Cyberwatch Finland

VIIKKOKATSAUS
VIIKKO 12/2024

”KYBERTURVALLISUUS SYNTYY PIENISTÄ TEOISTA JA KOKONAISUUDEN HALLINNASTA”

Cyberwatch Finland

KEY TAKEAWAYS

1. Gazan konfliktissa Hamasin rooli kyberympäristössä on pienentynyt. Sen sijaan Iran on ottanut päävastustajan roolin Israelia vastaan käytävässä kybersodassa.

2. Kyberresilienssi on merkittävä osa organisaation kokonaisresilienssiä. Se käsittää erityisesti kyvyn ennakoida, sietää ja toipua häiriötilanteista.

3. Lahjakorttihuijaus on yleinen kyberrikoksen muoto. Alustajäteiltä on alettu vaatia aiempaa kovempia toimia ilmiön torjumiseksi.

1. GAZAN KYBERKONFLIKTI JATKUU

Viime viikolla Googlen tietoturvayhtiö Mandiant kertoi tarkkailunsa kohteena olevan UNC1549-nimisen hakkeriryhmittymän viimeaikaisesta toiminnasta. Yhtiön mukaan kyseessä on lähes varmasti Iranin valtiollinen uhkatoimija eli APT-ryhmä. Ryhmä on viime aikoina toteuttanut laajoja tiedonkeräys- ja vakoilukampanjoita, joiden kohteina ovat olleet Lähi-Idän valtiot ja erityisesti Israel. Osassa toimintaa on hyödynnetty suoraan käynnissä olevaa Israelin ja Hamasin välistä konfliktia, ja tietoa on pyritty keräämään etenkin puolustus- ja ilmailualan toimijoista. Operaatio on monella tavalla hyvä kuvaus siitä, mitä konfliktin kyberrintamalla tällä hetkellä tapahtuu. Rintama on ollut erittäin aktiivinen koko sodan ajan ja etenkin Israelia kohtaan tapahtuva kybervaikuttaminen on kasvanut tasaisesti viime kuukausien kuluessa.

Suurinta osaa kyberiskuista ei kuitenkaan ole toteuttanut Hamas tai siihen suoraan liittyvät toimijat (jotka olivat kuitenkin huomattavan aktiivisia ennen itse sodan alkua), vaan nimenomaan iranilaiset hakkeriryhmät. Vaikuttaa siltä, että Hamasin ”roolin” konfliktin kyberympäristössä on ottanut Israelin vanha vastustaja Iran. Vaikka maiden välinen kyberkamppailu ja molemminpuoliset hyökkäykset ovat olleet arkipäivää jo vuosien ajan, on Gazan konflikti selvästi kiihdyttänyt tätä toimintaa. Heti sodan alettua iranilaiset hakkerit riensivät Hamasin tueksi. Mielenkiintoista kyllä, nämä alkuvaiheen iranilaiset operaatiot vaikuttivat varsin heikkotasoisilta ja huonosti valmistelluilta. On mahdollista, että tämä johtui esimerkiksi siitä, että ryhmät eivät olisi saaneet etukäteen tietoa tulevasta hyökkäyksestä ja joutuivat siksi kiireesti toteuttamaan iskuja ilman kunnon valmistelua. Toinen syy voi olla se, että valmistellut iskut olisivat voineet nimenomaan paljastaa kiinteän yhteistyön Iranin valtiollisten hakkeriryhmien ja Hamasin välillä. Alun jälkeen iskujen taso on kasvanut, mutta merkittäviin vaikutuksiin ei Israeliin kohdistuvassa vaikuttamisessa ole silti päästy.

