Cyberwatch Finland

MAGAZINE 4/2025

2025 KYBERTURVALLISUUDEN TÄRKEIMMÄT TRENDIT

& KYBERENNUSTEET VUODELLE 2026

Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

Tavoitteena kyberkyvykkäämpi maailma

CWF
Cyberwatch Finland

SISÄLTÖ

Cyberwatch Finland
MAGAZINE 4/2025

Cyberwatch
MAGAZINE

JULKAISIJA Cyberwatch Oy
Nuijamiestentie 5 C
Helsinki, Finland

TOIMITUS Päätoimittaja
Aapo Cederberg
aapo@cyberwatchfinland.fi

TAITTO PuulaMedia / Mari Riepponen
KUVAT AdobeStock, PhotoShopAI
PAINO Scanseri Oy, Helsinki

ISSN 2490-0753 (print)
ISSN 2490-0761 (web)

Ajatuksia kuluneesta vuodesta ja katse tulevaisuuteen

Kulunut vuosi on ollut myrskyisä ja ennalta-arvaamaton. Tämä on näkynyt kybermaailmassa levottomuutena ja hyökkäysten kasvavana määränä. Vaikuttaa siltä, että sama meno tulee jatkumaan ensi vuonnakin, erityisesti, koska Ukrainan sodalle ei näy loppua, vaikka rauhanneuvotteluja käydään koko ajan. Yllätyksiä voi toki tapahtua, mutta on vaikea uskoa, että ne olisivat positiivisia.

Pitkän aikavälin kehitys näyttää kuitenkin paljon paremmalta: tekoäly tarjoaa uusia mahdollisuuksia, kansallinen kyberlaki tuli voimaan huhtikuussa ja yhtenäistää kyberturvallisuutta yhteiskunnan kriittisillä sektoreilla. Paljon on toki vielä tehtävää, mutta kehitys on ollut kuitenkin rohkaisevaa. Kyberriskianalyysimalleja on kehitetty ja riskipohjainen päätöksenteko on alkanut kantamaan hedelmää. Sotilaallisen puolustuksemme vahvistuminen parantaa myös kyberpuolustustamme, joka on entistä kiinteämpi osa modernia taistelukenttää. Laajasti ymmärretään, että kybermaailmassakin hyökkäys on paras puolustus ja hyökkäyskyvykkyyteen on panostettava myös siviiliyhteiskunnan kyberturvallisuutta kehitettäessä. Kyberrikolliset ovat käyttäneet laaja-alaisesti tekoälyä hyökkäystapojensa kehittämiseen. Vaikka uhkatoimijat ovat lyhyellä aikavälillä ketterämpiä ottamaan tekoälyn käyttöönsä, pitkällä tähtäimellä vaa´an uskotaan kääntyvän kyberpuolustajien eduksi.

Kriisijohtamisvalmiutta on parannettava niin valtakunnan, alueellisella tasolla kuin yrityksissä ja kaikissa organisaatioissa. Kyberturvallisuus onkin meidän kaikkien yhteinen haaste, koska ihminen on edelleen aina keskiössä. Se näkyy erityisesti erilaisten huijausten kehittymisessä määrällisesti ja laadullisesti. Meitä yritetään huijata päivittäin ja valitettavasti teemme virheitä kiireessä tai huolimattomuuttamme. Edelleen valtaosa onnistuneista kyberhyökkäyksistä saa alkunsa tietojenkalastelusta tai muusta inhimillisestä erheestä. Kyberkoulutus on edelleenkin paras tapa parantaa kyberturvallisuuttamme. Hyvin koulutetulla organisaatiolla on parempi tilannetietoisuus ja osaaminen. Tähän uusi kyberturvallisuuslakikin velvoittaa. Johdon vastuu ja rooli korostuu entisestään, on esimerkiksi tarkoin harkittava mitkä kyberturvallisuuden osa-alueet kannattaa ulkoistaa ja kenen kanssa kumppanuuksia kehitetään. Kyberturvallisuus ja siihen perustuva liiketoiminta pohjautuu mitä suuremmassa määrin luottamukseen.

Miltä se tulevaisuus näyttää? Hämärältä, koska olemme osa eurooppalaista hybridisodan näyttämöä. Venäjän viimeaikaiset sabotaasioperaatiot Isossa-Britanniassa ja Puolassa osoittavat selkeästi, että tavoitteena on aiheuttaa taloudellista vahinkoa ja ihmisuhreja, eikä pelkästään pelotella. Iskuissa on käytetty paikallisia ihmisiä, joita on värvätty rahalla. Verkossa on helposti löydettävissä ihmisiä ja rikollisia, jotka ovat ideologisista syistä ja taloudellisten syiden takia valmiita melkein mihin tahansa. Aina he eivät edes tiedä kenen hyväksi toimivat. Kybermaailmassa rikolliset ovat myyneet palveluitaan valtiollisille toimijoille jo pitkään, ja nyt sama trendi näkyy voimistuvan myös fyysisessä maailmassa. Pyrkimys yllätykseen ja kostoiskujen tarve tullee ensi vuonnakin valitettavasti kiihdyttämään kyberoperaatioiden määrää. Fyysinen turvallisuus ja digitaalinen turvallisuus on entistä kiinteämmin kietoutunut yhteen.

Kun kaikki yhdessä parannamme omaa kyberpuolustusta ja kokonaisvaltaista turvallisuuttamme, selviämme varmasti näistäkin haasteista.

Onnea uudelle vuodelle 2026!

AAPO CEDERBERG
Toimitusjohtaja
ja perustaja
Cyberwatch Finland

RISTO RAJALA &
PETER SUND

Kyberturvallisuusteollisuuden merkitys kasvaa epävakautuvassa maailmassa

Kulunut vuosi on ollut monella tapaa läntiselle maailmalle poikkeuksellinen. Tammikuussa valtaan astunut presidentti Donald Trumpin hallinto on muuttanut radikaalisti Yhdysvaltojen lähestymistapaa kauppasuhteisiin, kansainvälisen yhteistyöhön, liittolaisuuksiin ja jopa liberaaliin demokratiaan perustuvaan yhteiskuntajärjestykseen. Konfliktit ovat lisääntyneet ja monimutkaistuneet, kansainvälisen oikeuden ja sääntöpohjaisuuteen nojaavien instituutioiden toimintaedellytysten heikentyessä kiihtyvää tahtia, kun Yhdysvallat ja muut keskeiset valtiot yhä selkeämmin valitsevat aktiivisesti toimia niitä vastaan.

Sääntöpohjaisuuden ja yhteistyön rapautuminen kansainvälisessä politiikassa näkyy myös kyberturvallisuudessa, sillä kyberrikollisilla ja kyberrikollisuutta tukevilla valtioilla on yhä vähemmän pidäkkeitä toimintansa hillitsemiseen, eikä yhteisistä toimista uhkien torjumiseksi ole mahdollista sopia. Toki myös päinvastaisia kehityskulkuja ja toimia on, mutta arvioita niiden tehokkuudesta ja vaikutusten laajuudesta on hyvin vaikea tehdä.

Yhdysvaltojen kehityksen merkitystä Euroopalle ei voi ylikorostaa. Yhdysvaltojen hallinnon uusi linja Eurooppaa kohtaan näkyy lukuisilla politiikan aloilla, aina turvallisuudesta talouteen ja digitalisaatioon. Yhdysvallat on osoittanut eri keinoin, ettei Euroopan turvallisuus ole sille enää prioriteetti, ja että Euroopan on vahvistettava puolustustaan ja rooliaan NATOssa huomattavasti. Turvallisuuden osalta huolestuttavinta on Yhdysvaltojen voimakas pyrkimys saada rauha Venäjän ja Ukrainan välille hinnalla millä hyvänsä, sekä ennen kaikkea sen ilmeinen valmius painostaa Ukrainaa hyväksymään epäoikeudenmukaiset ja maan suvereniteetin vaarantavat rauhanehdot. Tämä vaarantaisi samalla vakavasti Euroopan nykyisen turvallisuusarkkitehtuurin ja palkitsisi laittomaan hyökkäyssotaan syyllistyneen, luoden huolestuttavan ennakkotapauksen.

Yhdysvallat on myös asettanut massiivisia tullimaksuja kauppakumppaneilleen ympäri maailmaa, ja käytännössä turvallisuususkumppanuuteen liittyvällä painostuksella pakottanut EU:n hyväksymään epäsuhtaisen ja -tasapainoisen kauppasopimuksen. Yhdysvaltojen hallinto ajaa voimakkaasti maan teknologiasektorin ja erityisesti suurimpien jättien etuja, vastustamalla äänekkäästi EU:n digisääntelyä sen kaikissa ilmenemismuodoissa sekä painostamalla komissiota ja jäsenvaltioita pidättäytymään säädösten toimeenpanosta. Vahvana esimerkkinä tästä käy Yhdysvaltojen hallinnon ja sitä lähellä olevien tahojen raju reaktio komission X-alustalle määräämistä sakoista, vaikka seuraamusmaksu määrättiin selkeistä rikkomuksista digipalvelusäädösten velvoitteita kohtaan ja jotka koskevat yhtä lailla eurooppalaisia kuin Euroopan ulkopuolisia yrityksiä.

Kenties kuvaavin esimerkki Yhdysvaltojen uudesta suunnasta on joulukuussa 2025 julkaistu kansallisen turvallisuuden strategia, jossa irtaudutaan sääntöpohjaisesta kansainvälisestä järjestelmästä, korostetaan suurvaltojen oikeutta etupiireihin ja intressiensä edistämiseen muista välittämättä, hylätään demokratian ja oikeusvaltioperiaatteen edistäminen globaalisti sekä ilmaistaan tahtotila puuttua Euroopan valtioiden sisäisiin asioihin edistämällä hallintojen vaihtumista Euroopassa ja heikentämällä EU:ta.

Euroopan digitaalinen suvereniteetti ja kilpailukyky

Turvallisuuden lisäksi ja samalla siihen vahvasti kytkeytyen, Euroopan digitallinen infrastruktuuri on voimakkaan riippuvainen Yhdysvalloista. Riippuvuus käsittää käytännössä kaikki digitaalisen infrastruktuurin kerrokset laitekomponenteista ohjelmistojen kautta palveluihin. Trumpin hallinnon toimien myötä jo aiempina vuosina käynnistynyt keskustelu EU:n digitaalisesta suvereniteetista on noussut uusiin mittasuhteisiin, kun nykyhallinto on osoittanut olevansa valmis edistämään intressejään tavoilla, jollaisia on pidetty vastuulliseen valtiokäyttäytymiseen kuulumattomina. Huolta ovat herättäneet etenkin skenaariot, jossa Yhdysvallat estäisi jonkun kriittisen digitaaliseen infrastruktuuriin kuuluvan ohjelmiston, palvelun tai

komponentin toimittamisen, tai vaatisi esimerkiksi Yhdysvalloissa toimivaa palveluntarjoajaa luovuttamaan tämän Euroopassa säilyttämää dataa Yhdysvaltoihin (oikeusperusta tälle on ollut jo pitkään olemassa, ks. Cloud Act).

Digitaalinen suvereniteetti on kytketty myös laajempaan keskusteluun Euroopan kilpailukyvystä ja kansainvälisessä vertailussa heikoksi jääneestä talouskasvusta, johon on haettu ratkaisuja kuumeisesti. Digitaalisen suvereniteetin vahvistaminen korvaamalla Yhdysvalloissa tuotetut teknologiat eurooppalaisilla vaihtoehdoilla on hyvin kallis ja lyhyellä aikavälillä myös epärealistinen tavoite. Poliittinen tahtotila eurooppalaisten teknologioiden tukemisen ja riippuvuuksien hillitsemisen takana vaikuttaa olevan kuitenkin niin voimakas, että digitaaliseen suvereniteettiin pyrkiminen on syytä nähdä merkittävänä, lähivuosien politiikkatoimia ohjaavana kehityskulkuna Euroopassa. Tämän ovat tunnistaneet myös eurooppalaiseen digitaaliseen infrastruktuuriin elimellisesti kuuluvat yhdysvaltalaiset suuryritykset, joista osa on pyrkinyt vastaamaan eurooppalaisten asiakkaidensa huoliin kehittämällä ratkaisuja ja palvelukonsepteja, joiden toiminta ei olisi riippuvainen Yhdysvaltojen poliittisista ”tuulista”.

EU:ssa annetun laajan digitalisaation sääntelyn väitetään usein heikentävän eurooppalaisten yritysten kilpailukykyä ja mahdollisuuksia kehittää uusia, innovatiivisia tuotteita ja palveluita. Selvää on ainakin se, että sääntelyn noudattamiseen liittyvästä hallinnollisesta työstä syntyy mittavia kustannuksia, joista osa ei kuitenkaan edistä liiketoiminnan ydinasioita eli tuotteiden ja valmistusmenetelmien kehittämistä tai tuottavuuden kasvua. Vastatakseen tähän huoleen komissio antoi digitalisaatioon kohdistuvan sääntelyn yksinkertaistamiseen tähtäävän ”Digital Omnibus” -asetusehdotuksen marraskuussa 2025.

Kyberturvallisuuden osalta asetusehdotuksella pyritään yksinkertaistamaan ja yhdenmukaistamaan keskeisimpien lakien, NIS2-direktiiviin ja kyberkestävyyssäädökseen, liittyviä raportointivelvoitteita. Kokonaisuuteen kuuluu olennaisesti yhtenäisen EU-laajuisen kyberturvallisuuspoikkeamien ilmoituskanavan rakentaminen Euroopan kyberturvallisuusviraston (ENISA) yhteyteen. Ilmoituskanavan tehtävänä on mahdollistaa kyberturvallisuuspoikkeaman raportoiminen kertaluonteisesti niin, että kaikki lainsäädännön vaatimukset tulevat täytetyiksi. Uudistuksia esitetään myös Tekoälyasetukseen ja Yleiseen tietosuoja-asetukseen.

Yleiseen tietosuoja-asetukseen esitetyistä muutoksista Elinkeinoelämän osalta olennaisimpia olisivat asetuksen neljännen artiklan (henkilötiedon määritelmä) yhteensovittaminen EU:n tuomioistuimen viimeaikaisen päätöksen kanssa riittävästä pseudonymisoinnin tasosta, sekä asetuksen kuudenteen artiklan (henkilötietojen käsittelyperusteet) muuttaminen niin, että jatkossa oikeutettu etu riittää perusteeksi henkilötietojen käsittelylle tekoälymallin kouluttamisessa ja käytössä. Tekoälyasetuksessa olennaisimpia esitettyjä muutoksia ovat asetuksen liitteen II korkean riskin käyttötarkoituksia koskevien velvoitteiden soveltamisen pysäyttäminen teknisten standardien valmistumiseen asti sekä ennen asetuksen voimaantuloa markkinoille tuotujen tekoälyjärjestelmien ”vesileimausvelvollisuudelle” (Artikla 50) siirtymäaika. Tietosuoja-asetuksen noudattamista esitetään helpotettavaksi sallimalla tekoälyjärjestelmien ja -mallien tarjoajien ja käyttöönottajien käsitellä henkilötietoja puolueellisuuden havaitsemiseksi ja korjaamiseksi, edellyttäen että asianmukaiset suojatoimet toteutetaan. Esitettyihin muutoksiin suuntautuu voimakkaita poliittisia intohimoja, joten nähtäväksi jää, millaisen muotoon ”Digiomnibus” lopulta Euroopan parlamentin ja jäsenvaltioiden käsittelyssä päätyy. **Komission on** myös tarkoitus antaa vuoden 2025 lopulla säädösehdotus kyberturvallisuusasetuksen tarkistamisesta. Tämän hetken tietojen mukaan ENISA:n tehtävien ja kyberturvallisuuden sertifiointikehyksen tarkistamisen lisäksi tarkistuksessa saatetaan keskittyä siihen, että löydetään yhtenäiset lähestymistavat tieto- ja viestintätekniikan, mukaan lukien viestintäverkkojen toimitusketjujen turvallisuuden parantamiseksi. Tämän kirjoituksen viimeistelyyn mennessä esitystä ei kuitenkaan ole vielä annettu.

Lakiesitys lasten suojelemiseksi verkkovälitteiseltä seksuaaliväkivallalta eteni parannettuna

Komission vuonna 2022 antama lakiesitys lasten suojelemiseksi verkkovälitteiseltä seksuaaliväkivallalta (CSAM-esitys) on ollut EU:n neuvoston käsittelyssä useita kertoja, kun eri jäsenvaltiot ovat tehneet esityksestä omia kompromissiesityksiään. Useimmat esityksistä olisivat toteutuessaan olleet hyvin vahingollisia sähköisen viestinnän luottamukselle, Euroopan kyberturvallisuudelle ja perusoikeuksille, koska ne sisälsivät vaatimuksen tunnistamismääräyksistä, joilla sähköisen viestinnän palveluita (ml. säilytyspalvelut) tarjoavat yritykset olisi velvoitettu skannaamaan palveluissaan tapahtuva viestiliikenne ja käytännössä luopumaan vahvasta salauksesta. Viimeisimpänä tunnistamismääräyksen sisältävää esitystä yritti viedä läpi loppuvuoden 2025 puheenjohtajamaana toiminut Tanska, joka kuitenkin kaatui Saksan ja eritoten Kristillisdemokraattien valtiopäiväedustajien vastustukseen. Suomi seisoi Eduskunnan ohjauksen myötä tukevasti Saksan rinnalla.

CSAM-ehdotuksella on koko ajan ollut hyväksyttävä ja erittäin painava tavoite suojata lapsia verkkovälitteiseltä seksuaaliväkivallalta. Pyrkimys väkivallattoman lapsuuden turvaamiseksi ja vakavien rikosten uhreina olevien lasten suojelemiseksi on luonnollisesti kannatettava. Epäonnistuneen ehdotuksen jälkeen Tanska muutti lähestymistapaansa edellisestä kompromissiehdotuksestaan ja antoi pääosin Puolan aiempaan ehdotukseen perustuvan kompromissiehdotuksen marraskuussa 2025, joka myös lopulta hyväksyttiin neuvostossa. Tanskan uusi, hyväksytty ehdotus on monestakin syystä kannatettava ja sen tavoitteet ovat aiempiin ehdotuksiin verrattuna oikeammassa suhteessa tavoiteltuun päämäärään verrattuna ja tarjoavat tehokkaita keinoja torjua lapsiin kohdistuvaa seksuaalista hyväksikäyttöä kaikkien verkon käyttäjien yksityisyyttä ja perusoikeuksia kunnioittaen.

Kyberala ja monet muut elinkeinoelämän ja kansalaisyhteiskunnan järjestöt ovat vaikuttaneet Suomen kantaan CSAM-esitykseen aktiivisesti lähivuosina kaikissa valmistelun vaiheissa. Suomen kanta olikin syksyllä 2025 tasapainoinen ja perustui oikeasuhtaisuuteen sekä vain välttämättömään puuttumiseen perusoikeussuojaan. Tärkeintä tietenkin on, että aiemmin ehdotetusta tunnistamismääräyksestä päädyttiin luopumaan. Kannatettavaa on myös numeroista riippumattomien viestintäpalveluiden vapaaehtoisten torjuntatoimien (materiaali ja grooming) vakiinnuttamista osaksi CSAM-säädöstä. On myös tärkeää, että jatkovalmistelussa varmistetaan, että näille toimille asetetaan soveltuvat suojakeinot väärinkäytösten estämiseksi.

Uusikaan esitys ei ole ongelmaton, mutta tärkeimpänä viestinnän luottamuksellisuuden suojaan sekä muihin perusoikeuksiin puuttumista on rajoitettu perustellusti ja selvästi.

Sääntely ei ole enää johtamassa laajaan ja yksilöityyn rikosepäilyyn perustumattomaan viestinnän sisällön tarkkailuun ja tunnistamiseen viranomaisten toimesta. Ehdotuksen avulla voidaan kuitenkin suojata lapsia seksuaaliselta hyväksikäytöltä ja se on paremmin perusoikeuksien rajoittamisedellytysten tarpeellisuus- ja suhteellisuusperiaatteen mukainen ja edistää vähemmän haitallisia, mutta tehokkaita ratkaisuja lasten suojelemiseen. Ehdotus mahdollistaa myös yritysvarallisuuden arvon ja elinkeinotoiminnan taloudellisten edellytysten sekä huoltovarmuuden turvaamisen aiempaa paremmin.

Ehdotuksen ongelmallisin kohta on säännös (85 artikla), jonka perusteella komissiota kehotetaan arvioimaan kolmen vuoden kuluessa asetuksen voimaantulosta, olisiko velvoittavalle tunnistamismääräykselle olemassa teknologiset ja oikeudelliset edellytykset. Näin ei tule toimia. Tarkemmin analyysin tulisi kattaa arvio CSA-materiaalin tunnistamiseen tarkoitettujen teknologioiden kehitystasosta, valmiudesta ja virhemarginaaleista. Artikla tarkoittaisi käytännössä, että kolmen vuoden kuluttua aloitettaisiin uudelleen jo moneen kertaan käyty keskustelu, jonka ytimessä olisi edelleen laaja ja yksilöimätön viestinnän sisällön tarkkailu ja tunnistaminen viranomaisten toimesta. On epärealistista olettaa, että digitaaliteknologia voisi kehittyä kolmen vuoden aikana niin, että perusoikeuksien ydinalueelle ulottuvaa, laajaa ja yksilöimätöntä luottamukselliseen viestintään puuttumista voisi välttää.

Pidämme kannatettavana, että tähän mennessä vapaaehtoisten toimien, eli tietyille palveluntarjoajille mahdollistetut vapaaehtoiset käsittelytoimenpiteet tuodaan pysyvän sääntelyn piiriin. Samalla on välttämätöntä varmistaa, että kompromississa esitetyn mukaan käsittelyyn käytettävien teknologioiden olisi muun muassa oltava mahdollisimman vähän yksityisyyteen puuttuvia alan viimeisimmän kehityksen mukaisesti. Tekstin käsittelyn osalta edellytyksenä on, että teknologialla ei tule voida päätellä viestinnän sisältöä vaan käsittelyn tarkoituksena tulisi olla sellaisten toimintamallien (patterns) tunnistaminen, jotka viittaavat mahdolliseen lasten hyväksikäyttöön. On tärkeää ja luottamusta herättävää, että puheenjohtajan ehdottamaan tekstiin on jälleen palautettu Puolankin puheenjohtajuuskaudella ollut lauseke siitä, ettei asetuksella kielletä, kierretä tai muutoin heikennetä kyberturvallisuustoimenpiteitä. Lisäksi asetuksella ei luoda velvoitteita purkaa päästä päähän -salausta tai rajoittaa sen käyttöä. Tunnistamismääräyksen poistamisen myötä myös salattuihin viestisisältöihin liittyvä ja asian käsittelyssä ongelmalliseksi tunnistettu epäselvyys poistuu.

Jäsenvaltiot pääsivät lopulta Tanskan uusimman kompromissiesityksen myötä sopuun kannastaan. Seuraavaksi esitys etenee trilogeihin, eli Euroopan komission, Euroopan parlamentin ja neuvoston edustajien välisiin neuvotteluihin, joissa instituutiot hakevat yhteistä näkemystä lain lopullisesta sisällöstä. On toistaiseksi epäselvää, mikä neuvotteluiden lopputulos on ja missä aikataulussa lopullinen laki valmistuu. Parlamentin kanta esitykseen on kuitenkin painottanut vahvasti yksityisyyden suojaa, perusoikeuksia ja kyberturvallisuutta, joten on todennäköistä, ettei esitys ainakaan heikenny neuvotteluiden edetessä.

