Cyberwatch Finland

VIIKKOKATSAUS
VIIKKO 11/2024

”KYBERTURVALLISUUS SYNTYY PIENISTÄ TEOISTA JA KOKONAISUUDEN HALLINNASTA”

Cyberwatch Finland

KEY TAKEAWAYS

1. Kybersolidaarisuusasetuksella pyritään parantamaan EU:n kyberresilienssiä ja jäsenvaltioiden välistä yhteistyötä. Se on jatkumoa EU:n muulle kybersääntelylle, kuten NIS2-direktiiville sekä kyberkestävyyssäädökselle.

2. Onnistunut tiedonhallinta on voimavara organisaation kyberturvallisuudessa ja auttaa ongelmatilanteiden selvittämisessä.

3. Roskaposti- ja huijausviestien viime aikojen trendinä on ollut hyökkäyssyklien nopeutuminen, minkä lisäksi zip-tiedostot ovat edelleen suosittu tapa toimittaa haittaohjelma uhrille.

1. EU:N KYBERSOLIDAARISUUSASETUS SAI POLIITTISEN HYVÄKSYNNÄN

Euroopan unioni on lisäämässä kyberturvallisuuden sääntelyä jälleen uudella asetuksella. Komission huhtikuussa 2023 tekemä aloite kybersolidaarisuusasetuksesta (Cyber Solidarity Act, CSA) sai viime viikolla poliittisen hyväksynnän Eurooppa-neuvosto eli valtioiden päämiehistä koostuvan toimielimen sekä Euroopan parlamentin välisissä neuvotteluissa. Seuraavaksi asetusehdotus etenee Euroopan parlamentin ja neuvoston virallisesti hyväksyttäväksi, jonka jälkeen se astuu voimaan EU:n asetusprosessin mukaisesti. Asetukset ovat sitovia säädöksiä, joita on sovellettava kaikilta osin ja sellaisenaan EU:n jäsenmaissa. Ne siis eroavat merkittävästi direktiiveistä, joiden kohdalla jäsenmaat saavat itse päättää miten EU:n asettamaan tavoitteeseen päästään. Mistä kybersolidaarisuusasetuksessa on kyse?

Euroopan komission mukaan asetuksen tavoitteena on EU:n kyberresilienssin eli sieto- ja palautumiskyvyn parantaminen. Samalla sen toivotaan edesauttavan jäsenmaiden välistä solidaarisuutta ja EU:n kykyä tunnistaa, varautua ja vastata kyberuhkiin. Käytännössä asetus tuo EU:lle kolme uutta toimintoa. Ensimmäinen näistä on koko unionin kattava kyberturvallisuushälytysjärjestelmä (European Cybersecurity Alert System). Sen tehtävänä on havaita kyberuhkia ja tarjota reaaliaikaista tilannekuvaa viranomaisille ja muille relevanteille toimijoille. Hälytysjärjestelmä koostuisi jäsenvaltioiden ylläpitämien SOC-keskusten (Security Operations Centre) verkostosta, joka tunnistaisi ja jakaisi uhkatietoutta yli rajojen. Toiseksi asetuksella luodaan hätämekanismi (Cybersecurity Emergency Mechanism), jonka tarkoitus olisi parantaa valmiuksia reagoida merkittäviin ja laajoihin kybertapahtumiin. Mekanismi koostuu kolmesta osiosta: varautumisesta kriittisillä sektoreilla, niin kutsutun ”kyberturvallisuusreservin” perustamisesta sekä jäsenvaltioiden taloudellisesta tuesta merkittävän tai laajamittaisen kyberonnettomuuden kohteeksi joutuneelle valtiolle.

