitetty. Mutta totuus on, että meillä kaikilla on pääsy sellaisiin järjestelmiin ja käytämme digitaalisia palveluita joka päivä ja meillä pitää olla samanlainen kyberhygienia näissä palveluissa kuin mitä meillä on esimerkiksi näissä meidän ihan fyysisissä palveluissamme. Fyysisillä palveluilla tarkoitan sitä, että jos menet vaikka töihin ja sinulla on työpaikan avaimet, niin pidät näistä avaimista hyvää huolta. Et anna avaimia kellekään ulkopuoliselle ja huolehdit siitä, että jos avaimesi katoavat, niin ilmoitat asiasta. Samalla tavalla kotiavaimesi on sellainen, mistä jo pienestä pitäen opetetaan pitämään huolta, kerrotaan jos se hukkuu ja toivotaan, että avain pysyy tallessa. Samalla pieteetillä meidän pitäisi käsitellä näitä digitaalisia ympäristöjämme tai verkkopalveluitamme esimerkiksi sähköpostia tai sosiaalisen median tiliä, jonka takana saattaa olla pitkä elämäntyösi, vaikka verkostotoiminnassa. Jos olet sosiaalisen median vaikuttaja tai teet työksesi pelkästään verkossa asioita, miten käy jos verkkopalvelusi niin sanottu avain, salasana tai muu tunniste häviää tai jos joku muu nappaa sen? Meillä ei ehkä ole syntynyt vielä tarpeeksi vakavaa asennetta siihen, että pitäisimme myös näistä asioista huolta. Toivoisinkin, että jokainen pitäisi omaa sometiliä tai muita verkon palveluita, tietokoneita tai verkkopankkitunnuksia ihan yhtä tärkeinä kuin kotiavaimiaan ja muita omia fyysisiä tavaroitaan. Koska näihinkin rikolliset haluavat päästä käsiksi ja pääsyä järjestelmiin halutaan hyödyntää, vaikka olisitkin niin sanottu tavallinen kansalainen. Kaikki kiinnostaa ja siksi meidän täytyy pitää näistä palveluista ihan yhtä hyvää huolta kuin meidän omista fyysisistä tavaroistamme ja kotiavaimistamme.

Laura Palovuori
Entä sitten työpaikalla ja etätyöntekijät? Mitä terveisiä sanoisit etätyöntekijöille ja yritykselle, joka tarjoaa etätyömahdollisuuksia?

Helinä Turunen
Sama asia pätee siihenkin. Fyysinen työväline ja siitä huolehtiminen on ollut tärkeätä aina ja samalla tavalla täytyy pitää huolta työläppäreistä ja työhön liittyvistä sähköpostitileistä sekä muista tunnuksista. Näistä on yhteistyössä yritysten kanssa ollut paljon keskustelua. Etenkin tässä korona-ajan alussa etätyöhön liittyviä erilaisia ohjeistuksia julkaistiinkin tiuhaan tahtiin niin kyberturvallisuuskeskuksen kuin muidenkin toimesta ja sielläkin tärkeimpinä nousee taas ihan perusasioita. Työntekijän näkökulmasta on tärkeää, että aina käytetään työnantajan antamia laitteita. Niistä pidetään hyvää huolta ja niihin asennetaan tarvittavat päivitykset. Päivitykset suojaavat niitä jokapäiväisiltä hyökkäyksiltä ja estävät suoran pääsyn laitteeseesi tai palveluihin haavoittuvuuksien kautta. Samaan tapaan kuin vaikka työpaikan rikki mennyt etuovi korjataan, päivityksiä hyödynnetään laitteiden kunnossapitoon. Oli kyse sitten vaikka sosiaalisen median ylläpitotunnukset tai sähköpostien ja erilaisten palveluiden tunnukset, niistä täytyy pitää samalla tavalla huolta, niissä pitää olla vahva salasana ja kaksivaiheinen tunnistautuminen käytössä. Ja jos ei sole työpaikan puolesta ohjeistettu, mikä turvallinen käyttö on niin aina saa kysyä ja työpaikkojen on tärkeää tukea etätyöntekijöitä turvallisessa työskentelyssä.

Tom Tuunainen
Teettekö itse paljon näitä töitä kyberturvallisuuskeskuksesta ja onko teillä sitten jotain erityisiä käytänteitä tähän.