Vuosi 2026 käynnistyy epävarmuuden vallitessa

Vuosi 2026 käynnistyy suuren epävarmuuden vallitessa. On odotettavissa, että vuonna 2025 todistetut kehityskulut jatkuvat ja voimistuvat. Yhdysvaltojen politiikan on syytä odottaa jatkuvan havaitulla linjalla ja mahdollisesti jopa kiihtyvän. Erityisesti Ukrainan sodan mahdollinen rauha ja ennen kaikkea sen ehdot ovat keskeinen, eurooppalaisiin yhteiskuntiin vaikuttava seikka. Olennaista kyberturvallisuuden näkökulmasta on myös se,

miten mahdollinen rauha vaikuttaisi Venäjältä peräisin olevaan kyberturvallisuuden vahingoittamiseen, kun ainakin tietty määrä tahtoa ja kykyä vapautuisi ”rintamasuunnasta” muuhun käyttöön.

Pyrkimykset Euroopan digitaalisen suvereniteetin vahvistamiseen tulevat olennaisesti määrittämään EU:n teknologiapolitiikan sisältöä, mikä tulee näkymään erityisesti tulevaa vuotta merkittävästi määrittävissä EU:n seuraavaa monivuotista rahoituskehystä koskevissa neuvotteluissa. Komissio on myös linjannut vuoden 2026 työohjelmassaan antavansa esityksen julkisia hankintoja koskevien direktiivien uudistamiseksi. Hankintadirektiivien merkitys kyberturvallisuusteollisuudelle saattaa nousta huomattavaksi, sillä komissio on eri tavoin ilmaissut, että uuden lainsäädäntökokonaisuuden tulisi mahdollistaa eurooppalaisten teknologisten ratkaisujen tukeminen, ja myös kyberturvallisuuden vaatimusten soveltaminen nykyistä vahvemmin hankintapäätöksen perusteena. Teollisuuden näkökulmasta keskeistä on, että uusien tukikeinojen avulla pyrittäisiin ennen kaikkea luomaan kysyntää kokonaistarkasteltuna luotettaville ja moderneille teknologiaratkaisuille protektionismin sijaan. Erityisen tärkeää on, että eurooppalaisten ratkaisujen tukeminen ei typistä jäsenvaltioiden rajoja entisestään, vaan kehittää eurooppalaisen yhteismarkkinaa, jolla kilpailukykyiset vaihtoehdot menestyvät. Kiinnostavaa on myös seurata, miten komission Omnibus-esitys ja Tanskan CSAM-kompromissiesitys mahdollisesti muuttuvat Parlamentin ja neuvoston välisissä trilogineuvotteluissa. Molempiin esityksiin liittyy vahvoja poliittisia pyrkimyksiä, ja on mahdollista, että salauksen purkamiseen liittyvästä tematiikasta joudutaan käymään jo lähitulevaisuudessa uudestaan keskustelua EU:n sisäisen turvallisuuden strategian (ProtectEU) viitekehyksessä. Kotimassa keskeistä tulee olemaan valmistelu vuonna 2027 lähestyviin eduskuntavaaleihin, joiden asetelmia ja tavoitteita valmistellaan tulevana vuonna kovaa vauhtia.

Epävarmuuksien lisääntyessä luotettavien toimijoiden ja yhteistyökumppaneiden merkitys kasvaa entisestään. Suomalainen ja Suomesta käsin toimiva kyberturvallisuusteollisuus edistää osaltaan yhteiskuntien vakautta, omaisuuden suojaa, sekä muiden yksilöiden ja yritysten perusoikeuksien toteutumista digitalisoituneessa maailmassa. Kyberturvallisuusteollisuuden edustajana Kyberala ry on vahvasti mukana vaikuttamassa kyberturvallisuuden toimintaympäristöön vaikuttaviin sääntely- ja politiikkatoimiin, edistäen tarkoituksensa mukaan Suomen pitkäaikaista etua.

KIRJOITTAJAT:

PETER SUND

Kyberala ry:n (FISC ry) toimitusjohtaja

Teknologiateollisuus ry

Jukka Rapo

RISTO RAJALA

Kyberala ry:n (FISC ry) neuvonantaja

Teknologiateollisuus ry

2025 KYBERVUOSI

Vuosi 2025 lähestyy loppuaan ja perinteiseen tapaan yritykset, mediat ja viranomaistahot ovat julkaisseet omia katsauksiaan vuoden merkittävimmistä kybermaailman tapahtumista ja ilmiöistä. Suomessa pelin avasi teleyhtiö Elisa, jonka The State of Finnish Cybersecurity 2025 -raportti julkaistiin jo lokakuussa. Kyseessä on haastatteluiden ja kyselyiden avulla toteutettu tutkimus suomalaisten yritysten ja yritysjohtajien näkemyksistä kyberturvallisuuden nykytilasta yrityksissä. Raportissa on vahva strategisen kyberturvallisuuden painotus. Sen mukaan kyberturvallisuus on noussut yhä enemmän yritysten johtoryhmien agendalle, eikä myöskään IT-palveluiden toimittaja enää ole pelkästään tiettyjen tuotteiden toimittaja, vaan strateginen neuvonantaja. Johdon ja asiantuntijoiden välillä on kuitenkin erimielisyyttä kyberturvallisuusinvestointien riittävyydestä, mikä voi aiheuttaa haasteita tulevaisuudessa.

Yhdysvaltalainen talouslehti Forbes taas nostaa vuoden kärkihavainnoksi valtiollisten kyberhyökkäyksen muodostaman uhkan. Tätä selittävät Yhdysvaltojen kriittiseen infrastruktuuriin vuoden aikana kohdistuneet merkittävät kyberhyökkäykset. Erityisen näkyvä oli muun muassa Kiinan turvallisuusministeriöön linkitetyn Salt Typhoon -uhkatoimijan hyökkäyskampanja, joka on jatkunut aktiivisena koko vuoden. Hakkeriryhmän on muun muassa pelätty päässeen televiestintäverkkojen kautta käsiksi suureen määrään yhdysvaltalaisten tietoja. Muita Forbesin vuodesta 2025 esille nostamia teemoja ovat toimitusketjuihin kohdistuneiden kyberhyökkäysten aiempaa suuremmat seuraukset, kyberregulaation kehitys ja kyberalan osaajapulan muodostama strateginen riski. Lehti mainitsee myös tekoälyn. Vaikka se on tukenut kyberpuolustajia, ovat hyökkääjät toistaiseksi olleet Forbesin mukaan ketterämpiä adaptoitumaan muuttuneeseen tilanteeseen.

Useissa muissa julkisuissa, kuten verkkolehtien CSO Onlinen ja Government Technologyn vuosikatsauksissa, tekoäly nostetaankin vuoden merkittävimmäksi kyberilmiöksi. Se on pakottanut yrityksiä pohtimaan uudelleen turvallisuusstrategioitaan ja vaikuttanut sekä kyberhyökkääjien että puolustajien toimintaan. Toisaalta myös kriittisen infrastruktuurin ja kolmansien osapuolten tai toimitusketjujen kautta nousevat kyberuhkat mainitaan. Government Technology mainitsee lisäksi pilvipalveluiden turvallisuuden. Kyberrikollisuuden puolelta erityisesti kiristyshaittaohjelmat, joiden hyökkäysmäärät mahdollisesti rikkovat jälleen ennätyksiä, ovat säilyneet merkittävänä uhkana. Kiristyshaittaohjelmaryhmien toiminta on kehittynyt vuoden aikana, ja esimerkiksi aiempaa hienovaraisempia tietojenkalastelukampanjoita ja sosiaalisen median hyökkäyskampanjoita on havaittu.

Viranomaispuolella vuosiraporttien ja katsausten suhteen on ollut hiljaisempaa, mikä oli toki odotettavissakin. Usein raportteja kuluneesta vuodesta voidaan odottaa putkahtelevan seuraavan alkuvuoden ja kevään aikana. Poikkeuksen on tehnyt Iso-Britannian kyberturvallisuuskeskus NCSC (National Cyber Security Centre), jonka vuosiraportti 2025 julkaistiin jo lokakuussa. Nimi vuosiraportti on tosin hieman harhaanjohtava, sillä tosiasiassa raportti tarkastelee aikaväliä 1.9.2024-31.8.2025. Joka tapauksessa on mielenkiintoista tarkastella, millaiseksi viranomaiset ovat kokeneet kybermaailman viimeaikaisen kehityksen. Britannian kohdalla merkittäviä uhkia ovat olleet Kiinan, Venäjän, Iranin ja Pohjois-Korean valtiollinen kybertoiminta. Kiristyshaittaohjelmat, tekoäly ja kriittiseen infrastruktuurin kohdistuvat uhkat nousevat esille myös Iso-Britannian uhka-arviossa. Mielenkiintoisena yksityiskohtana NCSC:n raportissa mainitaan kyberdiplomatia ja niin kutsuttu Pall Mallin -prosessi, jonka puitteissa pyritään rajoittamaan kyberaseiden ja kaupallisten vakoiluohjelmistojen leviämistä. Tämä on uhka, joka muissa raporteissa on jäänyt pääosin huomioimatta.

Kokonaisuutena eri toimijoiden koostamissa raporteissa on paljon samankaltaisuuksia. Tekoäly, kriittinen infrastruktuuri, valtiolliset uhkatoimijat, kiristyshaittaohjelmat ja regulaatio mainitaan jossain muodossa valtaosassa raporteissa. Haasteen aiheuttaa silti kyberalan monimuotoisuus. Seurattavia ilmiöitä, teknologioita ja tapahtumia on valtava määrä, mikä pakostakin jättää katveita jokaiseen raporttiin. Seuravaksi Cyberwatch Finland esittelee omia avainhavaintojaan vuodesta 2025.

2025 KYBERVUOSI

Vuoden merkittävin kyberilmiö:

TEKOÄLY

Tekoälyuutisoinnilta on viimeisen vuoden aikana voinut välttyä vain aktiivisesti vaivaa näkemällä. Se on aihealueesta riippumatta ollut jatkuvasti pinnalla niin hyvässä kuin pahassa, ja kyberturvallisuuskin on luonnollisesti saanut osansa. Tekoäly oli kaikkein merkittävimpänä teemana myös marraskuisilla Cyber Security Nordic -kyberturvallisuusmessuilla, eikä näin ollen liene yllättävää, että myös Cyberwatch on valinnut sen vuoden merkittävimmäksi ilmiöksi. Kuluneen vuoden aikana se on näyttäytynyt kyberturvallisuuden näkökulmasta ennen kaikkea uhkana. Kyberrikollisuus on ottanut tekoälyn käyttöön vauhdilla, ja tässäkin asiassa puolustajat tuntuvat tulevan perässä. Tekoälyä on tänä vuonna hyödynnetty hyökkäyksissä esimerkiksi seuraavilla tavoilla: hyökkäys on kohdistettu tekoälymalliin itseensä kuviin piilotetuilla syötteillä, malli on tahallisesti rikottu suorittamaan haitallisia toimintoja ja jopa valjastettu automatisoimaan lähes koko hyökkäys. Samalla on puhuttu tekoälykilpailusta etenkin Yhdysvaltojen ja Kiinan välillä. Kiina otti aimo harppauksen eteenpäin DeepSeekin julkaisun yhteydessä vuoden alussa, mutta laitteiston ja etenkin sirujen osalta kiinalaiset ovat tänä vuonna olleet vielä takaa-ajajia. Vain aika näyttää, mihin suuntaan tekoälykilpailu kehittyy ensi vuonna ja löydetäänkö rikollisten tekoälytyökaluille kyberpuolustuksellisia vastineita.

Vuoden yllättävä kyberilmiö:

GEOPOLIITTISET RISKIT

Kenties hieman ironisesti vuoden suurin kyberturvallisuuteen liittyvä yllätys on tullut geopolitiikan puolelta. Vaikka jo koko viime vuoden ajan spekuloitiin laajasti Donald Trumpin vaalivoiton seurauksilla, ei kovin moni varmasti osannut ennustaa ihan näin radikaaleja seurauksia. On lähes mahdotonta käsittää, miten valtava muutos vuoden aikana on tapahtunut. Asia kiteytyy varsin hyvin Tanskan tilanteeseen. Sen kansallisen turvallisuuden strategiassa Yhdysvaltojen kerrotaan olevan Tanskan tärkein turvallisuuspoliittinen liittolainen. Tämän vuoden lopulla tilanne oli kuitenkin joiltain osin keikahtanut lähes täysin päälaelleen Tanskan sotilastiedustelun luokiteltua Yhdysvallat ensimmäistä kertaa koskaan turvallisuusuhkaksi. Kybermaailmassa Yhdysvaltojen ja Euroopan välien tulehtuminen vaikuttaa ennen kaikkea yhdysvaltalaisten digijättien palveluiden kautta. Toukokuussa koko maailmaa kohautti tapaus, jossa Microsoft esti ICC:n syyttäjän pääsyn omaan sähköpostiinsa Trumpin asettamien pakotteiden seurauksena. Tapaus sai monet uudelleenarvioimaan yhdysvaltalaisten tuotteiden ja palveluiden luotettavuutta, ja sen seurauksena etenkin Euroopassa on käyty vilkasta keskustelua digitaalisesta omavaraisuudesta. Myös kauppasodan uhka on lisännyt kysyntää eurooppalaisille tuotteille, mutta toistaiseksi kilpailukykyisiä vaihtoehtoja ei juurikaan ole.

Vuoden aliarvostetuin kyberilmiö:

KYBERTURVALLISUUSLAKI

Euroopan unionin NIS2-kyberturvallisuusdirektiivi implementoitiin Suomessa osaksi kansallista lainsäädäntöä huhtikuun alussa 8.4.2025. Uusi kyberturvallisuuslaki asetti useita kyberriskienhallinnan velvoitteita etenkin suurille ja keskisuurille kriittisten ja tärkeiden alojen toimijoille. Näihin lukeutuvat ilmoittautuminen keskeisten ja tärkeiden toimijoiden luetteloon, velvollisuus ilmoittaa merkittävistä poikkeamista sekä useat muut kyberriskienhallinnan toimenpiteet. Merkittäviä ovat myös lain asettamat uudet vastuut organisaatioiden johdolle. Kyberturvallisuuslain myötä johdon on henkilökohtaisesti varmistettava organisaation tietoturvallisuuden toteutuminen ja varmistettava, että tietoturvallisuuteen liittyvät riskit ovat hallinnassa. Useissa organisaatioissa johdon tietoisuus kyberturvallisuuden nykytilasta sekä tavoitteista on silti edelleen usein vajavaista. Johdon kybertietoisuus ja kyvykkyys johtaa kyberresurssien jakamista sekä kybertoiminnan ohjaamista ja valvomista on aliarvostettua niin meillä Suomessa kuin myös yleisesti EU:n alueella. Tähän auttaa ensi tilassa kouluttautuminen ja perehtyminen kyberturvallisuuteen. Kyberturvallisuus tulisikin nähdä organisaation toiminnan mahdollistavana voimavarana, ei niinkään kulueränä. Panostukset ja erilaiset resursoinnit kyberturvallisuuteen maksavat itsensä takaisin toiminnan pysyessä kyberhyökkäyksiltä suojassa. Lisäksi vahvempi läsnäolo ja ymmärrys kyberturvallisuuden toteuttamisessa ja kybertilannetietoisuuden ylläpidossa on johdolle velvoitteiden toteutumisen kannalta tärkeää. Viestit kentältä osoittavat, että useissa organisaatioissa on myöhästytty lainvelvoittamista toimenpiteistä, kuten toimijaluetteloon ilmoittautumisesta 8.5. mennessä sekä kyberriskienhallintamallin luomisessa 8.7. mennessä. Kyberuhkan säilyessä korkeana olisi toimenpiteisiin silti parempi ryhtyä myöhään kuin ei milloinkaan.

Vuoden pettymys:

UHKATOIMIJOIDEN VANHAT KIKAT PUREVAT EDELLEEN

Kulunut vuosi toi esiin myös ikäviä tosiasioita siitä, että valtaosa kyberhyökkäyksistä tapahtuu edelleen ihmisten osaamattomuuden, huolimattomuuden sekä piittaamattomuuden takia. Tietoturvayhtiö DeepStriken statistiikan mukaan vuonna 2025 68 % onnistuneista kyberhyökkäyksistä tapahtui ihmisten erehdyksien kautta. Tämä on toki parannus vuoden 2017 lukuihin, jolloin lähenneltiin eri lähteiden mukaan 90 prosenttia. Tätä lukua olisi silti mahdollista pienentää henkilökunnan kouluttamisella, motivoimisella ja erilaisilla harjoituksilla. Kyberhyökkäyksiä, joissa ihminen on lopulta heikoin lenkki, on paljon erilaisia. Tällaisia ovat esimerkiksi tietojenkalastelun ja sosiaalisen manipulaation eri muodot. Lisäksi saman salasanan käyttö useissa eri palveluissa, työsähköpostin väärinkäyttö ja muiden kyberturvallisuuden perusasioiden unohtaminen näyttelevät suurta roolia onnistuneissa kyberhyökkäyksissä. Tämä kaikki voitaisiin estää hyvin helposti. Mikäli jokaiselle organisaation henkilökunnan jäsenelle olisi selvää, että työsähköpostiosoitetta ja työtietokonetta ei käytetä vapaa-ajan palveluihin tai muihin kuin työhön konkreettisesti liittyviin toimintoihin, ei tämänkaltaisia ongelmia juuri syntyisi. Mikäli kaikille olisi lisäksi selvää uniikkien salasanojen tärkeys, olisi vuodettujen käyttäjätunnusten hyödyntäminen kyberhyökkäyksessä entistä hankalampaa. Perusasioiden tärkeys kyberturvallisuuden toteutumisen kannalta korostuu siis edelleen. Yksilön rooli kyberturvallisuuden takaajana on niin ikään merkittävä. Organisaation johdon tuleekin huomioida sekä valvoa kybertietoisuuden ja -osaamisen jatkuvaa ylläpitämistä organisaatiossa.

Vuoden 2025 merkittävimpiä

KYBERHYÖKKÄYKSIÄ

MARKS & SPENCER

AJANKOHTA: Huhtikuu 2025
KUVAUS: Britannialainen vähittäiskaupan suuri toimija Marks & Spencer koki kyberhyökkäyksen, jonka seurauksena sen järjestelmät kryptattiin haittaohjelmalla. Samalla hyökkääjät saivat käsiinsä myös asiakastietoja. Hyökkäyksen epäillään alkaneen jo helmikuussa, mutta eskaloituneen tietojen kryptaamiseen huhtikuussa.
TEKIJÄ: Scattered Spider/Oktapus/UNC3944. Ryhmän arvellaan koostuvan Yhdysvalloissa ja Isossa-Britanniassa elävistä nuorista ja aikuisista, joita on myös joutunut pidätetyiksi viime vuosien aikana.
MOTIIVI: Taloudellinen
VAIKUTUKSET: Jokapäiväinen liiketoiminta keskeytyi, ja yhtiö käski noin 200 työntekijän jäädä pois töistä siksi aikaa, kunnes järjestelmät saadaan takaisin käyttöön. Verkkokaupan toiminta keskeytyi kahdeksi kuukaudeksi kokonaan, ja palautui sen jälkeenkin hitaasti. Yhtiön tulos laski lähes 400 miljoonaa puntaa hyökkäyksen takia. Mainehaitan rahallista arvoa on vaikea mitata, mutta etenkin varastetut asiakastiedot voivat vielä lisätä tapauksen hintaa yhtiölle.

AEROFLOT

AJANKOHTA: 28.7.2025
KUVAUS: Ukrainan ja Venäjän välisen kybersodan kenties näkyvin tapahtuma nähtiin heinäkuussa, kun yli vuoden ajan Aeroflotin järjestelmissä iskua valmistelleet hyökkääjät toteuttivat operaationsa. Pitkällisten valmisteluiden tuloksena he olivat saaneet järjestelmänvalvojan käyttöoikeudet kaikkiin yhtiön järjestelmiin. Niiden avulla hyökkääjät saivat varastettua käytännössä kaikki yhtiön tiedot. Lisäksi he tuhosivat valtavan määrän yhtiön järjestelmiä.
TEKIJÄ: Ukrainalaismieliset hakkeriryhmät Silent Crow ja valkovenäläinen Cyberpartisans toteuttivat iskun yhteistyössä.
MOTIIVI: Poliittinen
VAIKUTUKSET: Ensimmäisen päivän aikana lentoja peruttiin 108 ja pelkästään Sheremetyevon kentällä myöhästymisiä oli yli 80. Jos Aeroflot ei olisi heti katkaissut yhteyksiään kaikkiin mahdollisiin palveluihin ja lopulta myös pääkonttorinsa sähköjä, sen IT-järjestelmät olisivat tuhoutuneet kokonaan. Aeroflot onnistui lopulta kuitenkin palaamaan normaaliin toimintaan vain muutamassa päivässä, mutta varastetut tiedot tulevat piinaamaan yhtiötä vielä pitkään. Erityisen kiusallista oli se, että hyökkääjät julkistivat todisteet yhtiön yhteistyöstä Venäjän asevoimien kanssa, vaikka Aeroflot on toistuvasti julkisesti kiistänyt kaikenlaisen osallisuuden sotilaalliseen toimintaan.

BYBIT

AJANKOHTA: 21.2.2025
KUVAUS: Kryptovaluuttavälittäjä Bybit koki kyberhyökkäyksen, jonka tekijäksi epäillään pohjoiskorealaisia hakkereita. Hyökkäys kohdistui yhtiön sisäiseen siirtoprosessiin, jossa siirrettiin Ethereumia Offline-varastosta Online-käyttövarastoon. Varastetut kryptovaluutat siirrettiin aluksi kryptolompakoihin, jotka tunnistettiin Lazarus-ryhmän aiemmin käyttämiksi lompakoiksi. Tämän jälkeen varat on hajautettu tuhansiin eri kryptolompakoihin ja osa sekoitettu muiden kryptovälittäjien kautta sekä kryptovaluutan jäljitystä häivyttävien crypto-mixereiden avulla.
TEKIJÄ: Lazarus (Pohjois-Korean APT38)
MOTIIVI: Taloudellinen
VAIKUTUKSET: Bybit menetti hyökkäyksessä noin 1,5 miljardin dollarin arvosta Ethereum-kryptovaluuttaa. Summa on historian suurin yksittäisen kyberhyökkäyksen aikana haltuun saatu rahallinen summa. Bybit teki iskun seurauksena valtavia tappioita, mutta vakuuttaa kaikkien asiakkaidensa varojen olevan edelleen turvassa ja kantavansa itse vastuun tapahtuneesta. Tapauksen selvitys sekä varastettujen varojen jäljittäminen ja mahdollinen palauttaminen Bybitin haltuun on edelleen käynnissä. Bybit on tarjonnut varojen takaisin saamiseen johtavasta vinkistä tai toimista 10 % palkkion menetetystä summasta, mikä tarkoittaa karkeasti 150 miljoonaa Yhdysvaltain dollaria. On kuitenkin todennäköistä, että suurinta osaa varastetuista varoista ei saada koskaan takaisin. Tapaus on esimerkki Pohjois-Korean harjoittamasta rikollisesta toiminnasta taloutensa sekä ydinohjelmansa rahoittamiseksi.