Myöskään Israel ei ole jäänyt tuleen makaamaan, vaan on panostanut merkittävästi omaan puolustuskykyynsä ja samalla tehnyt hyökkäyksiä niin Hamasia kuin että Iraniakin vastaan. Hamasiin kohdistuvat hyökkäykset ovat kuitenkin vähemmän huomion arvioisia, sillä järjestöllä ei kybermaailmassa ole paljoa iskettäviä kohteita. Tämänkin takia suurin osa vaikuttamisesta on kohdistunut nimenomaan kyberympäristön vastustajaksi noussutta Irania kohtaan. Merkittävin Irania vastaan iskenyt ryhmä on Gonjeshke Darande (tunnetaan myös englanninkielisellä nimellä Predatory Sparrow) – niminen toimija, joka on yleisesti tunnistettu yhdeksi Israelin valtioon liitetyistä ulkomaille iskevistä ryhmittymistä. Samainen ryhmä on aiemminkin kohdistanut vaikuttamista Iraniin. Kohteina ovat olleet esimerkiksi maan joukkoliikenne sekä valtion omistuksessa olevat terästehtaat. Joulukuussa ryhmä onnistui lamauttamaan valtaosan, oman ilmoituksensa mukaan 70 %, Iranin polttoaineasemista, aiheuttaen huomattavia polttoaineen jakeluvaikeuksia. Suorien hyökkäyksien lisäksi Israel myös varmasti tukee fyysiseen sotaan liittyviä tiedusteluoperaatioita ja muita hankkeita kyberympäristöä hyödyntäen, vaikka näistä ei juuri julkisuuteen hiiskutakaan.

Kyberympäristössä käydäänkin jatkuvaa ja molemminpuolista kamppailua. Viimeisten viikkojen aikana on alkanut vaikuttaa siltä, että etenkin Iranin huomio on siirtynyt itse Israelista tätä tukeviin valtioihin tai toimijoihin. Myös tästä kertoo hyvin aiemmin mainittu Mandiantin tunnistama kampanja, jossa päähuomio ei ollut enää pelkästään Israelissa, vaan kohteita etsittiin laajemmin lähialueilta. Samankaltaiseen tulokseen on tullut myös kyberkonfliktia analysoinut Microsoft, joka helmikuisessa analyysissaan on päätynyt jakamaan Israelin ja Hamasin välisen kyberkonfliktin kolmeen selkeään vaiheeseen. Ensimmäiseen näistä kuuluvat alkuvaiheen reaktiiviset ja huonosti valmistellut hyökkäykset Israelia kohtaan ja toinen vaihe käsitti kiihtyvät molemminpuoliset kyberiskut Israelin ja Iranin välillä. Kolmas, nyt käynnissä oleva vaihe, on sodan leviäminen, ja etenkin Iranin vaikuttamisen kohdentuminen vastapuolen liittolaisiin ja tukijoihin.

On vaikea arvioida, miksi Iran on päätynyt siirtämään huomiotaan Israelista muualle. Yksi mahdollinen syy on se, että tähän mennessä Israeliin kohdistuvilla operaatiolla ei ole päästy merkittäviin vaikutuksiin. Israelin kyberpuolustusta voidaan pitää yhtenä maailman parhaimmista. Sillä on lisäksi vuosien kokemus Iranilaisen vaikuttamisen kohteena olemisesta, minkä lisäksi panostusta kyberpuolustukseen on varmasti lisätty konfliktin kuluessa. Näistä syistä liittolaisiin kohdistuvissa iskuissa on kenties potentiaalia parempaan menestykseen.

Toinen mielenkiintoinen arvioitava seikka on se, miten kyberkonflikti tästä jatkuu. On erittäin todennäköistä, että Israelin laajoja strategisia tavoitteita tukevat operaatiot jatkuvat yhä suljettujen ovien takana. Epävarmempaa on, kuinka laajalle Iran pyrkii omaa vaikuttamistaan levittämään, ja kuinka menestyksekkäitä operaatioita se onnistuu toteuttamaan. On hyvä muistaa, että Iranilla itselläänkin on kybermaailmassa jonkinasteinen liittolainen. Maan hakkeriryhmät ovat tehneet jo pitkään yhteistyötä venäläisten uhkatoimijoiden kanssa. Venäjän kyberresurssien voi arvella olevan tällä hetkellä melko kiinni omissa operaatioissa, mutta mahdollinen tiedonjakaminen tai yhteistyön kehittyminen voi silti olla huolestuttavaa, vaikka selkeitä merkkejä siitä ei olisikaan havaittu.