Helinä Turunen
Hyvistä käytänteistä on huomattu, että läheisessä yhteydessä muihin etätyöntekijöihin oleminen on tärkeää, niin turvallisuuden kuin muidenkin etätyötehtäviin liittyvien kysymysten saralla. Koska etätyössä käy helposti niin, että jos ei ole läsnä toimistolla eikä esimerkiksi keskustele kollegoiden kanssa niin saattaa jäädä epäilemään, että onko joku sähköpostiviesti tai sosiaalisessa mediassa tullut viesti aiheellinen vai ei. On tärkeää ylläpitää sellaista turvallisuuskulttuuria, myös etätyöaikana, että kertoo erilaisesta tietoturvaan liittyvistä ilmiöistä, jotka koskevat etätyöntekoa ja kannustaa ilmoittamaan erilaisista poikkeamista ja kertomaan, jos on saanut, vaikka sähköpostiin oudon näköisen viestin tai sosiaalisessa mediassa joku kysyy nyt vähän liian herkkiä kysymyksiä. On todella tärkeää pitää yhteys työntekijöihin myös etäaikana. Koska jos jää yksin arpomaan ja ei oikein tiedä kenelle pitäisi kertoa mahdollisista ongelmista niitä ei ehkä havaita. Saattaa esimerkiksi tulla kalasteluviesti, joka sisältää haitallisen liitteen tai kalastelulinkin, joilla yritetään saada tunnuksia haltuun. Koen, että yleisellä tasolla on etätyönteossa tärkeätä, että ylläpidetään yhtä hyvää turvallisuuskulttuuria kuin aiemminkin ja madalletaan kynnystä. Keskustellaan myös mahdollisista ongelmista ja jos vahingossa nyt sitten haksahtikin, niin on myös tärkeää, että siitä pystyy ilmoittamaan ja siitä ei seuraa häpeää, vaan yhdessä ratkaistaan ongelmat.

Laura Palovuori
Tuli mieleen kaikkia tuollaisia etätyössä jaksamiseen liittyviä kysymyksiä. Yksinäisyyden aiheuttamia ongelmia. Onko niin, että ihmisen psyykekin on sitten tietoturvauhka? Ymmärrätkö mitä tarkoitan?

Helinä Turunen
Ymmärrän mitä ajat takaa. En tiedä, onko psyyke uhka vai pitääkö meidän ymmärtää se toinen tulokulma, eli että ihmisten psyykettä hyödynnetään siinä, että meitä kohtaan voidaan hyökätä digitaalisten järjestelmien kautta. Ehkä enemmän siitä näkökulmasta katsoisin, että tekstipohjaisessa viestinnässä on helpompaa lähettää kalasteluviestejä, tai suostutella ilman, että käy mitään muuta interaktiota kuin tekstin kautta tapahtuva. Sanoisin, että se ei ehkä ole sen vastaanottajan vika koskaan, että joutuu kohteeksi ja uhriksi, vaan meillä on niin pitkälle kehittynyt rikollinen toiminta, etenkin kyberpuolella, että pystytään suostuttelemaan erilaisin keinoin pelkän tekstin perusteella esimerkiksi avaamaan linkki ja syöttämään tunnuksia. Toki, kun sen ilmiönä ymmärtää ja siitä on tietoinen, niin näitä yrityksiä pystyy jokainen käyttäjä havaitsemaan. Mielestäni on aika julmaa, että yksin käyttäjälle annetaan valtava vastuu tunnistaa kaikki edistyneet hyökkäykset, joissa saatetaan tekeytyä oman organisaation henkilöstöksi tai käyttäjän ystäväksi tai jonkun muun käyttäjälle merkittävän tahon edustajaksi ja sitä kautta ujutetaan hänelle haittaohjelma tai viesti. Mutta tässä on kaksi näkökulmaa. Yritysten pitää olla tietoisia siitä, että näitä tapahtuu ja yritysten ja organisaatioiden tulee pystyä tukemaan käyttäjää näiden asioiden tunnistamisessa. Turvallisuuskulttuuri on todella tärkeää ja yhä edelleen tekniset menetelmät ovat niitä, joilla pystytään estämään iso osa hyökkäyksistä. Kaksivaiheinen tunnistautuminen pitäisi olla käytössä melkein kaikkialla. Sen lisäksi pitäisi pystyä valvomaan verkkoliikenteestä minkälainen käyttäytyminen on tavallista ja minkälaisia tiedostoja esimerkiksi saa suorittaa käyttäjien koneella. Tätä teknistä näkökulmaa ei kannata myöskään unohtaa, koska käyttäjä ei ole heikoin lenkki niin kauan, kun meillä on verkkoon avoimena todella monenlaisia internetpalveluita erilaisista organisaatioista, ihan sähköpostijärjestelmistä ja tietokannoista lähtien. Joten on hyvä muistaa myös organisaatioiden oman teknisen tietoturvan vastuu näissä kysymyksissä.