Vuoden 2025 merkittävimpiä

UHKATOIMIJOITA

LUMMA MALWARE

KUVAUS: Lumma Malware tunnetaan myös nimellä Lumma Stealer tai Lumma Infostealer. Kyseessä on tietoa varastavien infostealer-haittaohjelmien ylivoimaisesti suurin ja laaja-alaisinta vahinkoa aiheuttava haittaohjelma. Lumma operoi Malware-as-a-Service (MaaS) -toiminnalla, eli se kauppaa kehittämäänsä haittaohjelmaa muiden toimijoiden käyttöön. Lumman kehittäjien ja ylläpitäjien epäillään olevan venäläisiä.
VIIME AIKOJEN TOIMINTA: Lumman kehittämällä infostealer-haittaohjelmalla suoritetaan tällä hetkellä yli puolet kaikista infostealer-haittaohjelmahyökkäyksistä. Kyseisellä haittaohjelmalla varastetaan käyttäjätunnuksia, kryptovaluuttalompakoiden sisältämää dataa ja käyttöavaimia, henkilökohtaisia tietoja, istuntoavaimia (session tokens), monivaiheisen tunnistautumisen tunnuksia (MFA) ynnä muita kriittisiä tietoja.
TOIMINTATAVAT JA TAKTIIKAT: Haittaohjelmaa levitetään pääosin tietojenkalastelukampanjoiden, sosiaalisen manipulaation, haitallisen mainonnan (malvertaising) ja hakukoneoptimoinnin avulla. Myös sosiaalisen median linkkejä käytetään Lumman levityksessä. Näiden kautta uhrin laitteelle latautuu kyseinen tietoa varastava haittaohjelma, joka alkaa kerätä uhrin laitteelta kriittisiä tietoja. Haittaohjelmaa ja sen toiminta- sekä levitystapoja kehitetään ja päivitetään jatkuvasti. Tämä tehdään toiminnan jatkumisen ja tehokkuuden varmistamiseksi. Lumman on muun muassa joissain tapauksissa todettu lataavan uhrin laitteelle myös muita haittaohjelmia.

QILIN RANSOMWARE

KUVAUS: Heinäkuussa 2022 ensimmäisen kerran tavattu lunnashaittaohjelmatoimija tunnetaan myös nimellä Agenda Ransomware. Kyberturvallisuustalo Cyber Intelligence Housen mukaan Qilin on ollut vuoden aktiivisin kiristyshaittaohjelmatoimija yli 1200 uhrillaan. Kiristyshaittaohjelmatoiminta on vuoden 2025 aikana säilynyt kärjessä organisaatioiden kyberuhkissa.
VIIME AIKOJEN TOIMINTA: Qilin Ransomware on ollut vuoden 2025 aktiivisin lunnashaittaohjelmatoimija eri lähteiden mukaan. Toiminnan tasosta kertoo se, että myös valtiolliset kybertoimijat hyödyntävät sen ohjelmakoodia. Esimerkiksi helmikuussa 2025 pohjoiskorealainen kyberuhkatoimija Moonstone Sleet aloitti iskut Qilin Ransomwaren haittaohjelmalla.
TOIMINTATAVAT JA TAKTIIKAT: Qilin Ransomware myy kehittämäänsä haittaohjelmakoodia “alihankkijoilleen”. Qilin Ransomwarella toteutetut hyökkäykset alkavat usein kalasteluviestillä. Päästyään laitteelle sisään, haittaohjelma pyrkii sammuttamaan virustorjuntaohjelmat ennen kuin se laukaisee varsinaiset haittaohjelmatoiminnot. Qilin Ransomware räätälöi haittaohjelmansa jokaisen uhrin kohdalla tilanteeseen sopivaksi.

SALT TYPHOON

KUVAUS: Vuodesta 2020 aktiivisena ollut Salt Typhoon on Kiinan turvallisuusministeriöön linkitetty uhkatoimija. Historiansa aikana se on kohdistanut hyökkäyksiään yli 80 eri maahan. Salt Typhoon on malliesimerkki niin kutsutuista APT-ryhmistä, joilla usein viitataan valtiollisiin kyberuhkatoimijoihin. Muita merkittäviä vuoden 2025 valtiollisia APT-toimijoita ovat olleet muun muassa Venäjän, Iranin ja Pohjois-Korean alaisuudessa toimivat ryhmät.
VIIME AIKOJEN TOIMINTA: Vuonna 2025 Salt Typhoon oli otsikoissa erityisesti Yhdysvaltain kansalliskaartiin kohdistuneen kyberhyökkäyksen takia. Lisäksi ryhmän aiempien toimien kuten Yhdysvaltain teleinfrastruktuuriin vuosina 2023 ja 2024 kohdistuneiden hyökkäysten jälkipyykki on jatkunut aktiivisena vuoden aikana. Villeimmissä arvioissa on arveltu ryhmän saaneen tietoja käytännössä kaikista yhdysvaltalaisista, sillä sen uhriluetteloon kuuluvat muun muassa teleoperaattorit Verizon, AT&T ja T-Mobile useiden muiden alan yritysten kanssa. Hakkereilla on ollut pääsy esimerkiksi käyttäjien puheluiden ja tekstiviestien metadataan, kuten päivämäärätietoihin, puhelinnumeroihin ja IP-osoitteisiin.
TOIMINTATAVAT JA TAKTIIKAT: Salt Typhoonin tiedetään hyödyntävän toimissaan tunnettuja CVE-haavoittuvuuksia, jotka koskettavat mm. Palomuureja, reitittimiä ja VPN-palveluita. Saatuaan pääsyn uhrijärjestelmään se pyrkii välttämään paljastumista esimerkiksi käyttäjäoikeuslistoja (access control list, ACL) manipuloimalla.

Vuoden ensimmäisessä viikkokatsauksessa on hyvä nostaa katse kohti tulevaa ja tarkastella edessä siintävää vuotta 2026. Useat kotimaiset sekä kansainväliset kyberalaa seuraavat toimijat ovatkin jo ehtineet julkaista arvioita tulevan vuoden kybertoimintaympäristön kehityksestä. Vaikka tunnetun sanonnan mukaan ennustaminen on hankalaa, varsinkin tulevaisuuden ennustaminen, parhaimmillaan ennusteet herättelevät organisaatioissa haastamaan totuttuja ajatusmalleja sekä kannustavat varautumaan tulevaisuuden haasteisiin ja skenaarioihin.

Kotimainen teleoperaattori ja tietoturvayhtiö Elisa ennustaa 12.10. järjestetyn Kyberintekijät 2025 -tapahtuman pohjalta kootussa artikkelissa vuodelle 2026 vähintään samanlaista epävakautta kuin vuonna 2025 nähtiin. Yhtiön mukaan kyberhyökkäyksistä on viime vuosien aikana tullut aiempaa kohdennetumpia sekä vaikutuksiltaan lamauttavampia. Tämän trendin uskotaan yhä jatkuvan. Toisena avainteemana Elisa korostaa johdon roolin tärkeyttä kyberturvallisuuden ytimessä — tulevaisuudessa johdolta vaaditaan yhä vankempaa osaamista ja tukea kyberturvallisuuden ylläpidolle sekä kehittämiselle. Myös tekoäly on oleellisesti läsnä Elisan tulevaisuuskuvassa. Kyberhyökkäyksistä saadaan tekoälyn avulla yhä tehokkaampia, toimivampia ja nopeampia. Lisäksi hyökkäysten skaalaus ja määrällinen lisääminen on tekoälyn avulla entistä helpompaa.

Verkkolehti ja IT-konsultointia tarjoava TechRepublic nostaa omassa ennusteessaan esille tietoturvaoperaatiokeskusten eli Security Operation Center (SOC) kehityksen kyberpuolustuksessa. TechRepublic ennustaa, että tekoäly tullaan implementoimaan SOC-toimintaan osaksi analyytikoiden työkalupakkia. Tekoäly ei kuitenkaan tule korvaamaan heitä, vaan lisää heidän kykyjään torjua kehittyviä uhkia. Ihmisten tehtäväksi jää etenkin tilannekohtainen harkinta, hienosäätö ja erilaiset luovat ongelmanratkaisut. Tekoälyllä taas voitaisiin hoitaa suuren tietomäärän haasteet poimimalla siitä oleellinen osuus analyytikon tietoon. Myös kaikki toistuvat ja yksinkertaiset tehtävät voidaan siirtää tekoälyn pureskeltavaksi. Mahdollisesti tekoäly auttaisi lisäksi luomaan kehittyneitä ratkaisuja, jotka pystyvät löytämään varhaisen vaiheen signaaleja ennen kuin kyberhyökkäykset ehtivät aiheuttaa tuhoa. Toisaalta TechRepublic nostaa esille mahdollisuuden kehittää haittaohjelmia suoraan uhrin

järjestelmän sisällä. Monet organisaatiot ja yksityishenkilöt ovat asentaneet erilaisia paikallisia tekoälymalleja, jotka pyörivät omien laitteiden ja palvelinten varassa, eivätkä siis ole yhteydessä julkisesti pyöriviin tekoälymalleihin. Näihin paikallisiin tekoälymalleihin hyökkääjät voisivat ujuttaa haitallisia käskyjä tai koodia. Tämä voisi lopulta johtaa tekoälyn paikallisesti kehittämään haittaohjelmaan suoraan uhrin järjestelmän sisällä. Tekoälyn käyttöönottoa ei tulisikaan kiirehtiä ja sen implementoinnissa tulisi aina kiinnittää huomiota turvallisuusnäkökulmiin.

Tekoälyn merkitystä korostavan ennustuksen on tehnyt myös kyberturvallisuusyhtiö Palo Alto, joka korostaa tekoälyn mahdollistavan kokonaisvaltaiset identiteettivarkaudet. Tekoälyn avulla voidaan helposti koota ihmisen ulkoinen olemus, ääni ja henkilötiedot digitaaliseen muotoon, jossa niitä voidaan hyväksikäyttää loputtomin eri keinoin. Myös datan luotettavuus on koetuksella tekoälyn tuottaessa niin tahattomasti kuin tahallisestikin suuria määriä vääristeltyä tietoa. Lisäksi Palo Alto arvioi raportissaan tulevan kvanttivallankumouksen haasteiden olevan jo käsillä. Kvanttilaitteita varten kerätään jo nyt varastettua salatussa muodossa olevaa dataa, joka on myöhemmin mahdollista purkaa selkokielelle. Kvanttisuojattuja kryptausmenetelmiä tulisikin Palo Alton mukaan kiireesti ajaa sisään hyvissä ajoin jo ennen kvanttiteknologian saapumista.

Talouslehti Forbes arvioi niin ikään tulevan vuoden olevan entistä työläämpi kyberpuolustuksen näkökulmasta. Forbes arvioi kyberhyökkäysten lisääntyvän entisestään. Valtiollisten toimijoiden se uskoo kohdistavan yhä enemmän iskuja arkielämää pyörittävään infrastruktuuriin. Kulunut vuosi 2025 osoitti Internetin megayhtiöiden pyörittämien pilvipalveluiden haavoittuvuuden, ja Forbes uskookin kyberhyökkääjien kohdistavan niihin iskuja tulevan vuoden aikana. Tällä olisi potentiaalisesti laajoja vaikutuksia, sillä pilvipalvelumarkkinat ovat hyvin pitkälti keskittyneet muutaman globaalin toimijan varaan.

Konsulttiyhtiö PwC ennustaa tulevan vuoden kyberhyökkäysten olevan yhä kehittyneempiä, hankalammin havaittavia, identiteettikeskeisiä sekä liittyvän yhä vahvemmin oikean maailman geopoliittisiin tai ideologisiin konflikteihin. Hyökkääjät yhä harvemmin ”murtautuvat” sisään uhrijärjestelmiin vaan kasvavana trendinä PwC näkee käyttäjätunnuksien kanssa kohdejärjestelmiin kirjautumisen. Nämä käyttäjätunnukset joko varastetaan, huijataan, ostetaan tai muilla keinoilla otetaan haltuun, jonka jälkeen kohdejärjestelmään sisään pääseminen onkin huomattavasti helpompaa. Myös PwC nostaa tekoälyn merkityksen korkealle niin puolustuksen kehittämisessä kuin myös hyökkääjien skaalautumisessa tai kyberhyökkäysten demokratisoitumisessa. Tekoäly tulee yhä helpottamaan kyberhyökkäysten toteuttamista heikompitaitoisille ja kokemattomille toimijoille.

Kuten edellä kuvatuista esimerkeistä näkee, asiantuntijaorganisaatioiden kyberennusteissa vuodelle 2026 korostuvat teknologian kehityksen mukanaan tuomat uhkat, joista tekoäly vuoden 2025 trendin mukaan jatkaa kärjessä. Oikeastaan vain TechRepublic nosti esille teknologian mukanaan tuomia positiivisia kehityskulkuja SOC-palveluiden kehittymisen myötä. Varsinaisia irtiottoja tai maailmaa mullistavia ennustuksia ei asiantuntija-arvioissa kuitenkaan ole. Tekoälyn nostaminen kärkiaiheeksi onkin tietyllä tapaa helppo ja varma ratkaisu, jota veikkaamalla ei voi mennä pahasti pieleen. Tekoälyn kehityksen lisäksi on silti havaittavissa muitakin trendejä, joista organisaatioissa olisi hyvä olla tietoisia ja jotka niiden tulisi ottaa huomioon riskianalyyseissaan vuoteen 2026 siirryttäessä.

Cyberwatch Finlandin kyberennusteet 2026

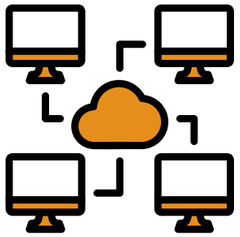
Ukrainan rauhanprosessin vaikutus kybermaailmaan tulee olemaan näkyvä

Ukrainan rauhanneuvottelut ovat jatkuneet pitkin vuotta 2025 ja tulevat jatkumaan myös vuonna 2026. Mahdollisella rauhansopimuksella tai edes tulitauolla voisi olisi suoria vaikutuksia kybermaailmaan sekä Ukrainassa että Euroopassa laajemmin. Vaikutukset riippuvat pitkälti siitä, kuinka todellinen rauha saadaan aikaan. Ideaalitilanteessa rauhansopimus johtaisi vihollisuuksien lakkaamiseen myös kybermaailmassa, mutta tämä ei ole todennäköistä. Sen sijaan vaikutukset voivat Ukrainan kannalta olla päinvastaiset. Kun Venäjän ei enää ole mahdollista pommittaa kriittistä infrastruktuuria perinteisillä aseilla, voi Ukrainan kohtaamien kyberhyökkäysten määrä jopa lisääntyä nykyisestä. Tosin Venäjän saadessa mieleisensä rauhan olisi sen rauhansopimuksen tullen mahdollista siirtää katseensa muualle. Tällöin kyber- ja hybridivaikuttamista sekä erilaisia koepalloja voitaisiin nykyistä enemmän kohdistaa esimerkiksi pohjoismaiden ja Baltian suuntaan.

Reagointiaika kyberhyökkäyksiin tulee romahtamaan

Tekoälyn kehityksen myötä kyberhyökkäysten hyökkäysvaiheita on tulevaisuudessa mahdollista automatisoida yhä enemmän, joten hyökkäyssyklit todennäköisesti nopeutuvat huomattavasti. Tiedusteluvaiheesta hyökkäyksen loppuunsaattamiseen saattaakin jatkossa kulua vain minuutteja. Jo nyt on viitteitä siitä, että uhkatoimijat ovat nopeita siirtymään tunnettujen CVE-haavoittuvuuksien (Common Vulnerabilities and Exposures) julkistamisesta hyökkäysten toteuttamiseen. Muutos vaatii organisaatioilta panostuksia kyberturvallisuuteen. Esimerkiksi tarve SOC-tietoturvakeskuspalveluille voi kasvaa tulevaisuudessa. Samalla ennakoinnin ja tilannekuvan merkitys korostuu kyberriskeihin varautumisessa.

Varajärjestelmien rooli korostuu



Vuonna 2025 nähtiin useita tapauksia, joissa skaalatut teknologiaratkaisut aiheuttavat heikkoudellaan globaaleja ongelmia. Tällaisiin lukeutuvat esimerkiksi Cloudflaren ja Amazon Web Servicen käyttökatkot, jotka lamauttivat verkkosivujen ja sovellusten toimintaa maailmanlaajuisesti. Internet-jättien heikkoudet voivat avata ovea pienemmille palveluntarjoajille ja vähintäänkin korostavat tarvetta jatkuvuudenhallinnalle ja varajärjestelmille. Euroopassa on ollut paljon puhetta digitaalisesta suvereniteetista ja yhdysvaltalaisten palveluntarjoajien muodostamista geopoliittisista riskeistä. Ehkä vuonna 2026 verkon isojen palveluntarjoajien rinnalla aletaan käyttää eurooppalaisia vaihtoehtoja, joiden käyttöön voidaan myöhemmin siirtyä kokonaan.

Informaation määrä vaikeuttaa päätöksentekoa

Informaation ja datan määrä maailmassa kasvaa kiihtyvästi myös vuonna 2026. Erityisesti tekoäly on nopea tuottamaan tekstiä, kuvia, videoita ja muuta materiaalia. Tällä on monenlaisia seurauksia. Toden ja epätoden erottaminen tulee jatkossa olemaan aiempaa haastavampaa. Lisäksi seurauksena voi olla “informaatioähky”, kun tietoa ja dataa tulee jatkuvasti useista eri lähteistä. Toisaalta kehittyneet työkalut mahdollistavat oivalluksien löytämisen tietolähteistä, joista se ei aiemmin olisi ollut mahdollista. Organisaatioiden analyytikoille ja päätöksentekijöille informaatiomäärän kasvaminen tuottaa haasteita. Edelleen datan suodattamiseen ja avainhavaintojen tekemiseen tarvitaan ihmissilmää, vaikka tekoäly voi analyysi- ja päätöksentekoprosesseissa toimia oivana työkaluna tai sparrauskumppanina.

LÄHTEET:

Cyberwatch Finland viikkokatsaukset 2025

Cyberwatch Finland kuukausikatsaukset 2025

https://yrityksille.elisa.fi/ideat/the-state-of-finnish-cybersecurity-2025-raportti-paljastaa-kyberturvan/

https://www.csoonline.com/article/4102893/cybersecurity-leaders-top-seven-takeaways-from-2025.html

https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025

https://www.govtech.com/blogs/lohrmann-on-cybersecurity/2025-the-year-cybersecurity-crossed-the-ai-rubicon

https://www.forbes.com/sites/emilsayegh/2025/12/06/2025-cybersecurity-recap-the-year-systems-broke-setting-up-a-harder-2026/

https://intosecurity.fi/blogi/nis2-direktiivi-mitka-ovat-johdon-velvoitteet-ja-sanktiot/

https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis-2-euroopan-unionin-kyberturvallisuusdirektiivi/tarkeaa-tietoa#68867-2

https://deepstrike.io/blog/data-breach-statistics-2025

https://chiefexecutive.net/almost-90-cyber-attacks-caused-human-error-behavior/

https://threats.wiz.io/all-incidents/bybit-hack

https://yrityksille.elisa.fi/ideat/kyberturvallisuuden-trendit-vuonna-2026-ai-vastaan-ai-ja-8-muuta-havaintoa/

https://www.techrepublic.com/article/news-5-cybersecurity-predictions-2026/

https://www.forbes.com/sites/emilsayegh/2025/12/06/2025-cybersecurity-recap-the-year-systems-broke-setting-up-a-harder-2026/

https://www.paloaltonetworks.com/cybersecurity-perspectives/2026-cyber-predictions

https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/2026-cybersecurity-outlook.html?WT.mc_id=TC7-PL700_US_11FY26_AW_PM_CS_CY_TC-CISO_ADV-CRR_WHATS-AHEAD-FOR-CYBERSECURITY-IN-2026

Cyberwatch VIIKKOKATSAUS

JULKAISIJA Cyberwatch Finland | Nuijamiestentie 5 C, 04400 Helsinki | www.cyberwatchfinland.fi

KARI AHO

Kriittinen viestintä ja varautuminen murroksessa – mitä vuosi 2025 opetti ja mihin olemme menossa

Johdanto:

Vuosi 2025 toi varautumiseen ja kriittiseen viestintään paljon muutoksia. Uusi sääntely, kuten NIS2-direktiivi ja sen myötä voimaan astunut kyberturvallisuuslaki sekä aiemmin voimassa olleet lait, kuten valmiuslaki ja yksintyöskentelyn turvallisuuteen liittyvä lainsäädäntö, velvoittavat organisaatioita kehittämään toimintakykyään aiempaa järjestelmällisemmin. Näitä tietysti täydentävät myös erilaiset laatusertifikaatit vaatimuksineen, näistä esimerkkeinä ISO27001 tietoturvallisuuden hallintajärjestelmä ja ISO 45001 työterveys- ja työturvallisuusjohtamisen standardi.

Samalla toimintaympäristö on monimutkaistunut: häiriöt voivat syntyä nopeasti ja levitä laajalle toimitusketjuun. Näistä esimerkkeinä mm. tahalliset tietoliikenne- ja sähkökaapeleiden katkot, fyysiset sekä kyberhyökkäykset sekä yhtälailla vaikkapa tulipalo tai tuotantolinjan vikaantuminen.

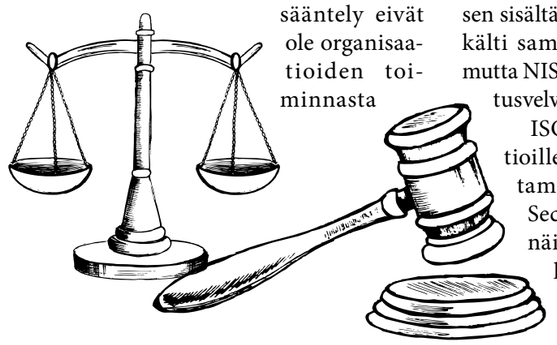
Näissä tilanteissa olennaista on, että viestintä, toimintamallit ja yhteistyö toimivat myös silloin, kun tilanne on päällä. Jotta tähän päästään, tulee organisaatioiden varautua, päivittää turvallisuussuunnitelmia ja toimintaohjeita ja ennen kaikkea harjoitella erilaisia tilanteita varten. Harjoittelu nostaa esiin kehitettäviä asioita, jotka viedään taas osaksi suunnitelmia ja ohjeita. Tämä muodostaa jatkuvan kehittämisen prosessin.

Vuosi 2025 jatkoi aiempien vuosien kehityssuuntaa, jossa uhkakuvat ja poikkeustilanteet ovat lisääntyneet ja toi varautumiseen sekä kriittiseen viestintään useita merkittäviä muutoksia. Muutokset eivät ole olleet äkillisiä, vaan tänä vuonna monet aiemmin keskusteluissa olleet uudistukset astuivat voimaan ja tulivat osaksi arkeamme. Myös turvallisuus- ja puolustusbudjetteja on kasvatettu vuoden 2025 aikana. Budjettien kasvattaminen on osaltaan johtanut toimintojen kehittämiseen ja lisännyt niihin käytettävää aikaa.

Samaan aikaan organisaatioissa on ymmärretty, että varautuminen on tärkeämpää kuin koskaan. Se ei ole erillinen projekti, jota tehdään kerran vuodessa, vaan osa jokapäiväistä johtamista. Kriisit ja häiriöt voivat olla harvinaisia, mutta ne ovat selkeästi yleistymässä ja niiden vaikutukset ovat laajoja. Siksi on olennaista, että organisaatiolla on kyvykkyys toimia nopeasti ja varmistaa toiminnan jatkuvuus myös silloin, kun poikkeustilanne iskee.

Nämä seikat ovat johtaneet siihen, että varautumisesta puhutaan paljon, mutta valitettavasti käytännön toteuttamisessa on vielä parannettavaa. MTV3 Uutiset kertoi 5.11.2025 artikkelissaan1, että vain harva yrityksistä on varautunut kunnolla. Artikkelin mukaan esimerkiksi teknologia-alan yrityksistä vain kolmanneksella on kirjallinen varautumissuunnitelma ja vain 10 prosenttia on testannut sitä käytännössä. Erityisesti harjoittelussa ja suunnitelmien testaamisessa on parannettavaa.