Kolmanneksi asetuksella luodaan mekanismi kybertapahtumien jälkiarvioille (European Cybersecurity Incident Review Mechanism). Sen avulla olisi tarkoitus tarkastella ja arvioida tapahtumia niiden jälkeen ja antaa arvioon perustuvia suosituksia EU:n kyberturvallisuuden parantamiseksi. Tässä merkittävä rooli olisi Euroopan kyberturvallisuusvirasto ENISAlla, joka tuottaisi raportin siitä, mitä tapahtumasta voidaan oppia ja millaisia suosituksia kyberturvallisuuden kehittämiseksi voidaan tehdä.

Vaikka uudistus vaikuttaa olevan pikemminkin kansallisvaltioille suunnattua toimintaa, on siinä sisällä myös yksityisiä yrityksiä koskevia osuuksia. Tällainen on esimerkiksi edellä mainittu ajatus ”kyberturvallisuusreservistä”, jossa yksityisen sektorin ”luotettavat toimijat” olisivat valmiita toimimaan jäsenvaltion, EU:n toimielimen, viraston tai sopimuskumppanina olevan EU:n ulkopuolisen maan pyynnöstä laajamittaisen kyberturvallisuushäiriön aikana. Lisäksi hätämekanismissa mainitut valmiustoimet sisältävät erittäin kriittisillä sektoreilla toimivien tahojen valmiuden koordinoitua testaamista. Suomessa on jo hyvä yhteistyö viranomaisten ja yritysten kesken, toisin kuin monissa muissa EU-maissa.

Asetus on jatkoa EU:n muille kyberturvallisuutta käsitteleville säädöksille, kuten esimerkiksi NIS2-kyberturvallisuusdirektiiville sekä kyberkestävyyssäädökselle (Cyber Resilience Act), joista jälkimmäisen tarkoituksena on varmistaa digitaalisten tuotteiden ja niiden oheistuotteiden kyberturvallisuus. Kybersolidaarisuusasetuksen vaikuttavuudesta on toistaiseksi hankala tehdä arvioita – taustalla oleva ajatus yhteistyöstä, solidaarisuudesta, uhkatietoisuuden jakamisesta ja virheistä oppimisesta on tietysti kannatettava. Paljon riippuu käytännön toteutuksesta sekä siitä, kuinka yhteistyö tosiasiallisesti saadaan toimimaan. Kriittisin silmin tarkasteltuna hätämekanismissa oleva optio taloudellisesta tuesta pulaan joutuneelle jäsenvaltiolle kiinnittää huomiota. Yhtenä pelkona voikin olla asetuksen muodostuminen yhdeksi tulonsiirron keinoksi unionin sisällä, jossa hyvin asiansa hoitavat jäsenmaat joutuvat huonommin hoitavien jäsenmaiden virheiden tai välipitämättömyyden maksumiehiksi. Tästä näkökulmasta ei toistaiseksi ole käyty paljon keskustelua, mutta kyberturvallisuuden tason vaihdellessa laajasti jäsenvaltioissa ja taloudellisten kysymysten ollessa jatkuva poliittinen kiistakapula unionissa, on myös se aiheellista huomioida.

2. ONNISTUNUT TIEDONHALLINTA TUKEE KYBERTURVALLISUUDEN POIKKEUSTILANTEISSA

Tiedonhallinnalla tarkoitetaan organisaation hallussa olevan tiedon pysymistä turvattuna, oikeassa paikassa ja saavutettavissa. Siihen sisältyy myös tavoite siitä, että organisaatiossa tiedetään koko ajan, missä tietoa ja dataa säilytetään, ja ettei esimerkiksi ylimääräisiä kopioita tai vanhoja versioita ole muualla kuin siellä, missä niiden kuuluu olla. Paitsi että onnistuneella tiedonhallinnalla on merkittävä vaikutus organisaation jokapäiväisen toiminnan tehostamisessa, sillä on tärkeä rooli myös kyberturvallisuuden toteutumisessa. Tiedonhallinnan merkitys korostuu erityisesti pahimman sattuessa, eli organisaation joutuessa kyberhyökkäyksen kohteeksi, kun sitä, mitä tietoa uhkatoimijan haltuun on voinut päästä, ryhdytään selvittämään.