Laura Palovuori
Meillä itse asiassa aikaisemmissa podcasteissa käydäänkin läpi, mikä on kaksivaiheinen tunnistus, mutta kertoisitko nopeasti, mitä se tarkoittaa?

Helinä Turunen
Totta kai. Kaksivaiheinen tunnistautuminen on sellainen menetelmä, jolla salasanan lisäksi kirjaudutaan myös jotain muuta tunnistautumistapaa käyttäen. Eli jos mietitään vaikka verkkopankkitunnistautumista, niin siellä on yleensä ollut käyttäjätunnuksesi ja sitten salasana tai pin- koodi, palvelusta riippuen ja sen lisäksi sinulle tulee sitten lisäkoodi, joka pitää syöttää joko puhelimella hyväksyen tai jostain koodilistasta. Tämä on kaksivaiheinen tunnistautuminen, tarvitaan jotain muuta käyttäjätunnuksen ja salasanan lisäksi, jotta päästään kirjautumaan järjestelmään. Näitä tapoja on aika paljon. Tuollainen puhelimeen tuleva koodi on aika yleinen. Se voi tulla tekstiviestin muodossa tai sitten koodisovelluksessa, jonka asennat puhelimeen. Tai sitten on myös fyysisiä koneeseen laitettavia USB- tikun kaltaisia. varmennetikkuja, joilla sitten voidaan kirjautua myös sisään. Nykyään myös pystyy puhelimeen NFC-tunnisteella lisäämään kaksivaiheinen tunnistautuminen. Eli tapoja on monia, mutta tärkeä juttu on, että se tuo lisäsuojaa pelkän käyttäjätunnuksen ja salasanan lisäksi. kun kirjaudutaan järjestelmiin.

Laura Palovuori
Minkälainen digiympäristön pitäisi olla, että yritykset uskaltavat lähteä siirtämään palvelujaan digitaalisiksi?

Helinä Turunen
Kyllä turvallisuus on kaikki kaikessa. Uskalletaanko viedä yrityksen tietoja digitaaliseen palveluun, koetaanko, että pilvipalvelut ovat tarpeeksi turvallisia. Minkälaista tietoa ensinnäkin yrityksellä on, pitääkö sitä suojata jotenkin erityisesti ja voiko sitä edes digitalisoida? Siinä on paljon erilaisia kysymyksiä, joita joutuu käymään läpi. Ja mistä saa tukea, kun digitalisoi palveluitaan? Tässä moni organisaatio tukeutuu esimerkiksi palveluntarjoajiin, saattaa löytyä toinen organisaatio, joka auttaa siirtymässä, tekemällä esimerkiksi käyttäjätunnukset pilvipalveluihin ja ylläpitämällä niitä ja sitä kautta organisaatio ainoastaan kirjautuu ja alkaa käyttää. Mutta näissä siirtymävaiheissa koen aina, että on todella tärkeätä, että ymmärretään kenellä on vastuu digitaalisen ympäristön turvallisuudesta. On myös ollut sellaisia tapauksia, joita meilläkin on nähty etätyön aikana, missä organisaatio on saanut kalasteluviestejä ja ne ovat sieltä lähteneet eteenpäin. Joku on vahingossa laittanut tunnukset ja kaksivaiheinen tunnistautuminen ei olekaan ollut päällä ja kalasteluviestejä lähtee sieltä eteenpäin. Koska organisaatio ei itse ylläpidä omaa sähköpostijärjestelmää saattaa selvittäminen yllättäen kestää kauan, koska palveluntarjoajalta täytyy pyytää apua ja tukea sähköpostin turvallisuuteen liittyen esimerkiksi siinä, kuinka paljon lähti viestejä ja miten tämä voidaan estää. Eräs isoimpia askeleita on että, jos ostaa sähköpostin joltakin firmalta, on selkeästi määritelty turvallisuusvastuut, oli yritys sitten pieni tai suuri. Täytyy tietää pitääkö firma huolta sen turvallisuudesta vai joutuuko yritys itse määrittelemään kaksivaiheiseen tunnistautumiseen ja joutuvatko he tekemään joitain maakohtaisia rajoituksia, vaikka kirjautumiseen? Tässä tulee olla tarkkana, että tiedetään varmasti, kenellä on vastuu, jos jotakin tapahtuu ja mitkä ovat yhteystiedot siinä vaiheessa. Koen että turvallisuudesta puhuminen on ensiaskel, kun hankitaan digitaalista ympäristöä. Määritellään se sopimuksessa, koska ilman turvallista palvelua ja turvallisuusvastuita en koe, että on kovin helppoa lähteä digitaaliseen maailmaan turvallisin mielin.