Tämän vuoksi korostan, että lait, direktiivit ja muu erilainen sääntely eivät ole organisaatioiden toiminnasta erillisiä vaatimuksia, vaan yksi keino varmistaa, että organisaation ja yhteiskunnan toiminta sekä työntekijöiden turvallisuus on varmistettu myös häiriötilanteiden aikana.



NIS2-direktiivi astui voimaan 8.4.2025

EU-maiden lainsäädäntöön vaikuttava NIS2-direktiivi, jonka vaatimukset on Suomessa katettu osana kyberturvallisuuslakia, auttaa organisaatioita varautumaan kyberturvallisuusriskeihin. NIS2 on tähän asti laajin kokonaisuus, joka ohjaa organisaatioita kehittämään kyberturvallisuuttaan suunnitelmallisesti. Sääntelyn kohteena on laaja joukko yhteiskunnan kriittisiä toimialoja. Velvoitteet astuivat Suomessa voimaan 8.4.2025, ja direktiivin tavoitteena on parantaa koko yhteiskunnan toimintavarmuutta.

Direktiivissä on listattu vähimmäistoimenpiteet, jotka kaikkien organisaatioiden on toteutettava varautuakseen ja hallitakseen niihin kohdistuvia kyberturvallisuusriskejä.

Standardit asettavat vaatimukset prosesseille, Secapin avulla jalkautat ne organisaatioon

Kyberturvallisuuden riskienhallinnan toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä on huomioitava ja ylläpidettävä ajantasaisena vähintään NIS2-direktiivin 21 artiklan sisältämän luettelon kymmenen keskeistä kohtaa. NIS2:sen sisältämät vaatimukset ovat pitkälti samoja mitä IS027001:sessä, mutta NIS2 sisältää tiukempia ilmoitusvelvollisuuksia.

ISO27001 antaa organisaatioille standardoidun toimintamallin, prosessit ja ohjeet. Secapp on taas työkalu, jolla näitä prosesseja voidaan jalkauttaa organisaatioon.

Mitä tulee NIS2:sen vaatimuksiin, secapp antaa organisaatioille työkalun, joka osaltaan auttaa vastaamaan kuuteen kymmenestä hallintatoimenpiteestä:

1. riskianalyysejä ja tietojärjestelmien turvallisuutta koskevat politiikat;
2. poikkeamien käsittely;
3. toiminnan jatkuvuuden hallinta, esimerkiksi varmuuskopiointi ja palautumissuunnittelu, sekä kriisinhallinta;
4. toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat;
5. verkko- ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus, mukaan lukien haavoittuvuuksien käsittely ja julkistaminen;
6. toimintaperiaatteet ja menettelyt, joilla arvioidaan kyberturvallisuusriskien hallintatoimenpiteiden tehokkuutta;
7. perustason kyberhygieniakäytännöt ja kyberturvallisuuskoulutus;
8. toimintaperiaatteet ja menettelyt, jotka koskevat kryptografian ja tarvittaessa salauksen käyttöä;
9. henkilöstöturvallisuus, pääsynhallintaperiaatteet ja omaisuudenhallinta
10. tarvittaessa monivaiheisen todennuksen tai jatkuvan todennuksen ratkaisujen, suojatun puhe-, video- ja tekstiviestinnän sekä suojattujen hätäviestintäjärjestelmien käyttö toimijan toiminnassa.

Kuten artiklasta käy ilmi, NIS2 ohjaa tekemään niitä asioita, mitä muutenkin organisaatioissa on oleellista tehdä toiminnan jatkuvuuden turvaamiseksi.

Valmiuslaki on keskeinen myös rauhan aikana

Suomessa valmiuslaki (1552/2011) muodostaa rungon sille, miten yhteiskunnan toimintaa turvataan häiriötilanteissa. Valmiuslaki ei ole vain aseellista kriisiä varautumista varten, vaan se ottaa kantaa myös myös muihin, todennäköisempiin, skenaarioihin.

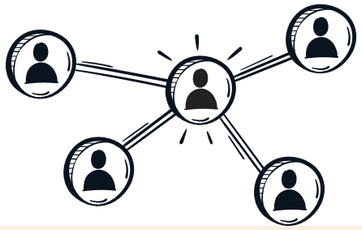
Arjen näkökulmasta todennäköisempiä skenaarioita ovat:

- tele- tai sähkökaapelien katkeamiset
- laajat verkkohäiriöt
- suuronnettomuudet
- sään ääri-ilmiöt, kuten myrskyt ja metsäpalot
- kyberhyökkäykset

Näissä tilanteissa yhteiskunnan kannalta keskeisten toimijoiden on pystyttävä reagoimaan nopeasti ja tuottamaan vähimmäispalvelut niin pitkälle kuin mahdollista. Valmiuslain keskeiset periaatteet ovat tärkeitä kaikille organisaatioille, eivät vain niille, joita laki suoraan velvoittaa.

Henkilöturvallisuus – perusta toimintakyvylle

Henkilöstö on aina organisaation tärkein voimavara. Onneksi tämä näkyy myös lainsäädännössä. Työturvallisuuslain (738/2002) mukaan



yksintyöskentelyyn ja työpaikan turvallisuuteen liittyvät riskit on arvioitava ja niihin on varauduttava.

Käytännössä tämä tarkoittaa:

- työntekijän on pystyttävä hälyttämään apua nopeasti
- hänen on voitava viestiä sijainnistaan ja tilanteestaan
- avun on päästävä perille ilman viivettä

Nämä ovat osa syistä miksi kriittisen viestinnän ja hälyttämisen järjestelmät ovat tänä päivänä olennainen osa monen toimialan arkea. Teollisuus, kunnossapito, terveydenhoito, pelastustoimi ja monet muut alat hyödyntävät järjestelmiä, jotka kasvattavat työntekijöiden turvallisuutta työskentelyn aikana.

Mitä organisaation kannattaa tehdä, ja ennen kaikkea mistä aloittaa?

Sääntelyn ja velvoitteiden määrä voi näyttää suurelta, mutta tarkemmin katsottuna ne ovat asioita, joita meidän pitää joka tapauksessa tehdä. Kokonaisuus on myös lopulta hyvin looginen. Hyvin toimiva varautuminen ei ole monimutkaista mutta se vaatii systemaattisuutta. **Kolme askelta riittää vauhtiin pääsemiseen:**

1. VARAUDU

Elämme nopeasti muuttuvassa toimintaympäristössä, jossa pelastussuunnitelmien, kriisivaste- ja muiden toimintaohjeiden täytyy olla ajan tasalla, selkeitä ja helposti löydettävissä, ei piilossa verkkolevyn kulmalla tai toimistolla fyysisessä kansiossa, jonka sijainnin muistavat vain harvat.

Tunnistakaa siis riskit ja tehkää selkeät toimintamallit niiden varalle. Paineen alla, kriittisissä tilanteissa, ihmisten toimintakyky altistuu virheille. Valmiit ohjeet, viestipohjat ja toimintasuunnitelmat voivat olla ratkaisevia tilanteen aikana.

Varautumista kannattaa ajatella jatkuvana prosessina, joissa kehitystoimenpiteitä tehdään vaiheittain. Ensimmäiseksi otetaan tekoon tärkeimmät asiat, myöhemmin muut asiat ja osa kuuluu jatkuvaan kehittämiseen.

2. VARMISTA TIEDONKULKU

Tiedon täytyy kulkea nopeasti ja luotettavasti: henkilöstölle, sidosryhmille ja tarvittaessa viranomaisille. Monet häiriötilanteiden ongelmat johtuvat tavoitettavuuden puutteesta. Suunnitelkaa, harjoitelkaa ja varmistakaa tiedonkulku häiriötilanteen aikana. Huolehtikaa myös, että teillä on varaviestintäkanava viestintään, jos organisaation pääjärjestelmät eivät ole käytettävissä.

3. HARJOITTELE

Harjoitukset kertovat, missä prosessit toimivat ja missä pitää parantaa.

Kyse ei ole siitä, että kaiken pitäisi olla heti valmista, vaan siitä, että toimintaa kehitetään askel kerrallaan. Harjoituksessa havaitut kehitystoimenpiteet viedään osaksi varautumisen suunnitelmia ja sitten niitä harjoitellaan uudestaan. Tämä muodostaa kehän, joka tukee jatkuvaa parantamista.

Harjoituksilla on rooli laissa, mutta ennen kaikkea ne ovat käytännöllinen tapa selvittää mitä pitää kehittää. Organisaatioiden ei aina ole välttämätöntä keksiä harjoituksia itse, vaan tarjolla on myös laadukkaita yhteiskunnan tarjoamia harjoituksia, kuten Digi- ja väestötietoviraston järjestämä vuosittainen Taisto-harjoitus.

Muut säätelyt: kemikaalit, kaasu, räjähteet ja kriittinen infrastruktuuri

Useat toimialakohtaiset säätelyt täydentävät NIS2:ta ja valmiuslakia.

Energia-ala, kemikaalit, räjähteet ja vesihuolto ovat muun muassa kaikki aloja, joissa yksittäinen häiriö voi aiheuttaa suurta vahinkoa.

Tämän vuoksi sääntelyissä korostetaan samoja periaatteita mitä muissakin laissa:

- Ohjeiden on oltava selkeitä
- Toiminta on suunniteltu etukäteen
- Viestinnän ja hälyttämisen täytyy toimia
- Yhteistyö viranomaisten kanssa on sujuvaa
- Toimintaa harjoitellaan ja dokumentoidaan

Yhteistoiminta on Suomen vahvuus, jota kannattaa vaalia

Asiakkaidemme ja sidosryhmiemme kautta olemme huomanneet, että yhteistyö on yksi Suomen suurimmista vahvuuksista. Harva kriisi koskettaa vain yhtä toimijaa ja tämän vuoksi viestinnän ja tilannekuvatiedon on kuljettava yli organisaatiorajojen. Esimerkiksi jos kaupungin yhdessä oppilaitoksessa on havaittu uhkaava henkilö, tulee siitä viestiä viranomaisten lisäksi myös kaupungin muille oppilaitoksille, kouluterveydenhuollolle ja kaupungille, muun muassa.

Suomessa organisaatiot ovat kehittäneet yhteistyömalleja, jotka kestävät vertailun kansainvälisesti. Konkreettisia esimerkkejä ovat hyvinvointialueiden ja kuntien yhteistyöverkostot, teleoperaattoreiden kriittisen infran yhteistoiminta sekä Huoltovarmuuskeskuksen poolit.

Näissä kokonaisuuksissa tarkennetaan rooleja, vastuita ja toimintatapoja poikkeustilanteissa sekä kehitetään yhteistyötä jatkuvasti. Tällainen yhteistoiminta on keskeinen osa koko yhteiskunnan turvallisuuden vahvistamista.

Secapp on tehty auttamaan organisaatioiden toiminnan jatkuvuutta

Secappin kriittisen viestinnän ja hälyttämisen ratkaisu on kehitetty tukemaan organisaatioiden valmiutta ja varautumista. Secappilla on yli 140 000 ammattilaiskäyttäjää, ketkä käyttävät sitä sekä arjen viestinnässä että häiriötilanteissa.

Secappin avulla hälytät henkilöstön ja sidosryhmän monikanavaisesti sekunneissa suunnitellun prosessin mukaisesti, viestit tietoturvallisesti tilanteen aikana ja ohjaat ihmiset ja muut resurssit oikeisiin tehtäviin. Voit viedä järjestelmään organisaationne turvallisuus- ja pelastussuunnitelmat ja tilanteen noustessa nämä suunnitelmat ovat kaikkien saatavilla ja jalkautettavissa nopeasti. Tämän ansiosta vaste paranee ja inhimilliset virheet voidaan minimoida.

Kaikki Secappissa tehdyt toimenpiteet tallentuvat automaattisesti lokiin, joka helpottaa tilanteeseen palaamista jälkikäteen ja raporttien toimittamista. Järjestelmän avulla voi myös kevyesti harjoitella erilaisia poikkeustilanteita varten ja testata suunnitelmia käytännössä.

Secapp toimii pilvipohjaisena erillisjärjestelmänä, jonka vuoksi sillä on korkea käytettävyys myös silloin, jos organisaation omat järjestelmät ovat alhaalla. Secappin SaaS-alustan tietoturvan hallinta on ISO 27001:2022-sertifioitu (Into Certification Oy). Lisäksi olemme täydentäneet sitä NIS2-vaatimuksilla. Hyödynnämme myös itse Secappia edellä mainittujen standardien vaatimuksien ja prosessien jalkauttamiseen.

Lopuksi – suunta on selkeä, ja matkaa tehdään yhdessä

Vuosi 2026 näyttää, miten hyvin organisaatiot ovat kiinni uudessa tavassa toimia. Mielestäni tärkeimmät asiat ovat kuitenkin nämä:

Varautuminen ei ole yhden henkilön työ, eikä se tapahdu kerralla, vaan sitä voi rakentaa palanen kerrallaan. Varautuminen rakentuu yhteistyöstä, harjoittelusta sekä nopeasta ja selkeästä viestinnästä.

Kun varaudumme, varmistamme tiedon kulun ja harjoittelemme, pysyy yhteiskunnan toiminta vakaana ja vaste nopeana myös epävarmoina aikoina.

VIITTAUKSET/LÄHTEET

1 MTV3 Uutiset, 5.11.2025 https://www.mtvuutiset.fi/artikkeli/jos-kriisi-iskee-suomen-infrasta-valtaosa-on-yritysten-hallussa-vain-harva-varautunut-kunnolla/9248400

KIRJOITTAJA:

Kari Aho

Toimitusjohtaja, Secapp

Secapp auttaa organisaatioita valmistautumaan ja reagoimaan erilaisiin kriisi- ja turvallisuusuhkiin. Kari Aho on ollut osa yritystä sekä turvallisuus- ja suojaussektoria yli 14 vuoden ajan.

Resilienssi – näkyvän maailman näkymätön selkäranka

KIMMO KASKI,
AAPO CEDERBERG,
TERHI KAJASTE,
CHATGPT5.1

On helppo kuvitella, että yhteiskunta pysyy kasassa sen lakien, infrastruktuurien ja talousjärjestelmien voimasta. Ne ovat tuttuja rakenteita, näkyviä ja käsinkosketeltavia. Niitä voi mitata, arvioida ja muokata. Mutta jos katsomme pintaa syvemmälle, näemme toisen, paljon tärkeämmän kudelman – sellaisen, joka ei näy toimintaympäristössämme, mutta ylläpitää sitä joka hetki muutoksienkin keskellä. Tämä kudelma on RESILIENSSI.

Resilienssi ei ole yksi kyky, eikä se ole tila, jonka voi saavuttaa ja sen jälkeen unohtaa. Se on jatkuva prosessi – eräänlainen hiljainen sopimus yksilöiden, yhteisöjen, organisaatioiden, teknologisten järjestelmien, yhteiskunnan ja luonnon välillä. Sopimus, joka sanoo: *kun maailma horjuu, me emme kaadu.*

Resilienssi on noussut aikamme avainkäsitteeksi, koska:

- ✔ Maailma on muuttunut vaikeammin ennakoitavaksi ja keskinäisriippuvaiseksi.
- ✔ Teknologinen ja yhteiskunnallinen haavoittuvuus kasvaa.
- ✔ Kriisejä ei voi estää, mutta niitä voidaan hallita ja niistä voidaan oppia ja siten uudistua.
- ✔ Luottamus, kulttuuri ja sosiaalinen pääoma ovat entistä kriittisempiä turvallisuustekijöitä.
- ✔ Tekoäly muuttaa sekä uhkien luonnetta että mahdollisuuksia torjua niitä.
- ✔ Resilienssi on edellytys sille, että moderni yhteiskunta on kriisinkestävä ja kykenee uusiutumaan nopeasti muuttuvassa maailmassa.

Toisin sanoen: resilienssi on tämän päivän ja tulevaisuuden yhteiskuntien sekä niiden eri rakenteiden keskeisin kyvykkyys – ei siksi, että maailma olisi epävakaa, vaan siksi että se on muuttunut pysyvästi vaikeammin ennakoitavaksi.

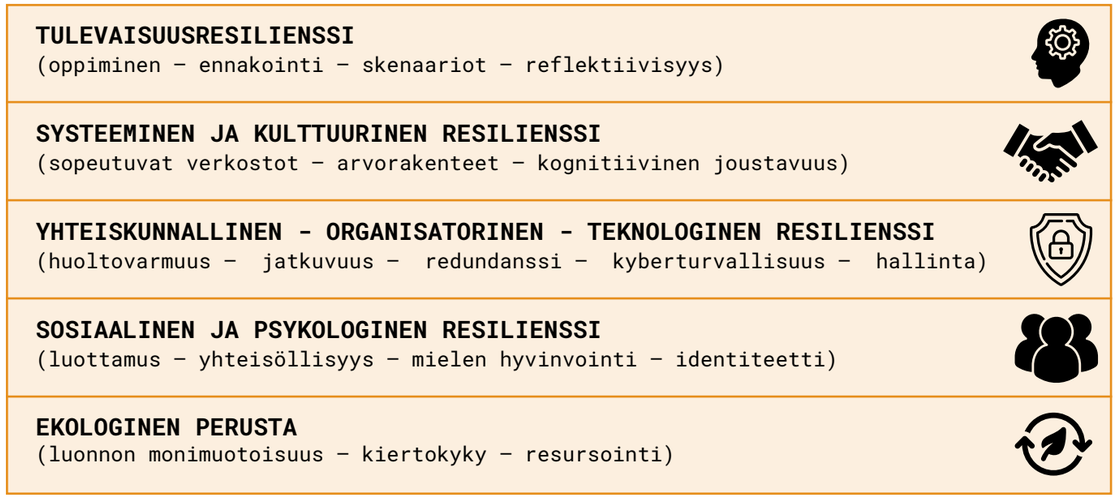
Kerroksellinen todellisuus

Resilienssiä voi ajatella kuin kaupunkia katsottuna ylhäältä ja systeemisesti. Sivusta katsottuna näemme kadut, rakennukset ja valot. Mutta kun alamme kuvitella kaupungin sisäisiä kerroksia, esiin piirtyy toinen tarina: ihmiset kiirehtivät töihin, järjestelmät siirtävät dataa valon nopeudella, verkot kuljettavat energiaa, yhteisöt jakavat hiljaista tietoa, organisaatiot tekevät päätöksiä, ja kaiken alla lepää luonnon hidas mutta väistämätön rytmi.

Resilienssi syntyy juuri tästä kerroksellisuudesta (Kuva 1). Alimpana on **ekologinen taso**, monimuotoisuus ja kiertokulut, jotka mahdollistavat fyysisen olemassaolomme. Sen päällä lepää **psykologinen taso**: ihmisten kyky sopeutua muutoksiin, menetyksiin ja kriiseihin, ylläpitää toimintakykyä ja löytää merkitys muutosten keskellä. Tämä taso kytkeytyy orgaanisesti **sosiaalisen tason resilienssiin**, joka koostuu luottamuksesta, solidaarisuudesta ja kyvystä toimia yhdessä.

Yhteiskunnallinen, organisatorinen ja teknologinen taso pitää sisällään yhteiskunnan kyvyn ylläpitää kriittiset toiminnot, yhteiskuntarauhan ja ihmisten toimintakyvyn häiriöiden keskellä, organisaatioiden taidon ennakoida, sopeutua ja jatkaa toimintaansa muuttuvissa ja yllättävissä olosuhteissa sekä teknisten järjestelmien ja infrastruktuurien kyvyn kestää häiriöitä ja palautua niistä ilman toimintakyvyn romahtamista.

Systeeminen ja kulttuurinen resilienssi sijoittuvat samalle tasolle keskenään, koska ne muodostavat yhdessä koko järjestelmän “ohjaavan



Kuva 1: Resilienssin monitasoinen systeemimalli

kerroksen": kulttuurinen resilienssi määrittää, millaisia arvoja, merkityksiä ja toimintatapoja kriiseihin liitetään, ja systeeminen resilienssi puolestaan säätelee, miten eri verkostot ja rakenteet reagoivat näihin muutoksiin ja tukevat toisiaan. Molemmat laaja-alaisia, emergenttejä ominaisuuksia, jotka eivät rajoitu yhteen toimijaan tai sektoriin, vaan vaikuttavat poikkileikkaavasti kaikkiin muihin resilienssin tasoihin. Yhdessä ne määrittävät, miten koko yhteiskunta kykenee oppimaan, sopeutumaan ja uudistumaan pitkällä aikavälillä.

Koko resilienssijärjestelmän ylimpänä kerroksena on **tulevaisuusresilienssi**, joka ohjaa kehityssuuntaa ja varmistaa, että haasteet muuntuvat osaamiseksi vahvistaen järjestelmän pitkän aikavälin kestävyyttä. Se yhdistää skenaariotyöskentelyn, strategisen ennakoinnin ja jatkuvan oppimisen niin, että sekä yksilöt, organisaatiot että yhteiskunta kykenevät mukauttamaan rakenteitaan uusiin uhkiin ja mahdollisuuksiin jo ennen kuin niistä tulee kriisejä.

Resilienssi on kerroksellinen kokonaisuus, jonka kerrosten välillä kulkevat palautesilmukat. Ne ovat kuin kaupunkia halkovia näkymättömiä käytäviä: jos yksi kerros muuttuu, muutos vaikuttaa väistämättä muihin.

Kompleksisuus ja sen varjo

Resilienssiä voi siis luonnehtia keskinäisriippuvuuksia sisältäväksi ekosysteemiksi. Sen osat eivät toimi irrallaan toisistaan, vaan ovat jatkuvassa vuorovaikutuksessa. Viime vuosien kriisit ovat tehneet tämän selväksi tavalla, joka on jättänyt jäljen sekä yksilöihin että instituutioihin. Kyberhyökkäys voi lamauttaa energiaverkon. Energiaverkon häiriö vaikuttaa logistiikkaan. Logistiikan ongelmat heijastuvat terveydenhuoltoon. Kun ketju katkeaa, koko järjestelmä alkaa haparoida. Kompleksisuutta lisää se, että systeeminen ajattelu on ihmiselle haastavaa, sillä se edellyttää laaja-alaista tietoa ja ymmärrystä yhdistettynä luovaan ajatteluun. Keskiöön nousee ihmisten, kansalaisten henkinen kriisinkestävyys ja kyky toimia kriisitilanteissa.

Tähän liittyy resilienssin ensimmäinen suuri haaste: ennakoimattomuus. Se ei synny vain siitä, että emme tiedä mitä tapahtuu, vaan siitä, että emme osaa kuvitella kaikkea sitä, mikä voi tapahtua. Resilienssi ei siis ole kyky pysäyttää kriisejä – vaan kyky hallita niitä eli estää niiden leviämistä, lyhentää niiden vaikutusaikaa, ja ennen kaikkea oppia niistä ja uudistua.

Resilienssin mittaamisen vaikea taito

Voiko resilienssiä mitata? Tämä kysymys nousee esiin aina, kun resilienssistä pyritään tekemään osa johtamista, strategiaa, riskienhallintaa tai yhteiskuntapolitiikkaa.

Kunnianhimoisesti resilienssi voitaisiin nähdä funktiona, jossa seuraavat viisi elementtiä määrittävät kokonaisuuden kestävyyden:

- **absorptiokyky** – kuinka suuri isku voidaan ottaa vastaan
- **kontrollikyky** – miten resurssit suunnataan kriisin keskellä
- **palautumisdynamiikka** – miten nopeasti järjestelmä löytää tasapainon
- **oppimiskyky** – muuttuuko toimintatapa seuraavalla kerralla
- **sopeutumiskyky** – pystyykö johtajat ja järjestelmä uudistumaan ilman romahdusta

Tämä on kuin orkesteri. Yksikään soitin ei yksin määritä esityksen laatua, mutta jos yksikin on pahasti epävireessä, kokonaisuus muuttuu.