Yhtenä esimerkkinä epäonnistuneen tiedonhallinnan vaikutuksista tietomurrossa toimii suomalainen pankki, joka joutui hyökkäyksen kohteeksi loppuvuodesta 2023. Pankilla meni aikaa kartoittaa, mihin kaikkeen tietoon hyökkääjä oli päässyt käsiksi. Tapausta selvitellessä kävi myös ilmi, että asiakastietoja oli käsitelty asiakastietojärjestelmän ohella myös työntekijöiden sähköposteissa. Tämän paljastuminen oli omiaan myös lisäämään mainehaittaa, joka pankille hyökkäyksestä koitui. Mikäli organisaatio ei puutteellisen tiedonhallinnan takia osaa riittävän ripeästi vastata siihen, onko asiakkaisiin tai yhteistyökumppaneihin liittyvää arkaluontoista tietoa päätynyt ulkopuolisiin käsiin, ei se ole omiaan lujittamaan näiden tahojen luottamusta organisaatioon. Pahimmillaan se saattaa johtaa syytöksiin, että iskun vahinkoja peitellään. Näin kävi esimerkiksi salasanahallintaan erikoistuneelle LastPass-yhtiölle, kun se vuonna 2022 joutui hyökkäyksen kohteeksi. Yhtiöllä meni useita kuukausia aikaa selvittää, mitä tietoja hyökkäyksessä oli vuotanut. Kun lopulta ilmeni, että asiakkaiden salasanoja on saattanut päätyä uhkatoimijoiden käsiin, yhtiö sai osakseen syytöksiä salailuyrityksistä ja myöhemmin sitä vastaan nostetun kanteen huonosta tietosuojasta.

Asianmukainen tiedonhallinta siis auttaa kyberhyökkäysten vahinkojen selvittämisessä. Tiedonhallinta on myös pääsyoikeuksien hallintaa. Kun tiedetään, mihin järjestelmiin ja millä oikeuksilla tunkeutujilla on ollut pääsy, tiedetään myös, mitä tietoa hyökkääjän haltuun on saattanut päätyä. Mikäli organisaatiolla on tarkka tieto siitä missä ja miten sen data on säilytetty, on se todennäköisesti myös paremmin suojattu. Kaiken perusta on tiedon luokittelu vähintäänkin kolmeen kategoriaan: julkinen, luottamuksellinen ja salainen. Luokittelun perusteella voidaan antaa ohjeet, millä välineillä mitäkin tietoa saa käsitellä ja antaa oikeudet kunkin luokan tietojen käsittelyyn vain nimetylle joukolle.

Kyberhyökkäyksiin varautumisessa tiedonhallinnassa korostuu etenkin se, että organisaatio tietää tarkkaan missä ympäristössä mitäkin dataa käsitellään, minne se tallennetaan sekä milloin ja miten se poistetaan. Pelkkä ohjeistus tämän suhteen ei kuitenkaan riitä, sillä myös sen toteutumisesta on pystyttävä pitämään huoli. Tärkeää on, että ohjeiden noudattamista valvotaan riittävästi esimerkiksi auditoinneilla. Yhtä tärkeää on, että ohjeistus on käytännössä toteuttavissa eivätkä työntekijät joudu tilanteisiin, jossa työn suorittaminen ja tiedonhallinnan ohjeistus ovat ristiriidassa. Näin voi olla esimerkiksi etätöissä, jota tekevillä voi olla houkutus tallentaa tiedostoja organisaation järjestelmäympäristöstä omille laitteilleen, jotta työskentely huononkin verkkoyhteydenkin kanssa onnistuu. Vaikka yksittäistapaukset eivät sinänsä tuota ongelmaa tiedonhallinnan kokonaisuudelle, voivat jatkuvat väärät toimintamallit aiheuttaa ylimääräisiä ja turhia riskejä.