Tom Tuunainen
Nämä hyvät ohjeet pätevät varmaan myöskin ihan tavallisiin kuluttajiin. Onko sinulla muuten jotain näkökulmia siitä, että millaisin toimenpitein tietoturvasta tulisi ihan kansalaistaito?

Helinä Turunen

Toimet ovat sellaisia, joita mielestäni on jo alettu tekemään. Keskustellaan tietoturvasta , kyberturvallisuudesta ja myös muista esiinnousseista tapahtumista kuten esimerkiksi kiristyshaittaohjelmista, hyökkäyksistä, tietojen kalasteluista tai vaikka viranomaisten nimissä tapahtuvasta pankkitunnusten keräämisestä, mistä esimerkiksi Omakanta ja Kela ovat tiedottaneet erinomaisen hyvin. Myös erilaiset ilmiöt nostetaan julkisuuteen ja ollaan tietoisia siitä, että tällaiset ovat arkipäivää. Näitä asioita tapahtuu joka päivä ja tietämyksen ylläpitäminen ja sitä kautta sen kehittäminen on ensiaskel kyberkansalaistaitojen kehittämiseen. Toivoisin kovasti, että nämä aiheet pääsisivät opetussuunnitelmaan asti. Näin pystyttäisiin käsittelemään turvallisuutta ihan koulun penkillä. Se on sellainen taito, joka saattaa puuttua joistain kodeista riippuen siitä, kuinka harrastanut on ja millä tavalla on toiminut turvallisuusasioiden kanssa. Kaikilla ei esimerkiksi ole kotona tietokonetta, millä voisi harjoitella turvallista tietokoneen käyttöä, joten sen pitää lähteä yhteiskunnan perusrakenteista, niin että kaikilla on mahdollisuus opetella niitä taitoja koulussa tai muissa julkisissa palveluissa. Sitä kautta rakennetaan perustietämystä arkisen turvallisuuden kasvattamiseen.

Tom Tuunainen
Myös tekoäly, vaikkapa Chat GPT on nostanut päätänsä. Näetkö, että tätä voisi ehkä hyödyntää myös tietoturva asioissa? Vai näetkö tässä jonkinlaista uhkaa?

Helinä Turunen
Tekoälyn kehitys on tässä viimeisen parin kuukauden aikana ollut todella merkittävää. On keskusteltu jo pitkään, millä tavalla tekoäly voi auttaa tietoturvatoimintoja ja millä tavalla se voi kehittää tietoturvaa. Mieleistäni mahdollisuuksia on. Microsoft esimerkiksi on tuonut omaan palvelutarjontaansa tekoälyavusteisia havainnetunnistepalveluita heidän pilvipuolensa maksullisiin palveluihin. He ovat ottaneet ensiaskeleen tekoälyn käyttöön ottamisessa poikkeamien havainnointiin ja niistä ilmoitusten tekemiseen. Olen edelleen sitä mieltä, että totta kai tekoäly on tärkeä askel tietojen käsittelyssä tai tiedon tulkitsemisessa. Mutta edelleen päätöksen tekee ihminen. Tekoäly on hyvä työkalu, mutta sen tulkitsijana pitää olla kuitenkin ihminen, joka ymmärtää turvallisuuden erilaisia ilmiöitä ja tekee päätökset sen perusteella.