Ulottuvuus	Mittariluokka	Esimerkki-indikaattoreita	Arviointimenetelmiä
Psykologinen	Psyykkinen joustavuus	Stressinsietokyky, toipumisaika, itsearviointiasteikot (CD-RISC, BRS)	Psykometriset testit, pitkittäistutkimukset
Sosiaalinen	Sosiaalinen pääoma	Luottamusindeksi, verkoston tiheys, osallisuuden aste	Sosiaalisen verkoston analyysit, kyselyt
Organisatorinen	Toiminnan jatkuvuus	MTTR (Mean Time to Recovery), redundanssikerroin, varautumissuunnitelmien kattavuus	Auditoinnit, riskianalyysit
Teknologinen	Järjestelmäkestävyys	Uptime-prosentti, varmuuskopiointisuhde, kyberturvaindeksi	Penetraatiotestit, stressitestit
Ekologinen	Ekosysteemin palautumiskyky	Biodiversiteetti-indeksi, hiilinielukapasiteetti, ekosysteemipalvelujen taso	Ympäristömonitorointi, satelliittidata
Yhteiskunnallinen	Kriisinkestävyys ja huoltovarmuus	Energiariippuvuus, elintarvikeomavaraisuus, kriittisten palvelujen saavutettavuus	Kansallinen riskinarviointi, huoltovarmuusanalyysi
Kulttuurinen/ kognitiivinen	Oppiminen ja mukautuvuus	Arvojen joustavuus, luottamus tietoon, reflektiivisyysindeksi	Narratiivianalyysi, kulttuuribarometrit
Systeeminen	Verkostojen redundanssi ja joustavuus	Kytkentätiheys, kriittisten solmujen määrä, palautesilmukoiden vahvuus	Kompleksisuusmallinnus, verkostoanalyysi
Tulevaisuus- ja oppimisresilienssi	Innovaatio- ja ennakointikyky	TKI-panokset, skenaarioprosessien määrä, resilienssiharjoitusten tiheys	Skenaariotyöpajat, foresight-mittarit

Taulukko 1: Keskeisiä resilienssiä kuvaavia ulottuvuuksia ja niiden tyypillisiä indikaattoreita.

Tänä päivänä resilienssin arvioinnissa käytettävät mittarit vaihtelevat psykologisista kyselylomakkeista teknisiin verkostomittareihin ja aina yhteiskunnan luottamusta arvioiviin indikaattoreihin asti. Resilienssi ei ole yksi numero – se on joukko suuntaviivoja, joiden avulla voimme nähdä, missä kudos on vahva ja missä se repeää. Alla olevassa taulukossa on listattuna joitakin eri resilienssin ulottuvuuksia kuvaavia indikaattoreita. Koska ihmisten ja johtajien merkitys on resilienssin ylläpitämisessä keskeinen, on harjoitusten rooli kriisinkestävyyden kehittämisessä ja mittaamisessa osoittautunut hyväksi toimintatavaksi.

Tekoälyn tulo – kun järjestelmä saa uudet aistit

Tämä on se kohta, jossa tarinaan astuu uusi roolihahmo: tekoäly. Sen myötä resilienssi ei ole enää pelkästään ihmisten rakentamaa – se on myös koneiden ymmärtämää ja hallitsemaa. Tekoäly ei väsy. Se ei kangistu ajattelumalleihin. Se ei pelkää kompleksisuutta, vaan elää siitä. Siinä missä ihminen näkee irrallisia pistemäisiä tapahtumia, tekoäly näkee verkoston - kokonaisuuden. Se pystyy lukemaan signaaleja valtavista tietovirroista – lokitiedostoista, sensoreista, sosiaalisesta mediasta, säädatasta, infrastruktuurien kuormitusluvuista. Sen kyky havaita heikkoja signaaleja tekee siitä eräänlaisen varhaisen varoituksen järjestelmän.

Tekoäly voi tunnistaa häiriön siemenen ennen kuin edes asiantuntija ymmärtää, että jotain on tekeillä. Mutta tunnistaminen on vasta alku. Tekoäly voi myös **simuloida** häiriöiden vaikutuksia, **optimoida** kriisiajan resurssien käytön ja jopa **ennaltaehkäistä** kriisejä ehdottamalla toimintatapojen muutoksia. Se voi mallintaa, miten häiriö leviää verkossa, mikä solmu on kriittisin, ja mikä toimenpide tuottaa suurimman vaikutuksen lyhyellä ja pitkällä aikavälillä. Tekoälyn myötä resilienssi saa uuden ulottuvuuden: se muuttuu **dataohjautuvaksi ja adaptiiviseksi**.

Resilienssialusta – yhteiskunnan digitaalinen hermosto

Tekoälypohjainen resilienssialusta muistuttaa ihmisen hermostoa. Se erottaa aistit, ajattelun, päätöksenteon ja muistin omiin kerroksiinsa:

- Datakerros on sensorinen järjestelmä – se kerää signaaleja kaikkialta.
- Analytiikkakerros tulkitsee ja ymmärtää, yhdistää ja ennustaa.
- Orkestrointikerros toteuttaa päätökset – automaattisesti tai ihmisen kanssa.
- Oppimiskerros varmistaa, ettei yksikään kriisi mene hukkaan ja oppiminen on jatkuvaa.

Tämä ei ole futuristinen visio, vaan uudenlaisen resilienssin väistämätön kehityssuunta. Se tekee resilienssistä jatkuvan tilannekuvan. Se siirtää painopisteen reagoinnista ennakointiin. Se muuttaa resilienssin staattisesta rakenteesta dynaamiseksi kyvyksi.

Tarina huomisesta

Kun resilienssiä tarkastellaan kaikkine kerroksineen ja suhteineen, se alkaa muistuttaa tarinaa ihmisestä itsestään, joka on aina etsinyt tasapainoa muutoksen keskellä ja pyrkinyt oppimaan virheistään, rakentamaan suojia, luomaan yhteisöjä sekä vahvistamaan niiden heikkoja kohtia. Resilienssi ei ole vain tekninen tai organisatorinen tavoite. Se on kulttuurinen arvo – kertomus siitä, että emme hyväksy haurauden olevan pysyvä tila. Se on kuvaus siitä, että vaikka maailma on monimutkainen, me voimme rakentaa järjestelmiä, jotka eivät pelkästään selviydy sen haasteista, vaan kasvavat niiden ansiosta.

Tulevaisuuden yhteiskunnat eivät ole niitä, jotka estävät kaikki kriisit. Ne ovat niitä, jotka **pystyvät elämään kriisien maailmassa murtumatta**. Ja ehkä tärkeimpänä: vahvimpia ovat yhteiskunnat, jotka ymmärtävät, että resilienssi ei synny ylhäältä tai alhaalta, vaan niiden kerrosten ja toimijoiden välisestä yhteistyöstä. Resilienssiä on siellä, missä psykologinen joustavuus kohtaa teknisen redundanssin, missä yhteisöt tukevat infrastruktuureja ja infrastruktuurit yhteisöjä, missä kulttuuri ohjaa tekoälyä – ja tekoäly auttaa meitä näkemään maailman selkeämmin.

Lopuksi

Resilienssi on näkyvän maailman näkymätön selkäranka. Se ei pysäytä myrskyjä, mutta se antaa meille mahdollisuuden purjehtia niiden läpi. Se ei estä kriisejä, mutta se estää meitä murtumasta niiden painosta. Se ei poista epävarmuutta, mutta se antaa meille keinot kohdata se rohkeasti ja ylläpitää yhteiskunnan kestävästi toimivana.

Ehkä resilienssin tärkein opetus on tämä:

Kestävä yhteiskunta ei ole vahva siksi, ettei se kaadu – vaan siksi, että se nousee aina uudelleen, viisaampana kuin ennen.

KIRJOITTAJAT:

KIMMO KASKI

Kimmo Kaski toimii emeritusprofessorina Aalto-yliopiston Perustieteiden korkeakoulussa, ja hänet tunnetaan kansainvälisesti tunnustettuna Laskennallisen Tieteen tutkijana. Hän on erikoistunut monimutkaisten järjestelmien tutkimukseen, käsittäen muun muassa sosiaaliset ja informaatioverkostot, ja hyödyntää työssään sekä suurten tietoaineistojen data-analytiikkaa että laskennallisia mallinnusmenetelmiä. Aalto-yliopistossa hän johtaa Digital Health, Wellbeing and Resilience -tutkimusryhmää, jonka tavoitteena on tuottaa myönteisiä vaikutuksia terveydenhuoltoon, yhteiskunnan hyvinvointiin, turvallisuuteen ja selviytymiskykyyn tutkimuksen ja datalähtöisten menetelmien avulla.

TERHI KAJASTE

Terhi Kajaste on kokenut asiantuntija ja mahdollistaja, joka on viime vuosina edistänyt tekoälyn tutkimukseen ja soveltamiseen liittyvää yhteistyötä Finnish Center for Artificial Intelligence (FCAI) -lippulaivaohjelmassa ja Digital Health, Wellbeing and Resilience -tutkimusryhmässä. Hänellä on laajalti kokemusta terveysteknologia-alasta ja viime aikoina myös turvallisuusalasta. Hänen taustansa yhdistää tieteellisen tutkimuksen ja teollisuusyhteistyön, mikä edistää ratkaisukeskeistä ja käytännön läheistä tutkimustyötä ja innovointia.

AAPO CEDERBERG

Toimitusjohtaja
ja perustaja

Cyberwatch Finland

Cyberwatch Finland

VIIKKOKATSAUSPOIMINNAT LOKAKUU-JOULUKUU

37/2025
Lunnashaittaohjelmat murroksessa

43/2025
Tuotanto - ja toimitusjärjestelmät kyberhyökkääjien kohteina

45/2025
Näin uhkatoimijoita tunnistetaan

47/2025
Datanhallinta on osa kyberturvallisuutta

49/2025
Olisiko Microsoftista irtaantuminen realistista tai turvallista?

Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

Lunnashaittaohjelmamarkkinat murroksessa

Lunnashaittaohjelmat ovat tällä hetkellä merkittävin yksittäinen organisaatioita koskettava kyberuhka. Ne estävät pääsyn omiin tiedostoihin, järjestelmiin tai verkkoon ja voivat pahimmassa tapauksessa yksittäisen päätelaitteen lisäksi kaapata jopa kaikki organisaation keskeiset palvelimet ja tietojärjestelmät. Alkuvuodesta 2025 yhdysvaltalainen Chainanalysis-yhtiö laski kiristyshaittaohjelmatoimijoille tietojen vapauttamisesta maksettujen lunnasmaksujen olleen vuonna 2024 yli 800 miljoonaa Yhdysvaltain dollaria. Kiristyshaittaohjelmien todelliset taloudelliset kustannukset ovat merkittävästi tätä korkeammat. Kustannukset koostuvat muun muassa liiketoiminnan häiriintymisestä tai keskeytymisestä sekä menetetystä datasta ja mainehaitasta. Merkittävimmät kohteet ovat perinteisesti olleet Yhdysvalloissa, jossa erityisesti maan terveydenhuoltosektori on ollut kiristyshaittaohjelmahyökkäysten kohteena. Suomessa Kyberturvallisuuskeskuksen tietoon on vuosittain tullut noin 40 kiristyshaittaohjelmatapausta todellisen määrän ollessa todennäköisesti jonkin verran suurempi, sillä kaikki tapaukset eivät tule viranomaisten tietoon. Uhreiksi on joutunut esimerkiksi kuljetusalan sekä rakennusalan yrityksiä.

Tällä hetkellä kiristyshaittaohjelmatoiminta on murroksen keskellä. Julkisten tietojen sekä datan ja tilastojen perusteella vaikuttaa siltä, että suuret kiristyshaittaohjelmatoimijat hiljalleen korvautuvat pienemmillä rikollistoimijoilla. Merkittävä syy tässä on viranomaistoiminta, sillä viranomaiset ovat onnistuneet operaatioissaan lopettamaan tai häiritsemään aiemmin suurten ja merkittävien toimijoiden, kuten Lockbitin ja AlphV/BlackCatin toimintaa. Jotkin ryhmät, kuten kesällä toimintansa lopettanut Hunters International, ovat ilmoittaneet toiminnan lopettamisen taustalla olevan kiristyshaittaohjelmatoiminnan kannattamattomuus ja riskit. Lisäksi on raportoitu hakkeriryhmien sisäisistä kiistoista.

Isojen kiristyshaittaohjelmatoimijoiden poistuessa markkinoilta uusien pienten toimijoiden määrä on kasvanut ennätysvauhtia. Heinäkuun 2024 ja kesäkuun 2025 aikana uusia kiristyshaittaohjelmatoimijoita havaittiin 40 kappaletta, ja parhaimmillaan ryhmiä havaittiin olleen samaan aikaan toiminnassa yli 60. Kuvaa kentän pirstaloitumisesta piirtää myös suurimmille kiristyshaittaohjelmaryhmille allokoitujen hyökkäysten määrä. Aiemmin 10 suurimman kiristyshaittaohjelmaryhmän laskettiin tekevän noin 70 % kaikista hyökkäyksistä, mutta sittemmin määrä on tippunut alle puoleen. Suurten ryhmien hajoamisen lisäksi teknologian kehitys ja erityisesti tekoäly ovat todennäköisesti helpottaneet uusien ryhmien perustamista ja toimintaa.

Käytännössä kehityksellä on monenlaisia vaikutuksia kyberuhkakuvaan, ja se tulisi tiedostaa organisaatioiden varautumisessa. Uusien ryhmien syntymisen ja hajoamisen sykli on nopeutunut huomattavasti, mikä tekee ilmiön ja toimijoiden seuraamisesta entistä vaikeampaa. Kiristyshaittaohjelmamarkkinoiden ollessa ”suurten toimijoiden” käsissä, toimintatavat ja niiden ennustettavuus auttoivat uhkaan varautumisessa ja tapausten estämisessä. Vaikka kiristyshaittaohjelmien uhriksi joutuneille ei ikinä suositella lunnaiden maksamista, sillä ne eivät takaa kryptattujen tietojen palauttamista tai kiristyksen loppumista, joidenkin ”luotettavien” kiristyshaittaohjelmatoimijoiden tiedetään toimineen lupauksensa mukaisesti ja palauttaneen uhrille kryptatut tiedot. Markkinoiden murros voi avata tietä aiempaa häikäilemättömämmille kyberrikollisille, ja lupauksiin tietojen palauttamisesta tulisi suhtautua aiempaakin skeptisemmin. Kyberrikollisille vakiintuneiden ryhmien ja ekosysteemin poistuminen tarkoittaa sitä, että luotettavia kumppaneita on yhä vaikeampi löytää. Tämä voi vaikuttaa kiristyshaittaohjelmien ja rikollisuuden tasoon, kun toiminta lepää aiempaa kapeammilla harteilla. Lyhyellä aikavälillä kenttä pysynee pirstaloituneena, vaikka pidemmällä tähtäimellä lunnashaittaohjelmamarkkina voi jälleen keskittyä.

Kiristyshaittaohjelmauhkaan varautumisessa perinteiset keinot ovat edelleen kultaa. Tilastojen valoissa onnistuneet hyökkäykset suoritetaan yhä valtaosin sosiaalisen manipuloinnin ja tietojenkalastelun avulla. Uhrit pyritään saamaan avaamaan saastuneita linkkejä ja asentamaan haitallisia sovelluksia päätelaitteelle. Henkilöstön koulutus ja tekniset rajoitukset uusien sovellusten asentamiseen päätelaitteille ovat hyväksi havaittuja keinoja uhkaan vastaamisessa.

Tuotanto - ja toimitusjärjestelmät kyberhyökkääjien kohteina

Syksyn aikana on nähty useita globaalisti huomiota herättäneitä kyberhyökkäyksiä, joiden vaikutus on ollut tuotantojärjestelmien (OT-järjestelmät) tai tuotteiden toimitusketjun häiriöt. Japanissa Asahi-panimon tuotteet loppuivat kaupoista kyberhyökkäyksen seurauksena, kun tilaus- ja toimitusluettelot hävisivät. Isossa-Britanniassa useat luksusautoliikkeet joutuivat jopa konkurssiuhkan alle, kun Jaguar Land Roverin tehtaat joutuivat pysäyttämään tuotannon. Molemmissa tapauksissa on kyse todennäköisesti taloudellisen motiivin hyökkäyksistä, joissa yhdeksi painostamisen keinoksi on valittu tuotteiden loppuasiakkaille päätymisen estäminen. Tämä on yleinen, mutta usein vähemmän huomiota saava osuus kiristyshyökkäyksiä. Kiristämisen kohteena ei välttämättä olekaan varastettu data, vaan tuotantoa tai toimitusjärjestelmiä saatetaan pitää pankkivankina lunnasrahoja vastaan.

Trendi tuntuu yleistyneen. Esimerkiksi Euroopan unionin kyberturvallisuusvirasto ENISA:n vuosittaisessa uhkakartoituksessa tuotantojärjestelmiin kohdistuvat hyökkäykset olivat kasvaneet huomattavasti. Tuotantoon ja toimitukseen liittyvät kyberhaasteet ovat hyvin tunnettuja, mutta vaikeasti ratkaistavissa. Järjestelmät ovat usein vanhoja, etäohjaukseen suunnittelemattomia laitteita, jotka on yhdistetty internetiin kasvaneiden tuotanto- ja valvontapaineiden myötä. Kyberturvallisuus ei ole usein ollut mukana alkuperäisissä suunnitelmissa, ja se on jouduttu suunnittelemaan ja implementoimaan jälkikäteen. Myös modernit järjestelmät ovat haavoittuvaisia. Uusimmat turvaominaisuudet tuovat järjestelmäpäivitykset voivat olla vaikeita asentaa ja vaativat usein toiminnan keskeyttämisen. Aina varmuutta niiden välittömästä toiminnasta ei ole. Päivittäminen aiheuttaa vähintäänkin hetkellisen keskeytyksen tuotantoon, mutta mahdollisesti myös pidempiaikaisia häiriöitä.

Toimitusjärjestelmiin iskeminen on harvinaisempaa, mutta ei ennen kuulumatonta. Toimitusjärjestelmät ovat usein kyberhyökkäyksissä olleet toissijainen kohde, mistä saadaan tietoa kohteen asiakkaista ja näiden tilausmääristä. Kuten Asahi-panimon tapaus osoittaa, myös niihin iskemällä ja dataa tuhoamalla voidaan aiheuttaa myös merkittävää vahinkoa. Etenkin suurempien organisaatioiden kohdalla tilaus-, logistiikka- ja sopimustietojen menettäminen voi johtaa tilanteeseen, jossa varmaa tietoa siitä kenelle ja mitä on toimitettu tai pitäisi toimittaa, ei ole. Tämänkaltaiset iskut ovat olleet yleisiä esimerkiksi merenkulun ja satamien kyberhyökkäyksissä, mutta Asahin tapaus osoittaa, että ne vaikuttavat rantautuvan myös maalle. Tilaus- ja toimitusjärjestelmiä ei välttämättä mielletä organisaatioissa arvokkaimmiksi kohteiksi, joten niiden suojaus voi olla muuta IT-omaisuutta heikompi.

Tuotantojärjestelmiin iskeminen ei välttämättä vaikuta pelkästään juuri siihen organisaatioon, johon hyökkäys kohdistuu. Esimerkiksi Land Roverin tapauksessa, suurimpiin vaikeuksiin joutuivat autovalmistajan sijaan myyjät, jotka olivat jo tehneet toimitussopimuksia autoista. Hyökkäykset aiheuttavat haasteita kohteen lisäksi sen kumppaneille tai asiakkaille, joiden toiminta nojaa tuotteiden saatavuuteen. Tuotannon keskeytymisellä voi olla merkittävä vaikutus myös organisaation luotettavuuteen ja tämä voi realisoitua vähentyvinä tilauksina tulevaisuudessa.

Tuotanto- ja toimitusjärjestelmiin kohdistuvat kyberuhkat ovat jatkuvasti kasvussa. Ne ovat korkealla taloudellista hyötyä tavoittelevien kyberrikollisten uhkalistoilla, mutta myöskään valtiollinen kybertoiminta tai haktivismi ei ole pois suljettua. Paras lääke kohteiden suojaamiseen on niiden pitäminen mahdollisimman irrallaan julkisesta internetistä. Etäohjausjärjestelmien tai niiden osien ei tulisi olla havaittavissa ulkoapäin. Sisäisiä yhteyksiä niiden ja oman IT:n välillä tulee pyrkiä valvomaan. Tärkeää on myös varautua häiriötilanteisiin, harjoitella toipumista, ja etenkin toimitus- ja tilausjärjestelmien kohdalla varmuuskopioida tärkeimmät tiedot.

Näin uhkatoimijoita tunnistetaan

Kyberhyökkäyksissä huomio kiinnittyy usein hyökkäyksen taustalla olevaan tahoon ja motiiveihin. Joskus hyökkääjän tunnistaminen voi olla helppoa – kiristyshaittaohjelmahyökkäyksen ohessa jätetty kiristysviesti tai pimeässä verkossa myyntiin tulevien tietojen kaupittelijan nimimerkki on helppo yhdistää hyökkääjään. Erityisesti valtiollisissa kyberhyökkäyksissä toimijan tunnistaminen voi olla huomattavasti hankalampaa, sillä ne eivät tyypillisesti tiedota julkisesti teoistaan. Myös valtiollisia uhkatoimijoita on kuitenkin onnistuttu nimeämään ja kyberhyökkäyksiä yhdistämään jopa tiettyihin turvallisuuspalveluihin ja niiden osastoihin.

Kyberuhkatoimijoiden nimeämiskäytännöt vaihtelevat ja sama uhkatoimija voidaan tuntea useilla eri nimillä. Microsoft hyödyntää nimeämisessään luonnonilmiöiden tematiikkaa, CrowdStriker eläimiä ja Mandiant numeroita. Ryhmillä voi olla myös muista yhteyksistä tunnettuja nimiä. Näin ollen esimerkiksi Venäjän tiedustelupalvelu FSB:hen liitetty Turla-uhkatoimija tunnetaan myös nimillä Secret Blizzard, Venomous Bear ja UNC4210. Tämänkaltaiset valtiolliset uhkatoimijat eivät jätä kiristyshaittaviestejä tai muita merkkejä toiminnastaan vaan pikemminkin pyrkivät häivyttämään omia jälkiään. Silti kaikesta verkossa tapahtuvasta toiminnasta jää aina jälki, mikä auttaa uhkatoimijan tunnistamisessa.

Käytännössä hyökkääjän tunnistamisen tukena käytetyt keinot voidaan jakaa kolmeen kategoriaan: käyttäytymisen, tiedostojen ja verkkoinfrastruktuurin avulla tehtyyn tunnistamiseen. Ensimmäisestä käytetään myös nimeä TTP-perusteinen seuranta (Tactics, Techniques ja Procedures), mikä tarkoittaa hyökkääjän käyttämien taktiikoiden, tekniikoiden ja toimintatapojen tutkimista ja analysointia. TTP-seurantaan on myös kehitetty työkaluja, joista tunnetuin on Mitre ATT&CK –viitekehys. Joskus uhkatoimijan tunnistaminen voi helpottua yllättävillä havainnoilla. Turla-uhkatoimijan hyödyntämän Snake-haittaohjelman tarkastelu on tästä oiva esimerkki. Haittaohjelman aktiivisuuden havaittiin osuvan varsin hyvin yhteen FSB:n työntekijöiden tunnettujen työaikojen kanssa, mikä helpotti haittaohjelman attribuointia juuri kyseiselle toimijalle.