Suomessa julkishallinnon toimijoita velvoittaa tiedonhallintalaki, jossa määritellään vähimmäisvaatimukset tiedon käsittelyyn ja suojaukseen. Lakia voivat käyttää ohjenuorana myös organisaatiot, jota se ei suoranaisesti koske. Lakitekstejä lukiessa on kuitenkin hyvä muistaa, että niissä määritellään yleensä nimenomaan vähimmäisvaatimukset, eli taso, jolle ainakin on päästävä. Omaa tiedonhallintaa suunnitellessa kannattaa tähdätä ylemmäs, sillä se voi paitsi erottaa kilpailijoista myös auttaa vahinkojen rajaamisessa kyberhyökkäyksen sattuessa.

3. ROSKAPOSTI- JA HUIJAUSVIESTIT PYSYVÄT SUOSIOSSA

Roskaposti- ja huijausviestit ovat yleinen arkipäivän riesa. Ne muodostavat merkittävän osan kaikista lähetetyistä sähköpostiviesteistä. Yleisempien arvioiden mukaan ne käsittävät 40–50 prosenttia kaikista viesteistä, vaikka myös korkeampia arvioita on esitetty. Huijausviestejä lähetetään myös sosiaalisen median palveluissa, minkä lisäksi huijauspuhelut ovat huomattava ilmiö. Vaikka roskaposti- ja huijausviestien ajatellaan usein olevan ilmiselvä ja pieni tietoturvauhka, niiden suuren määrän vuoksi joku aina päätyy uhriksi. Teknologiayhtiö IBM julkaisi helmikuun lopussa artikkelin vuoden 2023 trendeistä roskaposti- ja huijausviestien osalta. Myös useat tietoturvatoimijat ovat julkaisseet omia raporttejaan aiheesta. Niiden valossa huijausviestit elävät ja voivat hyvin.

Huijausviestien tavoitteena voi olla esimerkiksi sosiaalisen manipuloinnin avulla saada luotua kontakti uhriin ja myöhemmin huijattua rahaa tai esimerkiksi verkkopankkitunnuksia. Toinen tavoite voi olla haittaohjelman ujuttaminen uhrin tai uhriorganisaation tietojärjestelmiin, minkä kautta arvokkaisiin tietoihin päästään käsiksi. Tämä voi tapahtua esimerkiksi sähköpostissa olevien linkkien tai liitetiedostojen avulla. Yhdysvaltalaisen kyberturvallisuusyhtiö Vipren raportin mukaan 71 prosenttia tapauksista saa alkunsa linkeistä, liitetiedostoista on kyse 22 prosentissa tapauksista ja loput tapaukset käsittävät muita hyökkäysmuotoja, kuten esimerkiksi QR-koodeja.

Linkkihuijauksen avulla uhri usein ohjataan haitalliselle verkkosivulle. Linkit voivat myös sijaita kohteissa ja asiayhteyksissä, jotka kiinnostavat ihmisiä. Tällaisia ovat esimerkiksi mainokset. Pyrkimyksenä on saada uhri syöttämään linkin takana olevalla sivustolla sellaisia henkilö- ja muita tietoja, joita sivuston pahantahtoinen toimija voi myöhemmin hyödyntää.

Liitetiedostojen avulla toimitetuista haittaohjelmista Vipre korostaa html-tiedostojen suosiota hyökkäysmuotona. Toisaalta IBM:n mukaan edelleen suosituin tapa haittaohjelman toimittamiseen uhrin tietokoneelle on zip-pakkaustiedosto. Tiedostomuotoa merkittävämpää on kuitenkin sen tiedostaminen, että epämääräisiä tai tuntemattomalta lähettäjältä tulevia liitetiedostoja ei tulisi missään nimessä avata.