Koska olen myös käyttänyt välillä CHAT GPT- tekoälyä ja ihan mielenkiinnosta olen kysynyt siltä tietoturva-aiheisia kysymyksiä, en tiedä onko tässä nyt kyse siitä maksaako siitä palvelusta vai ei mutta olen kokeillut ilmaisversiota itse, ja tuntuu että sillä on ainakin tällä hetkellä, huhtikuussa 2023, joitain tiettyjä olettamia, mitä se ujuttaa omiin vastauksiinsa. Kannattaa muistaa, että tekoäly on koulutettu jollain datalla ja siellä datassa saattaa olla vääristymiä, jotka ohjaavat tekoälyä tekemään jonkunlaisen päätöksen, saman päätöksen joka kerta. Esimerkiksi olen kirjoittanut Chat GPT: lle, että haluaisin kirjoittaa blogipostauksen, missä kerrotaan, että yrityksessäni on ollut tietoturvapoikkeama. Hyvin yksinkertainen viestinnällinen kysymys ja chat GPT aina kirjoittaa minulle vastauksen, jossa se kertoo, että lopuksi koulutamme vielä käyttäjiämme tunnistamaan tietojen kalasteluyrityksiä ja erilaisia poikkeamia ja teemme käyttäjillemme tietojen kalastelukoulutuksen. Kummastelin tätä vastausta aina, koska siinä vastauksessa aina sysättiin tavallaan vastuu käyttäjälle. Eli tekoäly kokee, että tässä ulospäin menevässä viestinnässä tärkeintä oli kertoa, että loppukäyttäjille tehtiin jonkunlainen koulutus ja loppukäyttäjälle sysättiin jonkunlainen vastuu tietoturvan kehittämisestä, vaikka tekoäly olisi voinut kertoa myös niistä erilaisista teknisistä toimenpiteistä, joita olisin voinut tehdä, jotta tällaista tapausta ei enää tulisi. Mutta kyllä se osasi niistä teknisistä toimenpiteistä kirjoittaa, kun sille vaan erikseen määritti, että kirjoita minulle tekniset toimenpiteet myös, joita tulemme tekemään, että näin ei käy. Mahdollisuuksia siis on, mutta täytyy olla tarkkana, että ihan kaikkeen ei defaulttina usko, koska se on aina jollain tavalla koulutettu. Sillä on jokin pohjadata, joka ainakin tällä hetkellä on vääristynyt,

siihen liittyen, että minkälaisia vastauksia sieltä tulee. Onko siis kyseessä uhka vai mahdollisuus? Mielestäni erittäin suuri mahdollisuus, mutta vielä on paljon kehitettävää.

Laura Palovuori
Puhutaan aina siitä, miten kyberrikollisuudelta suojaudutaan. Ja niinhän mekin puhumme siitä, kun neuvomme miten suojaudutaan. Onko sitten niin, että netissä oleva rikollisuus on jotenkin niin pimeää ja piilotettua, että siihen ei osata suhtautua? Vai onko tapauksia, joissa rikollinen joutuu vastuuseen? Mitä heille tapahtuu ja tiedätkö sinä kuinka kovia tuomiot ovat?

Helinä Turunen
Kyllähän rikolliset joutuvat vastuuseen. Toki tietoturvan puolella haasteita asettaa Internetin globaalius, eli voi olla tilanteita, missä ihminen voi istua toisella puolella maailmaa ja voi pakoilla erilaisia tuomioita pitkään. Mutta on ollut myös tapauksia, missä ihmisiä on saatu kiinni. Monesti ne liittyvät sellaisiin pieniin virheisiin, mitä erilaiset rikoksia tehtailevat ihmiset ovat tehneet ja joiden perusteella erilaiset tutkijat ovat sitten päässeet heidän jäljilleen. Koko ajan esimerkiksi Europol julkaisee mielenkiintoisia Take down- operaation ja muiden vastaavien postauksia heidän verkkosivuillaan. Näissä kerrotaan esimerkiksi, että palvelunestohyökkäyksiä tehtaileva sivusto on otettu alas ja sen takana olleet henkilöt on pidätetty. Tai että kiristyshaittaohjelman ryhmän adminet on pidätetty jossain maassa paikallisen poliisiyhteistyön toimesta. Näitä rikollisia pystytään siis seuraamaan ja heitä saadaan kiinni ja saatetaan vastuuseen. Joskus tähän tulokseen pääseminen vaatii pitkäkestoista työtä. Mutta kyllä näitä joskus tapahtuu ja tapaukset ovat joskus merkittäviä.