2. RESILIENSSI OSANA KYBERTURVALLISUUTTA

Resilienssistä on tullut moderni muotisana ja sitä käytetään useissa eri yhteyksissä. Poliittisissa puheissa voidaan viitata muun muassa yhteiskunnalliseen resilienssiin ja yritysmaailmassa puhutaan organisaation resilienssistä. Lisäksi muun muassa taloudellisen tai ekologisen resilienssin käsitteet ilmaantuvat ajoittain julkiseen keskusteluun. Resilienssi-liite voidaan nykyään lisätä lähes kaikkiin mahdollisiin elämänalueisiin, joilla voi sattua usein ulkoisista tekijöistä johtuvia ei-toivottuja tapahtumia. Termiä käytetään myös kyberturvallisuudessa: puhutaan organisaation tai yhteiskunnan kyberresilienssistä. Mitä sanan taakse lopulta kätkeytyy?

Resilienssi on käsitteenä liukas eikä sille ole yhtä hyväksyttyä määritelmää tai viitekehystä olemassa. Se tekee myös käsitteeseen liittyvän keskustelun joskus hankalaksi. Yrityksiä määritellä resilienssiä on kuitenkin ollut. Suomessa käsitettä on yrittänyt määritellä esimerkiksi puolustusministeriön yhteydessä toimiva Turvallisuuskomitea, joka on varautumiseen keskittyvä yhteistyö- ja asiantuntijaelin. Sen julkaiseman Kyberturvallisuuden sanaston mukaan resilienssillä tarkoitetaan ”yksilöiden ja yhteisöjen kykyä ylläpitää toimintakykyä muuttuvissa olosuhteissa sekä valmiutta kohdata häiriöitä ja kriisejä ja palautua niistä”. Turvallisuuskomitea liittää käsitteen muun muassa kriisinkestävyyden ja kriisinsietoisuuden termeihin. Kyse on kuitenkin edellä mainitun lisäksi myös paljon muusta, kuten esimerkiksi joustavuudesta ja sopeutumiskyvystä.

Kyberresilienssillä taas voidaan tarkoittaa muun muassa kykyä ennakoida, sietää ja toipua kyberhyökkäyksistä. Resilienssi voi näkyä sekä proaktiivisina eli ennakoivina toimenpiteinä, että reaktiivisina toimina, jotka otetaan käyttöön kyberhyökkäysten osuessa kohdalle. Kyberuhkan konkretisoituessa kyse ei ole pelkästään tietojen ja järjestelmien palauttamisesta tapahtumaa edeltäneeseen tai sitä parempaan tilaan. Kyse on myös sopeutumisesta uuteen uhkamaisemaan, mikä näkyy esimerkiksi uusien kyberhyökkäystapojen ja uhkatoimijoiden tunnistamisessa. Ajantasaisen tilannekuvan ylläpitämistä ei voikaan liikaa korostaa ja se on tärkeä pilari organisaation kyberresilienssiä rakennettaessa.

Kyberresilienssin osa-alueita

Ennakointi: Ajantasainen tilannekuva, henkilöstön koulutus ja ohjeistus, riskiarvioinnit ja auditoinnit, testaustoiminta

Sietokyky: Palomuurit ja muut teknisen tietoturvan toimenpiteet, varmuuskopiot ja varajärjestelmät, harjoittelu häiriötilanteiden varalle ja toimenpiteiden jalkauttaminen kriisissä, kriisijohtaminen ja -viestintä

Toipuminen: Vahinkojen rajaaminen ja korjaaminen, tapahtuman selvitys, virheistä oppiminen ja kyberturvan kehittäminen

Yksiselitteisiä keinoja mitata kyberresilienssiä tai muutakaan resilienssiä ei ole. Kuitenkin esimerkiksi Maailman talousfoorumi WEF on julkaissut oman ehdotuksensa kyberresilienssin mittaamiseksi. Se on kehittänyt niin kutsutun kyberresilienssi-indeksin, joka on organisaatioiden vapaasti käytettävissä ja saatavissa järjestön verkkosivuilta. Indeksitulokseen vaikuttaa muun muassa organisaation henkilöstölle tarjoama koulutus, riskiarviointien toteuttaminen sekä haavoittuvuuspinta-alan tunnistaminen ja vähentäminen.