Tiedostoperusteinen tunnistaminen ja verkkoinfrastruktuuriin perustuva tunnistaminen ovat teknisempiä tunnistamisen työkaluja. Tiedostoperusteisessa tunnistamisessa voidaan analysoida hyökkääjän käyttämiä haittaohjelmia tai haittaohjelmaperheitä. Muun muassa koodin, tiedostojen metatietojen ja sisäisten nimeämiskäytäntöjen avulla voidaan tunnistaa uhkatoimijoita ja liittää eri hyökkäyksiä yhteen. Verkkoinfrastruktuuriin perustuva tunnistaminen taas hyödyntää uhkatoimijoiden käyttämien domainien, IP-osoitteiden sekä palvelinten sijaintien ja tyyppien muodostamia tunnistetietoja, yhdessä muiden teknisten tietojen kanssa. Verkkotoiminnasta jääkin aina sormenjälkiä, joita seuraamalla voidaan päästä uhkatoimijan luokse.

Edellä kuvattujen kolmen selkeän tunnistamismetodin lisäksi on olemassa muita seikkoja, jotka tukevat tunnistamista. Kenties merkittävin rooli on julkisen ja yksityisen sektorin yhteistyöllä ja tietojen jakamisella. Muun muassa viranomaistahojen julkistama tiedustelutieto ja havainnot voivat tukea uhkatoimijoiden tunnistamista tilanteissa, joissa yksityisillä tietoturvayrityksillä ei ole pääsyä tiedonlähteille. Tilanne toimii myös toiseen suuntaan, sillä yritysten toimittamalla datalla tietoturvaloukkauksista ja asiakastapauksista on suuri arvo kyberhyökkäysten analysoinnissa koko yhteiskunnan tasolla.

Uhkatoimijat tiedostavat keinot, joilla heidän toimintaansa pyritään seuraamaan, ja pyrkivät hämäämään tai muokkaamaan omaa toimintaansa, jolloin seurantamenetelmien käyttö muuttuu haastavammaksi. Esimerkiksi tiedostopohjaista tunnistamista voidaan pyrkiä huijaamaan muokkaamalla yksittäisiä koodirivejä, jolloin haittaohjelman tiedosto ei ole identtinen aiempiin verrattuna ja sen tunnistamisessa käytetty hash-arvo muuttuu. Toimintaa pyritään varioimaan esimerkiksi käytössä olevien tietokoneiden kelloja muokkaamalla ja uusia palvelimia pystytetään sitä mukaa kun ne havaitaan viranomaisten tunnistamiksi. Käynnissä on siis jatkuva kilpajuoksu uusien tunnistustapojen ja niiden välttämisen välillä. Yksi mahdollinen ratkaisu voi olla tekoälyn ja koneoppimisen hyödyntäminen uhkatoimijoiden tunnistamiseen ja kyberhyökkäysten attribuointiin. Tekoäly pystyy ihmistä tehokkaammin esimerkiksi tunnistamaan haittaohjelmia sen voidessa ihmistä monin kerroin nopeammin skannata koodia ja havaita piilotetut tai muokatut haittaohjelmat, tai niiden osat, jotka on erikseen suunniteltu läpäisemään tavalliset palomuurit ja skannausmenetelmät. Teknologian kehitys voikin tässä tapauksessa toimia kyberpuolustajien tukena, vaikka myös kyberhyökkäysten voidaan olettaa kehittyvän tekoälyn avulla.

Datanhallinta on osa kyberturvallisuutta

Digitalisaation myötä datan määrä maailmalla kasvaa jatkuvasti. Joidenkin arvioiden mukaan datan määrä tuplaantuu joka toinen vuosi, minkä pitäisi herättää myös organisaatiot pohtimaan omaa datastrategiaansa sekä datan ja tiedonhallinnan käytäntöjään. Esimerkit maailmalta osoittavat, että kyberhyökkääjät pystyvät löytämään arvoa jopa tiedoista, joita organisaatiot itse eivät pidä arvokkaina. Enää ei voi paeta sen taakse, että itsellä ei ole arvokasta tai hyökkääjiä kiinnostavaa dataa. Myös lainsäädäntö, kuten EU:n yleinen tietosuoja-asetus GDPR sekä Suomessa keväällä voimaantullut laki kyberturvallisuudesta, velvoittaa pohtimaan käytäntöjä datan käsittelyn ja pääsynhallinnan suhteen.

Datan hallinnassa ensimmäisen askeleen tulisi sisältää kartoitus siitä, mitä kaikkea dataa organisaation hallussa on, missä se sijaitsee ja onko se tarpeellista. Dataa voi kertyä yllättävistäkin paikoista. Sitä kertyy työssä käytettävistä sovelluksista, ja sitä voivat työntekijöiden lisäksi tuottaa asiakkaat, yhteistyökumppanit ja muut sidosryhmät. Kaiken datan löytäminen ei välttämättä ole helppoa ja haasteita voi olla lisäksi sen merkityksen tunnistamisessa. Harva laskee esimerkiksi arvoa työkavereiden kanssa vaihdetuille Teams-viesteille, mutta kyberhyökkääjille tämäkin tieto voi olla arvokasta.

Datan kartoituksen jälkeen tulisi tunnistaa, kuka sen omistaa sekä kuka hallinnoi sen elinkaarta. Selkeät roolit ja vastuut estävät tilanteet, joissa tietoja säilytetään liian pitkään tai unohtuneet tietovarannot joutuvat väärinkäytösten kohteeksi. Tämän suhteen ei voi ylikorostaa organisaatioiden johdon merkitystä. Johdon rooli korostuu vastuita jakaessa ja kokonaisuutta hallitessa.

Kolmantena on kriittistä tunnistaa tarpeet datan suojaukselle. Hallussa olevaa dataa tulisi luokitella, esimerkiksi arkaluontoisuuden ja säilytysaikojen perusteella. Tämän yhteydessä hyödyllistä on pohtia samalla identiteetin ja pääsynhallinnan käytäntöjä. Yleisesti parhaana pidetään niin kutsuttua vähimpien oikeuksien periaatetta (principle of least privilege), jossa tietojärjestelmien käyttöoikeudet rajataan niin suppeiksi kuin mahdollista. Missään nimessä oikeuksia ei tulisi antaa massamittaisesti kaikkiin tietovarantoihin vain kätevyyden vuoksi. Organisaatioiden tulisi jatkuvasti arvioida onko datan hallinta tehty turvallisesti ja kestävästi. Tässä tulisi tähdätä jatkuvaan kehitykseen ja dokumentointiin. Datan merkitys tulisikin ottaa huomioon organisaation jatkuvuudenhallinnassa ja esimerkiksi riskienhallintasuunnitelmissa.

Paitsi että datanhallinnassa on kyse kyberturvallisuudesta, on kyseessä myös kustannuskysymys. Turhat tai jo vanhentuneet varmuuskopiot ja samojen tiedostojen sijainti useissa eri paikoissa aiheuttavat säilytyskustannuksia. Oman palvelinkapasiteetin ylläpito tai pilvipalveluiden käyttäminen tiedonsäilytyksessä ei ole ilmaista. Samalla datan hyödyntämistä tulisi pohtia – voidaanko aineistoa hyödyntää jollain tapaa liiketoiminnan tukena ja missä määrin se on mahdollista? Kaikessa toiminnassa tulisi silti muistaa taustalla kyberturvallisuuden vire, eli tiedon tulee olla asianmukaisesti suojattua ja vain erikseen auktorisoiduilla henkilöillä saa olla siihen pääsy.

Olisiko Microsoftista irtaantuminen realistista tai turvallista?

Joukko europarlamentaarikkoja, mukaan lukien Suomen Aura Salla (EPP), Mika Aaltola (EPP) ja Merja Kyllönen (The Left), lähetti viime viikolla EU-parlamentin puheenjohtajalle kirjeen, jossa vaaditaan parlamentin irtautumista Microsoftista ja useista muista yhdysvaltalaista teknologiapalveluista. Vaikka kirje voidaan tulkita poliittisena peliliikkeenä, on taustalla aitoja huolia. EU:n riippuvuus Microsoftista ja muista yhdysvaltalaisista digipalveluiden tuottajista on tunnistettu ongelmaksi nykyisessä geopoliittisessa tilanteessa. Aiheellisia kysymyksiä on noussut myös siitä, että tällä hetkellä eurooppalaisten käyttäjien datan valuu käytännössä maksutta yhdysvaltalaisille yhtiöille muun muassa tekoälyn kehitykseen. Pikainen irrottautuminen yhdysvaltalaisista toimijoista ei kuitenkaan ole realismia. Pidemmällä aikavälillä muutos olisi mahdollinen.

Merkittävin ongelma Microsoftin tuotteista siirtymisen tiellä ovat käytännön vaikeudet ja siihen liittyvät kustannukset. Julkiset organisaatiot, yritykset ja kuluttajat nojaavat merkittävässä määrin Microsoftin luomaan ekosysteemiin. Tämä on ymmärrettävää helppouden takia. Esimerkiksi yrityksille tarjolla olevat palvelupaketit tuovat yhden seinän kautta mukanaan useat organisaation vaatimista palveluista: toimistosovellukset, sähköpostin, pilvipalvelut, mahdollisuuden käyttäjänhallintaan sekä tietoturvapalvelut ja virusskannaukset. Lisäksi pääosa kaupallisista sovelluksista on kehitetty nimenomaan Windows-käyttöjärjestelmää varten.

Euroopassa ainoa varteenotettava vaihtoehto Microsoftille olisi siirtyä käyttämään Linux-käyttöjärjestelmää ja sille kehitettyjä ohjelmistoja. Toisten teknologiajättien, kuten Applen tuotteet eivät todennäköisesti olisi vaihtoehto, sillä yhtiö on Microsoftin tapaan Yhdysvalloista. Linuxille vastaavaa yhden seinän kautta toimivaa kattavaa ekosysteemiä ei toistaiseksi ole syntynyt. Esimerkiksi toimisto-ohjelmistot pitäisi tällä hetkellä ottaa yhdeltä palveluntarjoajalta, sähköposti toiselta ja virusturva kolmannelta. Vaihtoehtojen kartoittaminen vaatisi paljon työtä ja IT-ympäristön kokonaisuudenhallinta muuttuisi aiempaa haastavammaksi. Kuluja tulisi niin ikään henkilöstön kouluttamisesta. Uuteen ympäristöön ja ohjelmistoihin tottuminen voisi herättää muutosvastarintaa, aiheuttaa keskeytyksiä ja viivästyksiä organisaatioille. Nykyisessä Microsoftiin luottamisessa on kyse myös riskienhallinnasta. Globaalin suuryrityksen tuotteisiin luottaminen on helpommin perusteltavissa sidosryhmille, kuin suurella yleisölle tuntemattomien sovellusten käyttäminen, erityisesti mikäli kyberuhka sattuisi realisoitumaan.

Sinällään vaihtoehtoja Microsoftin ekosysteemille ja muiden toimijoiden kehittämille Windows-ohjelmistoille löytyy. Linuxin tapauksessa ne usein ovat maksuttomia avoimen lähdekoodin ohjelmistoja. Tällöin olisi mahdollista säästää lisenssikustannuksissa. Konsulttitoimisto North Patrolin selvityksen mukaan vuonna 2024 Suomen julkinen sektori maksoi lähes 1,2 miljardia euroa Microsoft-käyttöoikeuksista. Tämä summa olisi mahdollista investoida vaihtoehtoisten ohjelmistojen käyttöönottoon, kehittämiseen ja henkilöstön kouluttamiseen.

Kyberturvallisuuden kannalta siirtymä olisi todennäköisesti toteutettavissa turvallisesti. Itse asiassa Linuxia pidetään jopa turvallisempana käyttöjärjestelmänä kuin Windowsia, koska sitä vastaan on kehitetty vähemmän haittaohjelmia ja käyttöjärjestelmä on perusrakenteeltaan turvallisempi. Samoin siihen saatavilla olevat sovellukset ovat usein avoimen lähdekoodin ohjelmistoja, mikä mahdollistaa niiden auditoinnin. Toisaalta on syytä muistaa, että monet kyberuhkista eivät ole riippuvaisia käyttöjärjestelmästä. Jos työntekijä lankeaa tietojenkalasteluun ja syöttää salasanoja, joita käytetään vaikkapa verkkopalveluihin kirjautumiseen, säilyy uhka entisellään. Lisäksi Linuxillekin on kehitetty haittaohjelmia, ja tietoturvahaavoittuvuuksia voi piillä Linuxille kehitetyissä avoimen lähdekoodin ohjelmistoissa.

Siirtymistä Windowsista toiseen käyttöjärjestelmään tai Microsoftin ohjelmistoista toisiin ei voidakaan tehdä yhden yön aikana. Se ei myöskään maagisesti paranna organisaation turvallisuutta. Sen sijaan hyvä vaihtoehto olisi hiljalleen kartoittaa työssä käytettäviä ohjelmistoja ja sitä, onko niille tarjolla luotettavia vaihtoehtoja, jotka eivät olisi sidoksissa Microsoftiin tai muihin yhdysvaltalaisiin toimijoihin. Nämä muut palvelut voisivat aluksi toimia aiempien rinnalla ennen lopullista siirtymää. Vaihtoehtojen tarkastelu ja varajärjestelmien omaaminen olisi hyödyllistä riskienhallinnan ja varautumisen kannalta, esimerkiksi kuvitteellisessa skenaariossa, jossa Microsoftin palveluihin tulisi maailmanlaajuinen häiriö.

Euroopassa erityisesti Tanska on pyrkinyt eroon yhdysvaltalaisista palveluntuottajista alkuvuodesta julkisuutta saaneen Grönlanti-kiistan jälkeen. Maan digiministeriö on valmistellut siirtymistään Microsoft Office -ympäristöstä avoimen lähdekoodin LibreOfficeen tämän vuoden aikana. Maan kaksi suurinta kaupunkia, Kööpenhamina ja Aarhus, ovat samalla tiellä ja vaihtaneet lisäksi pilvipalveluidensa toimittajat Microsoftista eurooppalaisiin vaihtoehtoihin, ja näin säästäneet merkittäviä summia rahaa. Askeleet kohti digitaalista itsenäisyyttä ja riippumattomuutta yhdysvaltalaisista toimijoista ovat siis mahdollisia. Mikäli EU ja EU-maat alkavat laajemmin siirtyä suosimaan eurooppalaisia vaihtoehtoja, toisi lisääntynyt kysyntä markkinoille todennäköisesti uusia palveluntarjoajia, kehittyneempiä tuotteita ja kilpailua. Organisaatioille siirtymä voi pitkässä juoksussa tuoda kustannussäästöjä, verrattuna lisenssimaksujen maksamiseen yhdelle lähes monopoliasemassa olevalle yhtiölle.

LÄHTEET:

Lunnashaittaohjelmamarkkinat murroksessa

https://therecord.media/ransomware-gang-takedown-proliferation

https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

https://www.theregister.com/2025/07/03/hunters_international_shutdown/

https://yle.fi/a/74-20124700

Tuotanto ja toimitusjärjestelmät kyberhyökkääjien kohteina

https://www.bbc.com/news/articles/c0r0y14ly5ro

https://www.bbc.com/news/articles/cwydxpdgx61o

https://edition.cnn.com/2025/10/08/business/japan-asahi-cyberattack-readiness-intl-hnk

Näin uhkatoimijoita tunnistetaan

https://www.virusbulletin.com/uploads/pdf/conference/vb2024/papers/Unveiling-shadows-key-tactics-for-tracking-cyber-threat-actors-attribution-and-infrastructure-analysis.pdf

https://attack.mitre.org/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a

Datan hallinta on osa kyberturvallisuutta

https://www.avoindata.fi/fi/opas/kartoita-tietovarannot

Olisiko Microsoftista irtaantuminen realistista tai turvallista?

https://www.eppgroup.eu/fi/mita-me-teemme/with-eu-countries/suomi/salla-eu-n-ja-suomen-lopetettava-microsoftin-kaytto

https://www.politico.eu/article/get-us-off-microsoft-eu-lawmakers-press-parliament-to-change-in-house-it/

https://therecord.media/denmark-digital-agency-microsoft-digital-independence

Cyberwatch VIIKKOKATSAUS

JULKAISIJA Cyberwatch Finland | Nuijamiestentie 5 C, 04400 Helsinki | www.cyberwatchfinland.fi

Cyberwatch Finland

KUUKAUSIKATSAUS

JOULUKUU/2025

Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

Tässä katsauksessa

Tässä kuukausikatsauksessa tarkastelemme edellisen kuukauden merkittävimpiä kybermaailman tapahtumia ja sidomme ne laajempiin kokonaisuuksiin. Katsaus jakautuu kolmeen tarkastelukulmaan: kuukauden merkittävimpiin kybermaailman tapahtumiin, ilmiöihin, joita haluamme erityisesti korostaa sekä kokonaisuuksiin, joiden kehitystä kannattaa seurata.

1 TAPAHTUMIA KYBERMAISEMASSA

Marraskuussa mediatilaa hallinneet otsikot Ukrainan sodan rauhansuunnitelmista eivät heijastuneet rintamalle, saati kybermaailmaan asti. Kuukauden merkittäviin kyberhyökkäyksiin kuuluvat muun muassa Ukraina-mielisen haktivistiryhmä Ukrainian Cyber Alliancen (UCA) kyberhyökkäys Donbas Postiin, eli miehitettyjen alueiden postipalveluun. Haktivistien omien väitteiden mukaan hyökkäyksen seurauksena onnistuttiin tuhoamaan useita terabitteja dataa, vaikuttamaan tuhannen työaseman ja noin sadan virtuaalikoneen toimintaan.

Kuukauden aikana Venäjä kohtasi muitakin kyberhyökkäyksiä, joiden taustalla arvellaan olevan ukrainalaisten tahojen. Merkittävän VSK-vakuutusyhtiön verkkopalvelut ja mobiilisovellukset kokivat miljooniin asiakkaisiin vaikuttavia häiriötä. Lisäksi Baltiassa, Mustalla merellä, Kauko-Idässä ja arktisella alueella toimiva satamaoperaattori Port Alliance raportoi kyberhyökkäyksistä, joiden vaikutukset eivät kuitenkaan olisi ilmeisesti vaikuttaneet sen operatiiviseen toimintaan. Tapahtumat ovat osoitus kybersodassa edelleen jatkuvista hyökkäyksistä, jotka tekevät sodasta näkyvän Venäjällä myös siviileille.

Myös Venäjän kyberaktiivisuudesta on tihkunut uutisia julkisuuteen. Alkukuussa slovakialainen kyberturvayritys ESET julkisti raportin, jonka mukaan Venäjän sotilastiedustelu GRU:n alainen Sandworm-ryhmä on pyrkinyt hyökkäämään Ukrainan vilja-, energia- ja logistiikka-alaa, sekä viranomaisia vastaan dataa tuhoavilla wiper-haittaohjelmilla kesän ja alkusyksyn aikana. Yhdysvalloissa kyberturvayhtiö Arctic Wolf tiedotti tunnistaneensa toisen GRU:n alaisen hakkeriryhmän, RomComin, hyökkäyksen paikallista insinööritoimistoa vastaan. Samanaikaisesti venäläinen haktivistiryhmä NoName057(16) on jatkanut hyökkäyksiään eurooppalaisiin kohteisiin. Erityisesti Tanskan paikallisvaalien yhteydessä nähtiin tuttuja palvelunestohyökkäyksiä poliittisten puolueiden ja medioiden verkkosivuille. Tällaista vaalihäirintää on vuoden 2025 aikana nähty useasti aiemmin esimerkiksi Moldovan, Puolan ja Romanian vaalien yhteydessä, ja sen voidaan olettaa jatkuvan tulevaisuudessakin.

Kyberhyökkäysten uhkan säilyessä korkealla, on länsimaissa pyritty parantamaan puolustuskyvykkyyksiä. Google Cloud ja Nato julkistivat marraskuun lopulla strategisen kumppanuuden, jonka tarkoituksena on parantaa Naton digitaalisia kyvykkyyksiä ja luoda korkean turvallisuustason pilviratkaisuja. Pilvipalveluiden turvallisuus ja rooli ovat puhuttaneet Suomessakin, ja myös yksityisten yritysten tulisi pohtia parhaita ratkaisuja omien tietojensa säilyttämiseen.

Yritysten ja organisaatioiden kohtaamista kyberuhkista merkittävimpänä on säilynyt edelleen uhka kiristyshaittaohjelmista. Mielenkiintoinen lähestymistapa ongelmaan nähtiin Iso-Britanniassa, jossa teknologiayhtiö Checkout ilmoitti joutuneensa ShinyHunters-kyberrikollisryhmän uhriksi. Vaadittujen lunnaiden maksamisen sijaan yhtiö tiedotti lahjoittavansa vaadittua summaa vastaavan rahamäärän paikallisille yliopistoille kyberturvatutkimukseen. Vaikka Checkout-menetti kyberhyökkäyksessä dataa, on sen vastaus kiristykseen saanut laajalti kehuja onnistuneesta maineenhallinnasta ja viestinnästä kyberhyökkäysten yhteydessä.

Arkipäivän kyberturvasta muistutus saatiin itävaltalaisten tutkijoiden julkaistua tutkimuksen yksinkertaisesta viestintäsovellus WhatsAppissa olleesta turvallisuushaavoittuvuudesta. Tutkijat havaitsivat, että käyttämällä WhatsAppin selainversiota WhatsApp Webbia, oli mahdollista massana ja suhteellisen nopeasti saada selville ihmisten puhelinnumeroita ja profiilitietoja. Yksinkertaisesti lisäämällä puhelinnumeron, vaikka satunnaisenkin, WhatsApp kertoi, onko numeroon liitetty profiilia sekä näytti profiilikuvan ja sen kuvauksen. Tutkijat pystyivät näin tarkistamaan noin 100 miljoonaa puhelinnumeroa tunnissa ja saivat lopulta selville 3,5 miljardin sovelluksen käyttäjän puhelinnumerot. 57 % tapauksissa haltuun saatiin profiilikuva ja 29 % profiiliin liitetty kuvausteksti. Sittemmin WhatsApp on tehnyt toimia vastaavanlaisen tietojenkaavinnan estämiseksi, mutta on korostanut, että periaatteessa kaikki vuotaneet tiedot ovat olleet julkisia tietoja - käyttäjillä on yksityisyysasetuksissa vaihtoehtona tehdä profiilikuvasta ja kuvauksesta yksityiset. Vaikka puhelinnumeron, kuvan ja kuvaustekstin vuotaminen ei välttämättä kuulosta isolta asialta, tietojen yhdistäminen muista lähteistä saatuihin tietoihin tarjoaa uhkatoimijoille aina mahdollisuuksia. WhatsApp-esimerkin tulisikin kannustaa tarkistamaan omat yksityisyysasetukset kaikissa käytössä olevissa digitaalisissa palveluissa.

2 VALOKEILASSA

2.1 Ensimmäinen koskaan tekoälyllä automatisoitu kyberhyökkäys?

Claude AI:n takana oleva Anthropic julkaisi äskettäin lausunnon tekoälyn käytöstä kyberhyökkäyksissä. Yrityksen mukaan sen tekoälymallia oli käytetty laajamittaisen automatisoidun kyberhyökkäysoperaation mahdollistamiseen noin 30 organisaatiota vastaan lähes ilman ihmisten panosta. Anthropicin mukaan hyökkäysten takana oli ”suurella todennäköisyydellä” kiinalainen valtion tukema kyberuhkatoimija tavoitteenaan kybervakoilu.