Laura Palovuori
Hyvä kuulla. Suomessa Vastaamon tapaus toi kyllä ihmisten tietoisuuteen tietoturvan tärkeyden. Mutta aika usein tällaiset ”kyberiläiset” keskustelevat keskenään kyberturvallisuusasioista, mikä olisi tehokkain tapa levittää tietoa sillä tavalla, että siitä
kiinnostuisivat sitten tavallisetkin tallaajat.

Helinä Turunen
Koen, että arkipäiväistäminen on todella tärkeä askel ja myös keskusteleminen tietoturvasta uutisista lähtien, erilaisissa ohjelmissa keskusteleminen tai podcastissa, kuten nytkin tässä erinomaisessa podcastissa. Tehdään arkisia tekoja sen eteen, että voidaan jakaa myöskin selkeää tietoa näistä jokapäiväisistä ilmiöistä. Minusta tuntuu, että monesti on helppo sanoa, että no älä klikkaa linkkiä, ja laita nyt se kaksivaiheinen tunnistautuminen päälle, mutta jos ei ymmärrä sitä syytä, minkä takia näitä toimenpiteitä pitää tehdä, niin kommentti valuu kuin vesi hanhen selästä. Eli meidän pitää olla parempia kertomaan kaikille ihan perustermein, minkä takia tämä on tärkeää, minkä takia sinun pitää suojata omaa digitaalista ympäristöäsi, minkä takia sinun tietosi ovat tärkeitä tai minkä takia sinun yrityksesi tiedot ovat tärkeitä?

Koen että se vaatii sekä organisaatioilta että julkisilta toimijoilta, ja myös yksityisiltä toimijoilta toimenpiteitä. Olen nähnyt tässä viimeisen parin vuoden aikana todella hyvää kehitystä siinä, että on suuria tapahtumia, joista tulee hyviä keskusteluita siitä, miten voidaan parantaa arkista turvallisuutta. On myös näitä paikallisia kyberturvallisuus- ja tietoturva-asia toimijoiden yhteistapaamisia ja siellä keskustellaan, ja sieltä saadaan joskus ihan hyviä ideoita arkiosaamista parantavista projekteista. Olen kokenut, että tällaiset julkisesti saatavilla olevat projektit ovat hyvin tärkeitä, eli tietopaketit ja ohjeistukset ja niiden jalkauttaminen.

En usko, että kukaan menee kyberturvallisuuskeskuksen sivuille jonakin perjantaiaamuna ja päättää, että lukee sieltä kaikki ohjeistukset ajatellen, että nyt olen turvassa, kun itse tulin tänne ja luin tämän kaiken. Sen pitää olla ohjattua, arkisia keskusteluita pitää tehdä saatavimmiksi ja

turvallisuutta ylläpitäviä toimenpiteitä täytyy tehdä. Olen nähnyt esimerkiksi paikallisissa kirjastoissa aika hyviä aloitteita tähän liittyen. Siellä järjestetään digitukitoimintaa, missä neuvotaan ohjatusti sähköpostin turvallista käyttöä ja kerrotaan miksi se on tärkeää. Opetetaan myös, miten kaksivaiheisen tunnistautumisen saa päälle tarjotaan toisin sanoen matalan tason tukea siellä missä ihmiset ovat, eli julkisissa palveluissa.

Mutta samaan aikaan pidetään huolta myös siitä, että organisaatiossa, oli se sitten koulu, korkeakoulu, julkinen toimija, yksityinen toimija tai vaikka ihan paikallinen harrasteorganisaatio, tietyistä tietoturva-asioista tehdään arkipäiväisiä. Samaan tapaa kuin keskustellaan siitä, että mihin kaappiin laitetaan avaimet sen jälkeen, kun on lopetettu harrastetoiminta ja kuka sammuttaa valot, kun poistuu. Koen että olemme kyllä päässeet siinä eteenpäin, mutta vielä vaaditaan lisää askelia sen eteen.

Laura Palovuori
Kiitos. Tämä olikin hyvä pointti. Oliko sinulla vielä jotain, mitä tulee mieleen?