Yleisiä roskaposti- ja huijausviestien trendejä tarkastellessa huomio kiinnittyy myös hyökkäyssyklien nopeutumiseen. IBM:n artikkelissa esille on nostettu esimerkiksi OneNote-tiedostojen kautta levitettyjen haittaohjelmien suuri piikki vuoden 2023 puolivälissä ja sen jälkeinen dramaattinen lasku. Uhkatoimijat vaikuttavatkin olevan aiempaa ketterämpiä hyödyntämään haavoittuvuuksia ja nopeita myös muuttamaan toimintaansa, mikäli tietty hyökkäysmuoto menettää tehonsa. Yksi tehonsa menettänyt hyökkäysmuoto on muun muassa makrotiedostojen hyödyntäminen kyberhyökkäyksissä. Makro on sarja komentoja, joita käytetään toistuvan tehtävän automatisoinnissa ja esimerkiksi Excel-tiedostojen mukana toimitettujen makrojen käyttäminen on aiemmin ollut yleinen hyökkäystapa. IBM:n mukaan tämän hyökkäystavan suosiossa laskua oli vuonna 2023 jopa 93 prosenttia verrattuna edelliseen vuoteen.

Tulevaisuudessa roskapostien ja huijausviestien määrä ja laatu todennäköisesti kasvavat. Taustalla vaikuttaa muun muassa tekoälyn kehitys. Sen on arveltu tekevän huijausviesteistä aiempaa uskottavimpia. Myös syväväärennösten (deep fake) kehitys pakottaa pohtimaan aiempaa tarkemmin vastaanotettujen viestien luotettavuutta. Keinoja roskaposti- ja huijausviesteiltä suojautumiseen on monia. Organisaatiot voivat ottaa käyttöönsä teknisiä toimia roskaposti- ja huijausviesteiltä välttymiseen. Tällainen on muun muassa roskapostisuodattimien käyttöönotto tai niiden suojaustason muuttaminen. Suositeltavaa olisikin neutralisoida uhka jo ennen kuin se tavoittaa kohteensa. Ihmiset ovat perinteisesti olleet kyberturvallisuuden heikoin lenkki. Teknisten toimien ohella yleinen uhkatietoisuus sekä henkilöstön koulutus ja organisaation hyvät yleiset kyberhygieniakäytännöt ovatkin avainasemassa uhkan torjunnassa ja siihen varautumisessa.

LÄHTEET

1. EU:n kybersolidaarisuusasetus sai poliittisen hyväksynnän

https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1332

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0209

https://therecord.media/europe-cyber-solidarity-act-agreement

https://www.consilium.europa.eu/en/press/press-releases/2024/03/06/cyber-solidarity-package-council-and-parliament-strike-deals-to-strengthen-cyber-security-capacities-in-the-eu/

https://www.infosecurity-magazine.com/news/eu-cyber-solidarity-incident/

https://www.tivi.fi/uutiset/tv/d1a95a5a-e33e-40f8-a9b7-551cb045f3ea?ref=newsletter:d2ae&utm_source=Postiviidakko&utm_medium=email&utm_campaign=Tivi_Uutiskirje_ilta

2. Onnistunut tiedonhallinta tukee kyberturvallisuuden poikkeustilanteissa

https://www.cybersecuritydive.com/news/lastpass-cyberattack-timeline/643958/

https://blog.lastpass.com/2023/03/security-incident-update-recommended-actions/

https://betanews.com/2022/12/30/lastpass-accused-of-lying-in-security-breach-announcements/

https://www.cshub.com/attacks/news/iotw-lastpass-facing-class-action-lawsuit-following-data-breach

https://www.hs.fi/kotimaa/art-2000010073301.html

https://yle.fi/a/74-20063927

https://vm.fi/tiedonhallintalaki

3. Roskaposti- ja huijausviestit pysyvät suosiossa

https://cybersecurity-magazine.com/phishing-in-2024-heres-what-to-expect/

https://securityintelligence.com/x-force/spam-trends-campaigns-senior-superlatives-2023/

https://vipre.com/resources/email-security-in-2024-an-expert-look-at-email-based-threats/?ref=hackernoon.com

https://www.emailtooltester.com/en/blog/spam-statistics/

Kuvat: Pixabay