Kyberalan ulkopuolella sovellutuksia on resilienssin mittaamiseksi on tehty enemmän. Esimerkiksi Norjassa kuntien resilienssiä on tutkittu useiden asioiden, kuten esimerkiksi sosiaalisten, taloudellisten, ympäristöllisten sekä infrastruktuurillisten tekijöiden avulla. Lisäksi on olemassa niin kutsuttu kriittisen infrastruktuurin resilienssi-indeksi (CIRI), jossa resilienssiä mitataan seitsemän eri vaiheen, kuten riskinarvioinnin, ennaltaehkäisyn, reagoinnin ja toipumisen avulla. Mallissa kullekin vaiheelle asetetaan yleisiä sekä toimijakohtaisia indikaattoreita kypsyysasteikolla 0–5, joka myöhemmin lasketaan yhteen toimijan kokonaisresilienssiksi. Vaikka yhtä oikeaa tapa mitata tai laskea organisaation resilienssiä tai kyberresilienssiä ei ole, sen määrällinen mittaaminen voisi kuitenkin luoda pohjan heikkouksien tunnistamiseksi ja resilienssin tason kohottamiseksi.

Cyberwatch Finland

Organisaatiolle kyberresilienssin merkitys korostuu osana organisaation kokonaisresilienssiä ja linkittyy osittain perinteiseen riskienhallintaan, joskin resilienssi on standardisoitua riskienhallintaa laajempi käsite. Käsitteeseen sisältyy myös yllätyksen mahdollisuus - kaikkea ei voida ennakoida tai tunnistaa hienoimmissakaan riskienhallintaskenaarioissa. Käsitteellisen kikkailun ja semanttisen väittelyn sijaan olisikin aiheellista tunnistaa kyberturvallisuuden merkitys organisaation päivittäistoiminnassa, samoin kuin sen laajempi strateginen merkitys organisaation toiminnalle kokonaisuutena. Tärkeä osa organisaation kokonaisresilienssiä on myös sen työntekijöiden henkilökohtainen resilienssi, joka on yksilöllistä kykyä selviytyä ja toipua haastavista tilanteista.