29:54Helinä Turunen
Menee ehkä vähän kyberin puolelle tästä arkipäiväisestä digiturvasta, mutta kyberturvallisuus sanana on ehkä vähän sellainen mikä voi kolahtaa vähän etäisenä ja vieraana. Ei ehkä koeta, että kyberturvallisuus on itselle ensimmäinen prioriteetti, kun miettii minkälaisia suojaustoimenpiteitä pitäisi tehdä. Olen seurannut viimeisten vuosien aikana aika paljon, myös globaalisti, kyberturvallisuutta ja miten se liittyy ihan arkiseen elämään. Tavallisten ihmisten sähköpostit ja verkkopalvelut ja muut liittyvät kyberturvallisuuteen, siten että sinun jokapäiväisiä sähköpostitilejäsi saatetaan esimerkiksi kaapata ja niiden avulla voidaan toteuttaa muita hyökkäyksiä.

Otan esimerkin, vaikka Ukrainan uudelleen kiihtyneestä sodasta, jossa kyberturvallisuus oli keskiössä. Siellä tapahtui todella paljon kyberin saralla. Siellä hyvin tyypillinen tapa, millä pyrittiin levittämään esimerkiksi haittaohjelmia, oli kaapata isojen palveluiden ja julkisten palveluiden sähköpostitilejä ja niiden kautta lähettää kalastelu- ja haittaohjelmaviestejä eteenpäin halutuille kohteille esimerkiksi Ukrainan valtionhallinnossa tai halutussa kohdeorganisaatiossa. Tällaisten aitojen tilien käyttäminen palvelee hyökkääjää, koska tunnetulla palvelulla on hyvä maine. Silloin hyvä maine ja tekniset tietueet ovat sellaisessa kunnossa, että yleensä sähköpostiviesti pääsee läpi kohdeorganisaatioon. Ukrainassa suurissa käyttäjäfoorumeissa olevia käyttäjätilejä ja sähköpostipalveluita murrettiin, koska niiden kautta päästiin lähettämään hyökkäyksiä kohdeorganisaatioihin. tämä on yhteys, jota haluaisin, että tuotaisiin enemmän esille arkipäiväisessä turvallisuudessamme.

Eli niitä meidän omia digitaalisia ympäristöjämme, palveluita, sometilejä ja sähköpostikäyttäjätilejä voidaan haluta sen takia, että niitä voidaan hyödyntää sitten muissa hyökkäyksissä. Ja sitä keskustelua en näe kauhean paljon. Mikä on hirveän harmi, koska tämä on olennaista tietoa, joka auttaa meitä ymmärtämään oman digitaalisen ympäristön turvallisuuden merkitystä suuremmassa kontekstissa. Jokaisen arkipäiväinen turvallisuus rakentaa koko kansallista turvallisuutta ja kaikki yhdessä voimme tehdä jokapäiväisestä arjesta turvallisempaa.

Toivoisin, että ymmärtäisimme, että ei ole pelkästään kyse yhdestä sähköpostitilistä, joka menetettiin vaan se voi olla osa jotain suurempaa, ja voidaan yrittää hyödyntää jossakin vaiheessa suurempaan hyökkäykseen. Emme onneksi ole kybersodan kynnyksellä täällä Suomessa, mutta tällaisia esimerkkejä on noussut Ukrainasta, ja toivon että se herättelee ihmisiä arvostamaan omaa jokapäiväistä turvallisuutta.

Laura Palovuori
Hei, tämmöinen kevennys tähän loppuun!

Helinä Turunen
Mielestäni hyvin tärkeätä, koska nämä asiat eivät ole tyhjiössä, vaan kaikki asiat liittyvät toisiinsa. Arkipäiväinen turvallisuus on mielestäni tärkeä laittaa siihen kontekstiin. Eli tällainen pikku loppukaneetti minun osaltani tähän.

Laura Palovuori
Tästä sai työkaluja myös omaan argumentointiin, kun alkaa puhua ihmisten kanssa, jotka eivät tiedä mistä on kyse. Tämä oli hyvä.

Helinä Turunen
Erinomaista.

Tom Tuunainen
Ja vieraana oli Elina Turunen, kyberturvallisuuskeskuksesta. Kiitos meidän puolestamme.

Laura Palovuori
Kiitos oikein paljon tästä.

Helinä Turunen
Kiitos oikein paljon myös teille ja kyberturvallista arkea meille kaikille.