Hyökkäykset toteutettiin ilmeisesti manipuloimalla tekoälymallia uskomaan, että se työskentelee kyberturvallisuuden parissa lailliselle yritykselle. Jakamalla tehtävät pienempiin, vähemmän epäilyttäviin osiin voitiin välttää Clauden estojen kytkeytyminen päälle. Lopulta hyökkäykset olivat väitetysti 80–90 % automatisoituja, ja Claude toimitti yksityiskohtaisia raportteja, jotka sisälsivät varastettuja tunnuksia ja muuta arkaluontoista tietoa. Anthropicin uhkatiedustelujohtaja Jacob Kleinin mukaan Claude generoi tuhansia pyyntöjä sekunnissa. Toisaalta malli myös hallusinoi joitain tunnuksia ja muita yksityiskohtia, mikä viittaa siihen, että onnistuminen oli kaukana täydellisestä.

Tähän “epäonnistumiseen” olisi helppo takertua, ja monet kyberturvallisuuden ammattilaiset jopa kyseenalaistavat tapauksen täysin. Epäilykset johtuvat siitä, että Anthropic ei ole toistaiseksi julkaissut konkreettisia todisteita Clauden lähes automaattisesta käytöstä hyökkäyksissä, ja monet skeptikot pitävät tätä vain markkinointitemppuna, jonka avulla Claude vaikuttaisi paljon pätevämmältä kuin se todellisuudessa on. Vaikka ajatus saattaa kuulostaa epäuskottavalta, on yleisesti tiedossa, että nykyinen kilpailu tekoälymallien ja erityisesti agenttisen tekoälyn välillä on kovaa. Mahdollisuus väittää, että tekoälymalli pystyi suorittamaan operaation lähes itsenäisesti, voidaan nähdä merkittävänä saavutuksena, vaikka operaatio olisi ollut pahantahtoinen.

On mahdotonta tietää varmasti, onko kaikki, mitä Anthropic väittää totta. Todennäköisin vaihtoehto on, että hyökkäykset todella tapahtuivat, mutta Anthropic yrittää liioitella oman mallinsa suorituskykyä saadakseen sen näyttämään paremmalta ja kykenevämmältä kuin se todellisuudessa on. Sen tiedämme varmasti, että tekoälyä käytetään kyberhyökkäyksissä yhä enemmän, ja organisaatioiden on kaikkialla oltava tietoisia mahdollisista uhista, joita se voi aiheuttaa. Kuten Anthropic sanoi: hyökkäys on avannut tien tällaisten työkalujen hyväksikäytölle vähemmän kehittyneiden uhkatoimijoiden toimesta ja että tällaisia hyökkäyksiä tullaan varmasti näkemään enemmän tulevaisuudessa.

2.2 Ulkomaalaiset pilvipalvelut aiheuttavat uhkaa kansallisille kriittisille järjestelmille

Suomen oikeusministeriö päätti marraskuussa valita vaalidatan säilyttämisen uudeksi palveluntarjoajakseen yhdysvaltalainen palveluntarjoajan. Tämä tarkoittaa sitä, että suomalaisen vaalidatan käsittely ja säilyttäminen siirtyy ulkomaille. Lähes samanaikaisesti Kela ilmoitti siirtävänsä tietokantansa Suomesta paikallisilta palvelimilta ulkomailla sijaitsevaan pilveen. Molemmissa tapauksissa data siirretään Euroopassa sijaitseviin konesaleihin, joiden omistajia ja palveluntuottajia ovat yhdysvaltalaiset teknologiayhtiöt. Koska kyseessä olevat järjestelmät ovat kansallisesti hyvin merkittäviä ja kriittisiä, on niiden tietoturvan ja toimintavarmuuden takaaminen herättänyt aiheestakin huolta.

Historiasta on esimerkkejä tapauksista, joissa Yhdysvalloissa kaatunut palvelin on kaatanut myös eurooppalaisia palveluita. Keväällä 2025 taas Yhdysvaltojen presidentti Donald Trumpin päätös asettaa pakotteita Kansainvälisen Rikostuomioistuimen (ICC) pääsyyttäjälle, katkaisi pääsyyttäjän pääsyn työssään käyttämälle Microsoft tilille. Taustalla tässä oli ICCn aloittama tutkimus Israelin suorittamista ihmisoikeus- ja sotarikoksista Gazassa. Yhdysvaltojen yleisen poliittisen kehityksen ja nykyisen tavan tehdä politiikkaa onkin perustellusti nähty aiheuttavan geopoliittisen riskin eurooppalaisille organisaatioille, jotka luottavat yhdysvaltalaisiin palveluntarjoajiin.

Eri arvioiden mukaan pilviteknologian alueella Euroopassa omavaraisuusaste on 10–15 %. Tästä suurin yksittäinen eurooppalainen yhtiö kattaa vain kahden prosenttiyksikön osuuden. Tämä on pieni osuus, verrattuna yhdysvaltalaisiin megayhtiöihin, joista suurin kattaa noin kolmanneksen koko Euroopan markkinoista. Eurooppa onkin tällä hetkellä riippuvainen yhdysvaltalaisesta teknologiasta. Riippuvuuksista ja riskeistä Kiinan suhteen on puhuttu paljon, ja presidentti Trumpin toisen kauden aikana myös Euroopassa on herätty Yhdysvaltojen aiheuttamiin riskeihin. Niin teknologia-alan asiantuntijat, tutkijat kuin poliitikot ovat viime aikoina julkisesti esittäneet kannanottoja, että Euroopan on pyrittävä irti riippuvuudesta yhdysvaltalaiseen teknologiaan. Yksi kauhuskenaario on, että Yhdysvaltojen presidentin käskystä voisivat eurooppalaiset kriittiset järjestelmät lakata toimimasta. Vaikka yhdysvaltalaiset palveluntarjoajat rakentavat eurooppalaisille toimijoille Yhdysvalloista eriytettyjä järjestelmiä ja palvelinkokonaisuuksia Eurooppaan fyysisesti, nähdään edellä kuvattu ICC:n esimerkki varoituksena koko maanosalle.

Kyse ei ole siitä, etteikö yhdysvaltalaisissa yhtiöissä otettaisi tietoturvaa, tietosuojaa ja datan koskemattomuutta tosissaan. Kyse on geopoliittisesta riskistä ja siitä, että Yhdysvaltain hallinnon oikut voivat pakottaa teknologiayhtiöt toimimaan vaatimallaan tavalla, sillä muutoin heidän asemansa Yhdysvalloissa kärsisi. Kaikista kriittisimmät järjestelmät kannattaisikin niin Suomessa kuin Euroopassa pitää omassa hallinnassa tämänkaltaisten riskien välttämiseksi.

2.3 ”Pahan akselin” käsitys kumppanuudesta eroaa länsimaisesta

Venäjää, Irania, Pohjois-Koreaa ja Kiinaa on pidetty modernina ”pahan akselina”, ja tämä käsite on ulottunut myös kyberavaruuteen, suurelta osin maiden länsimaihin kohdistamien lukuisien vihamielisten kyberoperaatioiden vuoksi. Viime vuosina maat ovat vahvistaneet siteitään ja yhteistyötään ”rajoittamattomien kumppanuuksien”, ”kattavien sopimusten”, ”turvallisuuskumppanuuksien” ja jopa keskinäisten puolustussopimusten avulla. Olisi helppo ajatella, että tällainen yhteistyön ja kumppanuuden taso ulottuisi kaikille sektoreille, myös kyberalalle. Onhan edellä mainituilla mailla samankaltaiset tavoitteet länsimaisten demokratioiden ja sääntöihin perustuvan maailmanjärjestyksen heikentämisessä.

Jossain määrin kumppanuudet toimivat myös kyberavaruudessa, sillä marraskuun puolivälissä yhdysvaltalaisen Gen Digital -yhtiön julkaisema raportti esittää, että Venäjän ja Pohjois-Korean Advanced Persistent Threat (APT) -ryhmät ovat tehneet yhteistyötä. Jos tämä myöhemmin vahvistuu todeksi, tämä olisi ennennäkemätön löytö, sillä APT-ryhmät ovat perinteisesti olleet hyvin eristäytyneitä ja suojelevat omia menetelmiään. Lähin ennakkotapaus on työkalujen, kuten tiettyjen haittaohjelmien, jakaminen Venäjän ja Kiinan välillä. Samoin jotkut raportit viittaavat myös tekoälyyn liittyvään tiedon rajalliseen jakamiseen.

Venäjän ja Kiinan yhteistyö sai kuitenkin säröjä tässä kuussa, kun kiinalaisen APT-ryhmän vuosien ajan jatkunut soluttautuminen Venäjän tietojärjestelmiin paljastui. Ryhmä oli onnistunut soluttautumaan teknologiasektorin yrityksiin, varastaakseen tietoja hallituksen hankinnoista ja järjestelmien integraatiosta. Tällaiset tapaukset ovat olleet melko harvinaisia aiemmin, sillä virallisesti maiden on tarkoitus tehdä tiivistä yhteistyötä. Tämä korostaa länsimaiden ja Kiinan tai Venäjän kaltaisten arvojen eroja. Lännessä tällainen teko voisi vakavasti vaikuttaa suhteisiin ja yhteistyön jatkumiseen, mutta Kiinalla ja Venäjällä tämä todennäköisesti annetaan anteeksi ja unohdetaan pian. Kaikilta osin ja tarkoituksissa on mahdollista tai jopa todennäköistä, että Venäjä harjoittaa vastaavia operaatioita myös Kiinassa.

Vaikka länsimaisesta näkökulmasta saattaa vaikuttaa siltä, että nämä operaatiot ovat suorassa ristiriidassa yhteistyön vahvistamisen kanssa, näin nämä maat yleensä toimivat. Julkisesti sanottu voi olla melko erilaista, kuin mitä todellisuudessa tapahtuu, eikä edes korkea yhteistyötaso yhdellä sektorilla tarkoita, että kaikki haitalliset toimet keskeytettäisiin tai lopetettaisiin. Edes lähimmät liittolaiset eivät ole turvassa suoranaisilta vihamielisiltä operaatioilta. Myös länsimaiden tulisi pitää tämä mielessä rakentaessaan kumppanuuksia näiden maiden kanssa.

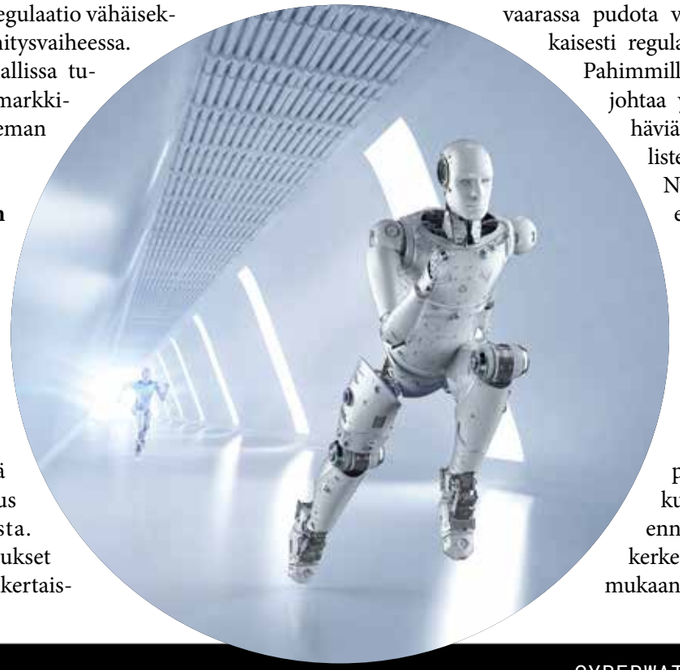
Tästä huolimatta mahdollinen uusi yhteistyötaso Pohjois-Korean ja Venäjän välillä voisi olla merkki uudesta strategiasta, jossa heidän suhteensa lähestyy länsimaiden odotuksia kumppanuudesta. Tällöin Pohjois-Korean odotetaan tukevan Venäjän tavoitteita myös kyberrintamalla. Toisin sanoen, Ukrainaa tukevien maiden tulisi varautua kohtaamaan lisää kyberhyökkäyksiä pohjoiskorealaisilta hakkereilta tulevaisuudessa.

3 SEURAA NÄITÄ

3.1 Vaihtuuko EU:n suunta digisääntelyn suhteen?

EU-komissio teki marraskuun 19. päivänä hieman yllättävän suunnanmuutoksen aiempaan digiregulaatiopolitiikkaansa, kun se laittoi jäihin tekoäly-regulaatiotyönsä, EU:n tekoälyasetuksen. Yksi syy tähän on tahto mahdollistaa eurooppalaisille tekoälyprojekteille vapaampi kilpailun yhdysvaltalaisia sekä kiinalaisia tekoäly-yhtiöitä vastaan. Toisena merkittävänä taustasyynä toiminnan muutokselle on arveltu olevan Yhdysvaltain hallinnon aggressiivinen tulliuhkailu. Yhdysvaltain presidentti Donald Trump on julkisuuteen todennut EU:n digiregulaation käytännössä olevan ”tullimaksujen perimistä mahtavilta yhdysvaltalaisyhtiöiltä” ja että regulaatioon voidaan reagoida tulleilla, mikäli muutosta ei synny.

EU on tunnettu vahvasta pyrkimyksestään reguloida sisämarkkinoitaan ja tavoitteestaan “Bryssel efektiin” eli vaikutusten saamiseen myös globaalisti. Toinen näkökulma AI-regulaation jäädyttämiselle on se, että EU tuntuukin nyt tiedostavan tekoälyn olevan kriittinen osa tulevaisuuden digiympäristöä ja sitä kautta myös talous- ja yhteiskuntaviitekehystä laajemminkin. Tämän takia EU haluaisikin tarjota eurooppalaisille jo valmiiksi reguloiduille yhtiöille mahdollisuuden taistella itsensä tekoälymarkkinoiden kilpajuoksuun mukaan, jonka jälkeen teknologian vakiinnuttua regulaatio seuraisi perässä. Tämä nyt omaksuttu toimintamalli digiregulaation jälkijättöisyydestä myötäilee Yhdysvaltain harjoittamaa regulaatiopolitiikkaa, jossa yritysten innovointia tuetaan jättämällä regulaatio vähäiseksi teknologian kehitysvaiheessa. Regulaatio tässä mallissa tulee jälkikäteen ja markkina-asetelmien jo hieman tasaannuttua.



Samalla, kun EU-komissio ilmoitti AI-regulaation jäädyttämisestä, ilmoitettiin myös komission uudesta Digital Omnibus -asetusehdotuksesta sekä sitä täydentävästä AI Digital Omnibus -asetusehdotuksesta. Nämä asetusehdotukset käytännössä yksinkertaistaisivat, keventäisivät sekä suoraviivaistaisivat EU:n nykyisiä regulaatiomenetelmiä. Tällä olisi tarkoitus parantaa EU:n kilpailua, vähentää kustannuksia, sekä selkeyttää ja helpottaa regulaation sisäistämistä sekä toteuttamista organisaatiotasolla. Kyseiset asetusehdotukset indikoivat kehityksestä, jossa EU haluaisi jatkossakin jossain määrin reguloida markkinoita, mutta aikaisempaa kevyemmin ja yksinkertaisemmin. Asetusehdotukset tulisivat voimaan loppuvuodesta 2026 tai vuoden 2027 aikana, jolloin tekoälymarkkinoilla olisi hetkellisesti vielä ”vapaat kädet” innovoida ja kehittyä ennen, kuin niitä valvottaisiin uusien asetusten muodossa.

Mitä tämä sitten tarkoittaa EU–kansalaisten ja yritysten näkökulmasta? Uusi ja löyhempi regulaatiomalli jättää väliaikaisen aukon EU:n aiemmin kovasti varjelemalle data- ja yksityisyyssääntelylle. Tämän aiemman tiukan sääntelyn tavoitteena on ollut taata datan ja yksityisyyden laaja suojaaminen niin eurooppalaisten kuin myös Euroopassa toimivien globaalien organisaatioiden osalta. Tästä hyvänä esimerkkinä on EU:n yleinen tietosuoja-asetus (GDPR). EU:n säätämän tietosuoja-asetuksen on käytännössä kopioinut omaan lainsäädäntöönsä jo yli 100 eri maata. GDPR säädös on siis toiminut EU:n tavoitteiden mukaisesti globaalina sääntelyvälineenä, joka on pakottanut globaalit teknologiajätit toimimaan GDPR:n mukaisesti muuallakin kuin pelkästään EU–alueen sisällä. Tapahtuva nopea teknologiakehitys etenkin tekoälypuolella on vaarassa pudota vähintäänkin väliaikaisesti regulaation ulkopuolelle. Pahimmillaan tämä saattaa johtaa yksityisyydensuojan häviämiseen taloudellisten tekijöiden takia. Nyt tuleekin toivoa, että teknologia-alan toimijat kuitenkin kunnioittavat vielä yksityisyydensuojaa siinä määrin, että tekoälyn kehittyessä itseregulaatio ja moraalikäsitykset pitävät teknologian kutakuinkin aisoissa ennen, kuin regulaatio kerkeää jälkijättöisesti mukaan.

3.2 Viranomaisten digivaltuuksia pyritään lisäämään maailmanlaajuisesti

Kansalaisten digitaaliset tiedot ja yksityisyys olivat näkyvä keskustelunaihe marraskuussa. Suomessa otsikoita keräsivät muun muassa lakiesitys veromenettelylain muutoksesta sekä mahdolliset muutokset perustuslain 10 pykälään. Ensimmäisen perusteella Verohallinto voisi päästä massana ja yksilöimättä käsiksi kansalaisten tilitietoihin. Jälkimmäinen taas laajentaisi tiedusteluvaltuuksia kotirauhan piiriin ja mahdollistaisi poliisin rikostiedustelun ilman konkreettista rikosepäilyä vakavassa järjestäytyneessä rikollisuudessa.

Euroopan tasolla paljon kiistelty Chat Control -asetus, jonka on pelätty vaikuttavan yksityiseen viestintään, sai EU-neuvoston, eli jäsenmaiden hyväksynnän. Alkuperäisestä ehdotuksesta poiketen, kansalaisten viestien skannaamisesta ei tehtäisi pakollista viestintäsovelluksia tarjoaville palveluille, mutta asetus mahdollistaisi sen ja tekisi siitä vapaaehtoista. Asetuksen läpimeno ei vielä ole varmaa, sillä seuraavaksi se etenee EU-neuvoston, parlamentin ja komission välisiin neuvotteluihin.

Keskustelua on ollut myös biometrisesta datasta. Yhdysvalloissa sisäisen turvallisuuden ministeriö DHS (Department of Homeland Security) julkisti marraskuussa suunnitelman kaikkien maahan saapuvien ja poistuvien ulkomaankansalaisten tietojen tallentamisesta kasvojentunnistusteknologialla. EU:ssa parlamentti antoi vihreää valoa ehdotukselle, joka antaa Europolille lisävaltuuksia datan jakamiseen ja biometristen tietojen tallennukseen ihmiskauppaa ja -salakuljetusta vastaan taistellessa. Europol oli muutenkin otsikoissa, viraston varapääjohtajan valitellessa Politico-lehdelle lainsäädännön, kuten datalainsäädännön ja perusoikeuksien, jarruttavan tekoälyn käyttöönottoa virastossa ja haitatessa rikosten selvittämistä. Tämä on loogista jatkumoa Europolin aiemmille kommenteille. Tammikuussa Europolin pääjohtaja totesi Internetin suuryhtiöiden velvollisuutena olevan kryptattujen viestien avaaminen, sillä muuten demokratia on uhattuna.

Digitalisaation edetessä dataa kansalaisista kertyy jatkuvasti enemmän. Samalla mahdollisuuksia datan keräämiseen ja tallentamiseen syntyy jatkuvasti lisää. Myös rikolliset ovat eturintamassa hyödyntämässä uusia teknologioita ja niiden tarjoamia mahdollisuuksia. On ymmärrettävää, että myös viranomaiset haluavat käsiinsä mahdollisimman tehokkaita työkaluja rikosten selvittämiseksi ja ennaltaehkäisyksi.

Tavallisten kansalaisten, demokratian ja oikeusvaltion näkökulmasta viranomaisten uusien oikeuksien ja toimivaltuuksien suhteen täytyy olla tarkka. Vaikka ajatukset taustalla ovat hyviä, mahdollisuudet väärinkäytöksiin ovat suuret. Ihmisten perusoikeuksiin, kuten oikeuteen yksityiselämän suojasta, ei tulisi puuttua. Kerran annettuja valvontaoikeuksia on hankala purkaa, ja poliittisten tuulien muuttuessa askel hyvää tarkoittavista ehdotuksista valvontadystopiaan voi olla yllättävänkin pieni.

Ylläesiteltyjä lainsäädäntöehdotuksia on perusteltu pääasiassa turvallisuusnäkökulmilla, kuten harmaan talouden kitkemisellä ja lasten suojelemisella. Toistaiseksi kansalaisyhteiskunta ei kuitenkaan ole selityksiä purematta niellyt. Suomessa media on varsin kriittisesti käsitellyt veromenettelylain muutosta, ja Chat Controlia vastaan on Euroopassa organisoitunut varsinainen kansalaisliike. Digitaalisen maailman muutos vaatinee valppautta jatkossakin. Median, järjestöjen, yritysten ja tavallisten kansalaisten rooli korostuu viranomaisten toimivaltuuksia tasapainottaessa.