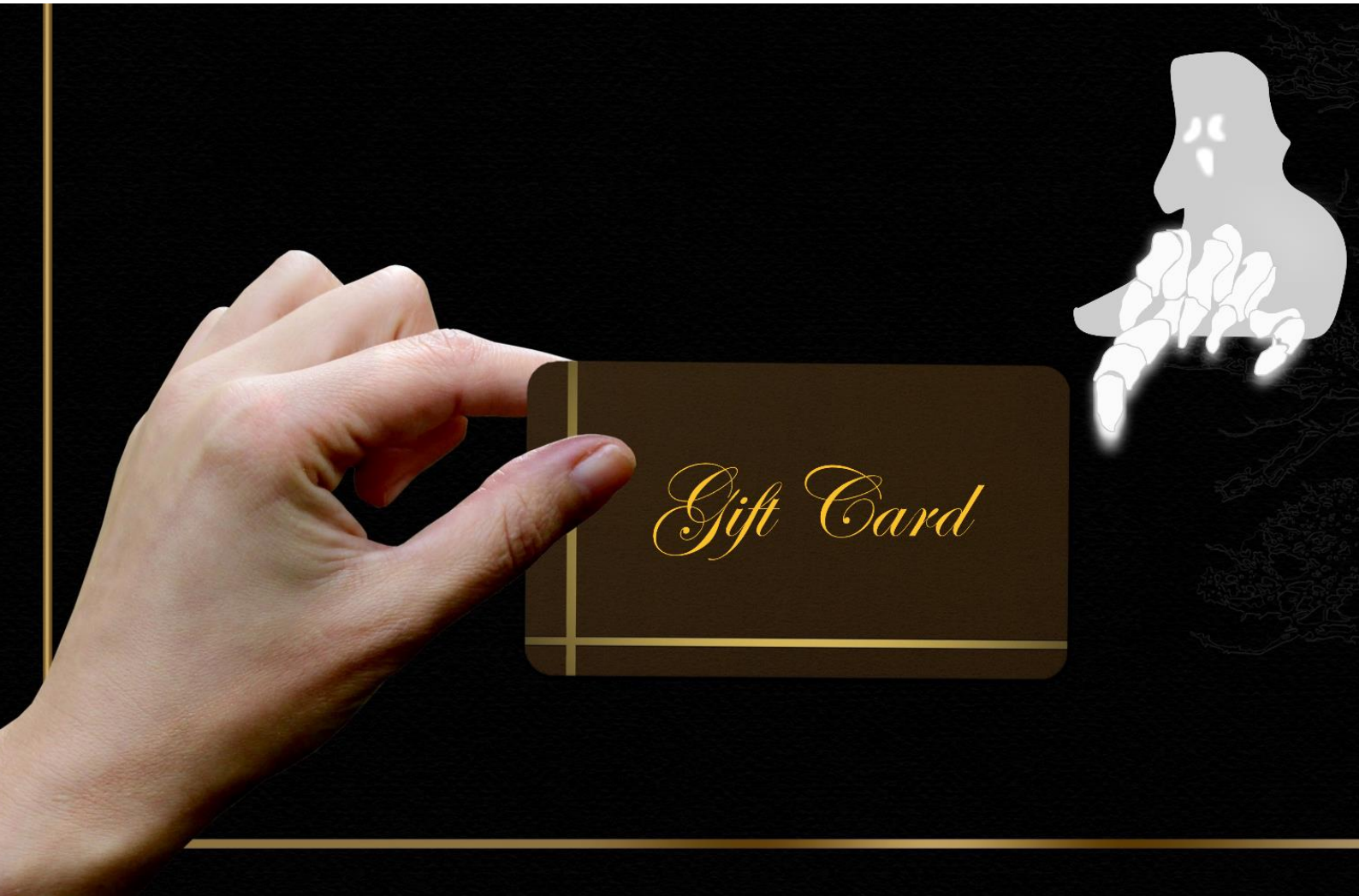
Cyberwatch Finland

3. LAHJAKORTTIHUIJAUKSET ON MERKITTÄVÄ ILMIÖ

Eräs matalan tason kyberrikollisuudessa paljon käytetty työkalu on erilaiset lahjakortit. Kyberhuijarit pyrkivät sosiaalisen manipulaation keinoin saamaan uhrin ostamaan lahjakortin ja luovuttamaan sen tiedot huijarille. Vaikka kyberuhkista perillä olevan korvaan saattaa kuulostaa oudolta, että joku menisi ostamaan lahjakortin ulkomaisen huijarin ohjeistamana ja päätyisi vielä luovuttamaan kortin tiedot tämän haltuun, on kyseessä silti yleinen ja tehokas tapa siirtää rahaa uhreilta huijareille. Käytännössä syitä, joilla huijari lahjakorttitarpeen perustelee, on lähes rajaton määrä.

Eräs suosittu tapa toteuttaa huijaus on tekeytyä Googlen tukipalveluksi ja uskotella uhrille, että tällä on maksamattomia, perintään menossa olevia laskuja, jotka tulisi hoitaa mahdollisimman pian. Nopeaksi vaihtoehdoksi voidaan tarjota “suoraan Googlelle” tulevaa maksua eli Google-kaupan lahjakortin ostamista. Tilanteessa korostetaan usein -sosiaaliselle manipulaatiolle tyypillisesti- kiirettä. Uhri saattaa luulla olevansa vaikeuksissa, joista luotettavaksi tekeytynyt huijari osaa auttaa pois. Lahjakorttitietoja kaapataan myös paljon erilaisten kalastelusivustojen kautta. Nämä jäljittelevät oikeita verkkokauppa-alustoja, mutta niille syötetyt tiedot päätyvät huijarin haltuun. Tämänkaltaiset huijaukset yleistyvät aina etenkin joulun ja muiden juhlapyhien aikaan, ja niiden uskottavuus kehittyy jatkuvasti rikollisten tekniikoiden parantuessa.

Huijauksen kohteena voi olla sekä fyysinen että digitaalinen lahjakortti, sillä molemmista löytyy numerosarjoja ja tunnuslukuja, joiden avulla lahjakortille ladattu summa voidaan käyttää ostosten maksamiseen. Käytännössä lahjakortit toimivat valuutansiirron välineenä. Huijareiden kannalta ne ovat hyvä väline monesta eri syystä. Ensinnäkin, koska varsinaisesti mitään ”valuuttaa” ei siirry esimerkiksi pankkitililtä toiselle, on rahoja hyvin vaikea jäljittää ja palauttaa uhreille, vaikka huijaus myöhemmin paljastuisikin. Toiseksi, koska mukana ei ole virallisia pankkeja, joiden kanssa uhri asioi, riski siihen, että joku varoittaa tätä mahdollisesta huijauksesta, on pienempi. Kolmanneksi: sen lisäksi, että rahoja on vaikea jäljittää, myös ne haltuun saanut huijari on vaikea saada kiinni. Vaikka uhri ymmärtäisikin tulleensa huijatuksi ja ilmoittaisi huijareiden haltuun saamien lahjakorttien numerot lahjakortin myöntäjälle, on pelkästään niiden avulla hyvin vaikea tavoittaa itse huijareita. Suurten alustojen kuten Google-kaupan, Amazonin tai Applen lahjakortit toimivat ympäri maailman. Ne voidaan joko käyttää itse tai myydä nopeasti eteenpäin, jolloin jäljittäminen on entistä vaikeampaa.



Cyberwatch Finland

Yhdysvaltojen kauppakomission FTC:n mukaan pelkästään Yhdysvalloissa lahjakorttien avulla huijatut summat pyörivät sadoissa miljoonissa dollareissa vuositasolla. Esimerkiksi vuonna 2021 pelkästään Googlen lahjakortteja käytettiin huijauksissa 17 miljoonan dollarin edestä. Applen vastaava luku oli 16 miljoonaa, mutta selkeästi kärkipaikalla oli kuitenkin kauppaketju Target, jonka lahjakortteja käytettiin huijauksissa 35 miljoonan dollarin edestä. Huijausten määrä on myös kasvava. Tämä ei tosin välttämättä kieli nimenomaan lahjakorttihuijausten suosion kasvusta, vaan pikemminkin yleisestä kyberhuijausten kasvusta.

Lahjakorttihuijauksissa tulisi pohtia myös kauppaketjujen ja eri alustojen vastuuta ilmiön torjumisessa. Arvioiden mukaan lahjakorttien katteet ovat hyviä ja esimerkiksi Googlen ja Applen tapauksissa alustanhaltija saa jopa 15–30 % kaikista lahjakorteilla tehdyistä ostoksista. Näin ollen alustajätit, ainakin välillisesti, hyötyvät tästä rikosilmiöstä. Niitä vastaan on myös nostettu oikeusjuttuja. Maaliskuun alussa Kaliforniassa Googlea vastaan nostettiin kanne, jossa sen toimenpiteitä ilmiön torjumiseksi moitittiin vähäisiksi. Valituksen mukaan Google ei esimerkiksi palauta lahjakorttien avulla tehtyjä maksuja tai menetettyjä lahjakortteja. Lisäksi sitä on kritisoitu tarpeellisten varoitusten ja riskien mainitsemisen riittämättömyydestä. Samankaltainen kanne oli jo tammikuussa nostettu Applea vastaan, mutta se soviteltiin lopulta oikeussalin ulkopuolella.

Toisaalta voidaan kysyä, millaiset toimet ilmiön estämiseksi lopulta olisivat riittäviä. Esimerkiksi Google varoittaa lahjakorttihuijauksista sekä verkkosivuillaan että tukipalvelussaan. Myös Apple-tuessa on oma osionsa huijausilmiölle. Molemmilla toimijoilla on myös fyysisten lahjakorttien yhteydessä varoitus mahdollisista huijauksista. Toimenpiteitä on siis tehty, mutta syystä tai toisesta lahjakorttihuijausten määrä on edelleen suuri. Yksi syy tähän voi olla, että estotoimet ovat usein huijareiden tiedossa. Kun uhria manipuloidaan ostamaan kortteja, tälle usein kerrotaan näistä varoituksista etukäteen, mikä voi vähentää niiden vaikuttavuutta. Lisäksi kun vastakkain asetetaan puhelimen päässä, kenties juuri Googlen tukihenkilönä esiintyvä huijari, joka jo on saavuttanut uhrin luottamuksen, ja lyhyt tekstinpätkä kaupan seinällä, ei liene yllättävää, että varoitusten vaikutus jää pienehköksi.

Parempi ratkaisu olisikin tietoisuuden lisääminen etukäteen ja selkeämmät ja näkyvämmät ohjeet, joissa ilmaistaisiin, että yksikään virallinen taho ei käytä lahjakortteja maksuvälineenä. Käytännöllistä hyötyä olisi esimerkiksi siitä, että jokaisen lahjakorttiostoksen yhteydessä tulisi ostajan vastattavaksi kysymys siitä, onko joku entuudestaan tuntematon taho kehottanut kortin ostamiseen. Kaikkea vastuuta ei kuitenkaan voida vierittää pelkästään yhtiöiden vastuulle, vaan vastuu on myös ostajalla itsellään. Sen vuoksi kansalaisten digitaitojen kehittäminen sekä jatkuva tiedottaminen erilaisista kyberhuijauksista ja -petoksista voisi toimia välineenä ilmiön rajaamisessa. Kyberrikollisuuden hinta yksilöille ja yhteiskunnalle on vuositasolla suuri eikä ongelma tule tulevaisuudessa ainakaan pienentymään.

LÄHTEET

1. Gazan kyberkonflikti jatkuu

https://www.mandiant.com/resources/blog/suspected-iranian-unc1549-targets-israel-middle-east
https://blog.google/technology/safety-security/tool-of-first-resort-israel-hamas-war-in-cyber/
https://www.darkreading.com/threat-intelligence/hamas-cyberattacks-ceased-after-october-7-attack-but-why
https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/
https://www.reuters.com/world/middle-east/software-problem-disrupts-iranian-gas-stations-fars-2023-12-18/
https://www.wired.com/story/predatory-sparrow-cyberattack-timeline/

2. Resilienssi osana kyberturvallisuutta

https://csrc.nist.gov/glossary/term/cyber_resiliency
https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf?file=pdf/Kyberturvallisuuden_sanasto.pdf
https://www.sciencedirect.com/science/article/pii/S2212420918312032
https://www.weforum.org/publications/the-cyber-resilience-index-advancing-organizational-cyber-resilience/
Pursiainen, Christer (2023): "Resilienssin ulottuvuudet". *Kosmopolis,* 4/2023, 30–54

3. Lahjakorttihuijaukset ovat merkittävä ilmiö

https://play.google/giftcards/
https://support.apple.com/fi-fi/gift-card-scams
https://support.google.com/googleplay/answer/9057338?hl=en
https://www.theregister.com/2024/03/07/google_sued_for_profiting_gift_card_fraud/
https://www.ftc.gov/business-guidance/blog/2021/12/gift-card-scams-out-shadows-ftc-data-spotlight
https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2021/12/scammers-prefer-gift-cards-not-just-any-card-will-do

Kuvat: Pixabay

Cyberwatch Finland