LÄHTEET:

Tapahtumia kybermaisemassa

Cyberwatchin viikkokatsaukset marraskuu 2025
https://therecord.media/cyberattack-on-russian-port-operator
https://therecord.media/russia-vsk-cyberattack-outages
https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2025-q3-2025.pdf
https://www.bleepingcomputer.com/news/security/checkoutcom-snubs-shinyhunters-hackers-to-donate-ransom-instead/
https://www.googlecloudpresscorner.com/2025-11-24-NATO-and-Google-Cloud-Sign-Multi-Million-Dollar-Deal-for-AI-Enabled-Sovereign-Cloud
https://www.securityweek.com/vulnerability-allowed-scraping-of-3-5-billion-whatsapp-accounts/

Ensimmäinen koskaan tekoälyllä automatisoitu kyberhyökkäys?

https://www.bleepingcomputer.com/news/security/anthropic-claims-of-claude-ai-automated-cyberattacks-met-with-doubt/
https://www.axios.com/2025/11/13/anthropic-china-claude-code-cyberattack
https://www.anthropic.com/news/disrupting-AI-espionage

Ulkomaalaiset pilvipalvelut aiheuttavat uhkaa kansallisille kriittisille järjestelmille

https://yle.fi/a/74-20194842
https://yle.fi/a/74-20191502
https://yle.fi/a/74-20193175
https://www.tivi.fi/uutiset/a/fb1c44f8-8bd8-423a-8d16-c8f87742b760
https://www.is.fi/digitoday/art-2000011652212.html?utm_medium=promobox&utm_campaign=is_tf&utm_source=hs.fi&utm_content=promobox
https://www.tekniikkatalous.fi/uutiset/a/ec5bd01b-9aaa-4e08-b6cb-901af7dba00f
https://www.hs.fi/paakirjoitukset/art-2000011262613.html
https://www.euronews.com/2025/05/15/trumps-sanctions-on-icc-halt-tribunals-work-staffers-claim
https://yle.fi/a/3-11397638
https://www.thefastmode.com/expert-opinion/46136-reclaiming-european-cloud-sovereignty-following-the-aws-outage
https://www.bbc.com/news/articles/cev1en9077ro
https://www.politico.eu/article/microsoft-did-not-cut-services-international-criminal-court-president-american-sanctions-trump-tech-icc-amazon-google/
https://www.ksml.fi/uutissuomalainen/9029151

"Pahan akselin" käsitys kumppanuudesta eroaa länsimaisesta

https://www.politico.eu/article/russia-north-korea-partner-cyber-crime-research-gamaredon-lazarus/
https://www.gendigital.com/blog/insights/research/apt-cyber-alliances-2025
https://therecord.media/russia-report-apt31-china-linked-hacks
https://smallwarsjournal.com/2025/11/26/cybersecurity-strategies-china-russia-north-korea-iran/

Vaihtuuko EU:n suunta digisääntelyn suhteen?

https://www.politico.eu/article/ursula-von-der-leyen-eu-parliament-showdown-digital-red-tape-crusade/ https://www.politico.eu/article/brussels-police-world-digital-tech-us-china-regulations/ https://www.dittmar.fi/news/digital-omnibus/
https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal
https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal
Viranomaisten digivaltuuksia pyritään lisäämään maailmanlaajuisesti
https://fightchatcontrol.eu/
https://oikeusministerio.fi/en/project?tunnus=OM067:00/2024
https://protectnotsurveil.eu/uploads/ProtectNotSurveil-Europol_Paper.pdf
https://therecord.media/eu-parliament-committee-votes-europol-data-sharing-agreement
https://www.finlex.fi/fi/hallituksen-esitykset/2025/141
https://www.hs.fi/paakirjoitukset/art-2000011615798.html
https://www.politico.eu/article/europe-police-europol-want-ai-fight-crime-red-tape-stands-way/
https://www.wsj.com/articles/homeland-security-biometric-policy-for-foreign-travelers-poses-data-theft-risks-83cb5603?mod=cybersecurity_news_article_pos4
https://www.ft.com/content/1e6a600d-8620-4ed6-a4cd-5c454d6247ba

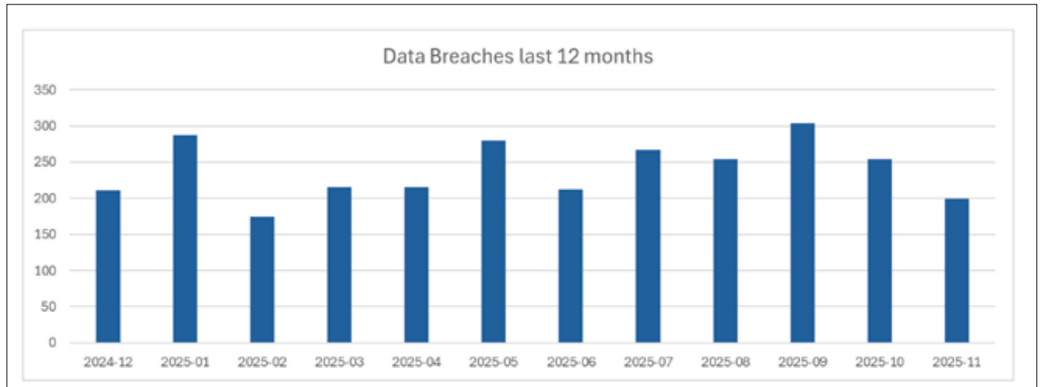
Cyberwatch KUUKAUSIKATSAUS

JULKAISIJA Cyberwatch Finland | Nuijamiestentie 5 C, 04400 Helsinki | www.cyberwatchfinland.fi

UHKATIEDUSTELUSEURANTA

Cyberwatch Finland julkaisee uhkatiedusteluseurannan, johon on koottu viimeisen kuukauden ajalta merkittävimpiä kyberhyökkäyksiä sekä tietoa aktiivisimmista ja nousevista uhkatoimijoista ympäri maailmaa. Cyberwatchin analyytikot seuraavat paitsi pintaverkossa, myös syvässä ja pimeässä verkossa tapahtuvaa toimintaa. Lähteinä on lisäksi kansainvälisten tietoturvatoimijoiden julkaisuja sekä laaja suomalaisen ja kansainvälisen mediakentän seuranta.

Merkittävimpiä kyberiskuja ja -kampanjoita



Tietomurrot kuukausittain viimeisen vuoden ajalta. Lähde: Cyber Intelligence House

(Huom. Graafi ei ota huomioon esimerkiksi palvelunestohyökkäyksiä, vaan vain tietomurrot, joissa dataa on todistetusti vuotanut)

DOORDASHIN TIETOMURTO

AJANKOHTA: 25.10.2025, tiedotettu 12.11.
KUVAUS: Ruokalähettiyhtiö DoorDash tiedotti marraskuussa asiakkaidensa, lähettikumppaneidensa ja alustalla tuotteita myyvien tahojen tietojen vuotamisesta. Tietomurron taustalla on uutisoitu olleen yrityksen työntekijään kohdistunut onnistunut käyttäjän manipulointi (social engineering), mikä olisi johtanut uhkatoimijan pääsyyn yhtiön järjestelmiin. DoorDash operoi yli 40 maassa, ja Suomessa se on tullut tunnetuksi ostettuaan suomalaisen start up –yritys Woltin.
TEKIJÄ: Julkisuuteen ei ole tullut tietoa hyökkäyksen toteuttajasta.
MOTIIVI: Todennäköisesti taloudellinen
VAIKUTUKSET: Yhtiö ei ole kommentoinut kuinka monen käyttäjän tietoja on vuotanut, mutta määrä lasketaan todennäköisesti miljoonissa. Ainakin kanadalaisten käyttäjien tietoja on vuotanut, mutta tietomurron vaikutukset voivat ulottua myös pidemmälle. Menetetyt tiedot voivat olla henkilöiden koko nimiä, osoitteita, puhelinnumeroita ja sähköpostiosoitteita. Tytäryhtiö Woltille kuuluvia tietoja ei tietomurron yhteydessä tiettävästi ole vuotanut.

RANSKALAINEN “KELA” SUUREN TIETOMURRON KOHTEENA

AJANKOHTA: 14.11.2025
KUVAUS: Ranskan Kelaa vastaavan URSSAF:in alaisuudessa toimiva Pajemploi toimii alustana kotihoidon järjestämiselle. Marraskuussa se joutui tietomurron kohteeksi, ja sen seurauksena onnistuttiin varastamaan yli 1,2 miljoonan lastenhoitajan henkilötietoja, jotka sisälsivät muun muassa henkilötunnuksia.

TEKIJÄ: Tuntematon
MOTIIVI: Tuntematon
VAIKUTUKSET: Tietojaan menettäneet lastenhoitajat ovat suuressa vaarassa joutua huijausyritysten tai jopa identiteettivarkauksien kohteeksi. Pajemploin mukaan sen oma toiminta ei häiriintynyt tapauksen seurauksena.

KNOWNSEC-TIETOMURTO PALJASTUI MAHDOLLISEKSI UUTISANKAKSI

AJANKOHTA: Marraskuun alku
KUVAUS: Marraskuun alussa useisiin kyberturvallisuudesta uutisoiviin medioihin ilmestyi uutisia kiinalaisen KnownSec-tietoturvayhtiön tietomurrosta. Uutisissa esitettiin, että yhtiöltä olisi vuotanut yli 12 000 tiedostoa GitHub-alustalle, jotka kuitenkin pikaisesti poistuivat. Paljastuneista tiedostoista olisi väitteiden mukaan selvinnyt yhtiön yhteydet Kiinan valtion toteuttamiin kyberhyökkäyksiin, hyökkäysten kohdelistoja ja edistyneitä kyberhyökkäystyökaluja. Tapahtuma olisi ollut merkittävä, sillä se olisi vahvistanut näkemystä yksityisten yritysten roolista kiinalaisessa kyberekosysteemissä.

TEKIJÄ: -
MOTIIVI: -
VAIKUTUKSET: Myöhemmin useissa lähteissä on kumottu alkuperäiset tiedot, ja tapahtumien ympärillä on tällä hetkellä epäselvyyttä. Vaikuttaa mahdolliselta, että tosiasiassa KnownSeciin liitettyjä tietoja on ollut myynnissä pimeässä verkossa loka-marraskuun vaihteessa. Uuden tietomurron sijaan kyseessä olisi ollut yhtiöön vuonna 2023 kohdistuneen tietomurron materiaaleja, mitkä sisältäisivät yhtiön työntekijöiden nimiä, sisäisiä koulutusmateriaaleja ja dataa pimeän verkon monitoroinnista.

CISCON JA CITRIXIN TUOTTEIDEN NOLLAPÄIVÄHAAVOITTUVUUDET

AJANKOHTA: Tiedotettu 12.11.2025, haavoittuvuudet on tunnistettu jo aiemmin, toukokuussa 2025
KUVAUS: Verkkojätti Amazonin uhkatiedusteluryhmä tiedotti marraskuussa verkkolaitevalmistaja Ciscon ja Citrixin tuotteissa havaituista nollapäivähaavoittuvuuksista ja niitä hyödyntäneistä hyökkäyksistä. Haavoittuvuudet koskivat Ciscon laitteidenhallintaan käytettyä Identity Services Engineä (ISE) ja Citrixin palveluita.
TEKIJÄ: Hyökkäysten taustalla on Amazonin mukaan edistynyt uhkatoimija, mutta hyökkäyksiä ei suoraan liitetty mihinkään tunnettuun valtioon tai kyberrikollisryhmään. Yksi hyökkäykseen liitetyistä IP-osoitteista on kuitenkin aiemmin ollut linkitetty RansomHub-kiristyshaittaohjelmatoimijaan.
MOTIIVI: Ei tiedossa
VAIKUTUKSET: Amazon ei ole tuonut julki hyökkäyksen onnistumisia tai niiden hyökkääjien tavoitteita. ISE-järjestelmää käytetään kuitenkin hallitsemaan verkkoihin pääsyjä, sitä kenellä on pääsy ja mihin osiin tietoverkkoja. Hyökkäykset vahvistavat vallalla olevaa trendiä, jossa uhkatoimijat keskittyvät hyökkäyksissään identiteetin- ja verkonhallinta infrastruktuuriin hyökkäämiseen.

Aktiivisimpia sekä nousevia uhkatoimijoita

KRAKEN RANSOMWARE

KUVAUS: Kyberrikollisorganisaatio, joka havaittiin ensimmäisen kerran helmikuussa 2025. Ryhmän uskotaan olevan HelloKitty-ryhmän uudelleenbrändäys. Tästä viitteitä antaa vuotanut lähdekoodi sekä maininta ryhmän ylläpitämällä pimeän verkon alustalla.
VIIME AIKOJEN TOIMINTA: Kraken Ransomwarella on kevään 2025 jälkeen yli 30 uhria monipuolisesti eri toimialoilta ja eripuolilta maailmaa. Uhriorganisaatioita on muun muassa Yhdysvalloissa, Kanadassa, Iso-Britanniassa, Panamassa, Kuwaitissa ja Tanskassa. Uhrien toimialoja ovat olleet rakennus-, hoito-, kosmetiikka-, autokauppa-, kenkäkauppa- sekä turvallisuusalan palveluntarjoajat. Kraken Ransomwarella on pimeässä verkossa toimiva sivusto, “The Last Haven Board”, jossa se käy neuvotteluja uhrien kanssa lunnaiden maksusta, datan palauttamisesta ja eteenpäin myymättömyydestä.
TOIMINTATAVAT JA TAKTIIKAT: Hyökkäyksissään Kraken hyödyntää usein Server Message Block (SMB) -haavoittuvuuksia uhrin tietojärjestelmiin sään pääsyssä. SMB on verkkoprotokolla, joka mahdollistaa tiedostojen, tulostimien ja muiden resurssien jakamisen ja yhdistämisen tietokoneiden välillä. Sisään järjestelmään päästyään Kraken hankkii käyttöönsä admin-tunnukset, joiden avulla se asettaa itselleen oikeuden hyödyntää Remote Desktop Protokollaa (RDP). Tämän etähallintajärjestelmän avulla hyökkääjä pääsee käsiksi uhriorganisaation tietokantoihin, kopioi ne itselleen, poistaa ne uhrin alustoilta, kryptaa alustat ja ottaa varmuusjärjestelmät pois käytöstä. Tämän jälkeen Kraken lähettää uhrille lunnasvaatimuksen sekä linkin neuvottelusivustolle. Kraken on myös ottanut toiminnassaan käyttöön ransomware-toimijoille hyvin epätyypillisen tehostustekniikan. Se testaa uhrin järjestelmää työkaluilla, joiden tarkoituksena on selvittää, kuinka nopeasti tietokannat voi kryptata ilman, että järjestelmä kaatuu ylikuormituksesta. Tämän testin avulla Kraken tekee päätöksen, kryptaako se uhrin järjestelmät kokonaisuudessaan vai ainoastaan kriittisiltä osin.

LUMMA MALWARE

KUVAUS: Lumma Malware tunnetaan myös nimellä Lumma Stealer tai Lumma Infostealer. Kyseessä on tietoa varastavien infostealer-haittaohjelmien ylivoimaisesti suurin ja laajimpaa vahinkoa aiheuttava haittaohjelma. Lumma operoi Malware-as-a-Service (MaaS) -toiminnalla, eli se kauppaa kehittämäänsä haittaohjelmaa muiden toimijoiden käyttöön. Lumman kehittäjien ja ylläpitäjien epäillään olevan venäläisiä.
VIIME AIKOJEN TOIMINTA: Lumman kehittämällä infostealer-haittaohjelmalla suoritetaan tällä hetkellä yli puolet kaikista infostealer-haittaohjelmahyökkäyksistä. Kyseisellä haittaohjelmalla varastetaan käyttäjätunnuksia, kryptovaluuttalompakoiden sisältämää dataa ja käyttöavaimia, henkilökohtaisia tietoja, istuntoavaimia (session tokens), monivaiheisen tunnistautumisen tunnuksia (MFA) ynnä muita kriittisiä tietoja.
TOIMINTATAVAT JA TAKTIIKAT: Haittaohjelmaa levitetään pääosin tietojenkalastelukampanjoiden, sosiaalisen manipulaation, haitallisen mainonnan (malvertaising) ja hakukoneoptimoinnin avulla. Myös sosiaalisen median linkkejä käytetään Lumman levityksessä. Näitten kautta uhrin laitteelle latautuu kyseinen tietoa varastava haittaohjelma, joka alkaa keräämään uhrin laitteelta kriittisiä tietoja. Haittaohjelmaa kehitetään ja sen toimintatapoja ja -tekniikoita sekä levitystapoja sekä -tekniikoita päivitetään jatkuvasti. Tämä tehdään toiminnan jatkumisen ja tehokkuuden varmistamiseksi. Lumman on muun muassa todettu lataavan uhrin laitteelle muita haittaohjelmia.

WATER SACI

KUVAUS: Brasilialaisiin pankkeihin on kohdistunut loka-marraskuun aikana laaja ja hyvin strukturoitu hyökkäyskampanja, jonka taustalla on tunnistettu vaikuttavan uhkatoimija, jonka operaation paljastanut Trend Micro nimesi Water Saciksi. Ryhmä on pyrkinyt levittämään “Maverick” ja “SORVEPOTEL” -haittaohjelmia useilla eri keinoilla, ja sen toimintaa etenkin marraskuussa on kuvattu aggressiiviseksi ja kiihtyväksi. Tiedossa ei ole onko operaation taustalla joku aiemmin tunnettu uhkatoimija, vai onko kyse täysin uudesta ryhmästä.

VIIME AIKOJEN TOIMINTA: Viimeisen kahden kuukauden aikana erittäin aktiivinen iskusarja on muokkautunut jatkuvasti, kohdevalikoiman ja hyökkäysten tavoitteiden pysyessä kuitenkin samoina. Iskut kohdistuvat pääosin Brasiliaan pankki- ja finanssialan toimijoihin ja tavoitteena on järjestelmiin tunkeutuminen ja haittaohjelman tartuttaminen. Ryhmä ei ole ilmoittanut itsestään tai onnistuneista operaatioista, joten tällä hetkellä ei ole varmaa tietoa siitä, mikä lopullinen tavoite on. Hyvin todennäköisesti haittaohjelmatartunnan avulla pyritään taloudellisen hyödyn saavuttamiseen. Tämä voi tarkoittaa joko sen kautta saavutetun takaportin myymistä muille rikollisille tai kiristyshaittaohjelman tartuttamista itse.

TOIMINTATAVAT JA TAKTIIKAT: Vaikka tarkat toimintatavat ovat muuttuneet operaation jatkuessa, pääasiallisena työkaluna on käytetty WhatsApp-viestisovellusta. Etenkin sovelluksen työpöytäversion kautta on lähestytty potentiaalisia uhreja lähettäen tarkoin rakennettuja linkkejä, joita sen enempää sovellus kuin monet palomuurit eivät tunnista haittasisällöksi. Ryhmä on valikoinut kohteikseen erityisesti BYOD (Bring your own device) -laitteita ja niiden käyttäjiä, joiden kautta tavoitellaan haittaohjelman tartuttamista organisaation verkkoon.

TENGU RANSOMWARE

KUVAUS: Ensimmäisen kerran lokakuussa 2025 havaittu uhkatoimija, joka on kuun vaihteen ensimmäisen operaation jälkeen iskenyt marraskuussa ainakin seitsemään organisaatioon ympäri maailman. Kyseessä on ilmeisesti täysin uusi rikollisryhmä, jolla ei ainakaan tämän hetken tiedon mukaan ole yhteyksiä muihin ryhmiin.

VIIME AIKOJEN TOIMINTA: Ryhmän operaatiot ovat kohdistuneet maihin, jotka eivät yleisesti ole olleet kovinkaan suosittuja ransomware-kohteita. Hyökkäyksiä on kohdistettu esimerkiksi Marokkoon, Iraniin, Yhdistyneisiin Arabiemiraatteihin, Espanjaan ja viimeisimmäksi marraskuun lopulla Meksikoon. Toimialoista suosituin kohde on ollut elintarviketuotanto kolmella iskulla, mutta datan vähäisen määrän vuoksi ei voida varmuudella sanoa onko tässä kyse sattumasta.

TOIMINTATAVAT JA TAKTIIKAT: Tarkoista menetelmistä tai yleisimmistä työkaluista ei tällä hetkellä ole kattavaa tietoa. Havaituissa hyökkäyksissä ryhmä on hyödyntänyt niin varastettuja käyttäjätunnuksia kuin huonosti suojattuja VPN-palvelimia, sekä kohdistettua kalastelua. Ryhmä vaikuttaa teknisesti melko kyvykkäältä, sen suorittaessa itse niin tunkeutumisen, kohdejärjestelmissä liikkumisen ja haittaohjelman lopullisen tartuttamisen. Kiristyksessä ryhmän on havaittu hyödyntävän kaksoiskiristystä.

Cyberwatch Finland

Kyberturvallisuuden kehityskaari

Cyberwatch Finland palvelee yrityksiä ja muita organisaatioita vahvistamalla ja kehittämällä niiden kyberturvallisuuskulttuuria. Tavoitteenamme on strategisen kybertietoisuuden ja -kyvykkyyden parantaminen toiminnan kaikilla tasoilla, yksittäisistä henkilöistä organisaatioiden ylimpään johtoon asti.
Kerromme kansantajuisesti kyberturvallisuuden ajankohtaisista ilmiöistä ja siihen vaikuttavista tekijöistä.

1. LÄHTÖTILANTEEN KARTOITUS
- Tarkastetaan yrityksen kybermaturiteetti
- Verkkoanalyysi ja haavoittuvuus-pinta-alakartoitus
- Toimintaympäristöanalyysi

2. TOIMINNAN VAKIINNUTTAMINEN
- Kyberturvallisuuslakitoimenpiteet & ohjeistus
- Riskienhallintasuunnitelma
- Cyber policy paper
- Yhteistyökumppanien osaamisen hyödyntäminen: mm. kyber-turvallisuuden toimintaohje ja toimija-analyysi

3. KOULUTUS JOHDOLLE JA HENKILÖSTÖLLE
- Tuotetaan tietoa kyberturvallisuu-desta toiminnan ollessa käynnissä koulutusten kautta
- Tilannekuvapalvelu: viikko- ja kuukausikatsaus
- Skenaarioharjoittelu asiakkaan kanssa

4. JATKOSEURANTA
- Ylläpidetään tilannekuvaa jatkuvan seurannan avulla ja annetaan tarvittaessa lisäkoulutusta
- Selvitetään toimitusketjujen turvallisuus ja tehdään niistä riskianalyysi/verkkoanalyysi

5. KEHITYKSEN TUKENA
- Johdon neuvontapalvelut
- Toimitusketjun auditointi
- Taustaselvitykset
- Cyber Due Diligence
- Vuosittainen skenaarioharjoitus ajankohtaisista kyberuhkista ja niihin varautumisesta

6. JATKUVUUDENHALLINTA
- Jatkoseurannat
- Henkilöstön koulutus
  –> esimerkiksi tilannekuva-palvelutallenteiden muodossa ja/tai toiveiden mukaan

Tilannekuvapalvelu

Cyberwatch seuraa jatkuvasti kyberturvallisuuden toiminta-ympäristöä keräämällä ja analysoimalla tietoa kyber-maailman tapahtumista, ilmiöistä ja muutoksista.

Tilannekuvaa tuotetaan ja ylläpidetään säännöllisesti ilmestyvillä tilannekatsauksilla.

Voit myös tilata 3 kk kokeilujakson tarjoushintaan!

Kysy lisää: info@cyberwatchfinland.fi

VIIKKOKATSAUS
Viikkokatsauksessa esitellään kybertoimin-taympäristön ajankohtaisia tapahtumia. Keskeistä viikkokatsauksessa on kyber-ilmiöiden ja trendien tunnistaminen ja nii-den asettaminen asianmukaiseen viiteke-hykseen. Viikkokatsaukset toimivat pohjana kuukausikatsauksille sekä vuosiennusteille. Viikkokatsausten avulla saat ajantasaista kuvaa merkittävistä kybermaailman tapah-tumista päätöksenteon tueksi. Viikkokat-saus ilmestyy 52 kertaa vuodessa suomeksi sekä englanniksi.

CYBERWATCH MAGAZINE
Cyberwatch magazine on digitaalinen ja painettu aikakauslehtemme, jossa sekä omat että verkostomme huippuasiantunti-jat kirjoittavat kybermaailman ajankohtai-sista tapahtumista, teknologian kehitykses-tä, lainsäädännön muutoksista sekä näiden vaikutuksista yhteiskuntaan, organisaatioi-hin ja yksittäisiin ihmisiin.

KUUKAUSIKATSAUS
Kuukausikatsauksessa tarkastellaan edel-lisen kuukauden merkittävimpiä kyber-maailman tapahtumia, ilmiöitä, trendejä ja niiden keskinäisriippuvuuksia sitoen ne laa-jempaan kokonaisuuteen. Katsaus jakau-tuu kolmeen tarkastelukulmaan, joita ovat kuukauden merkittävimmät kybermaailman tapahtumat, erityisesti korostettavat ilmiöt sekä kokonaisuudet, joiden kehitystä on syytä seurata. Kuukausikatsauksen avulla saat syvempää ymmärrystä siitä, miten kybermaailman tapahtumat vaikuttavat yh-teiskuntaan ja toimintaympäristöösi. Kuu-kausikatsaus ilmestyy 12 kertaa vuodessa suomeksi sekä englanniksi.

TEEMA- JA ERIKOISRAPORTIT
Tuotamme määrittelemästäsi teemasta, toimialasta tai kohdemarkkinasta erikois-raportteja ja katsauksia, kuten esimerkiksi uhkaraportteja, tulevaisuuskatsauksia ja -ennusteita, maa-analyyseja, toimintaymp-äristöanalyyseja tai muita erikoisraportteja.

Verkkoanalyysi - darkSOC®

LÄHTÖTILANNEKARTOITUS

DarkSOC® pimeän ja syvän verkon analyysi

- DarkSOC® -analyysi selvittää organisaation profiilin ja altistumisen tason pimeässä ja syvässä verkossa.
- Dataa kerätään ympäri maailmaa sijaitsevilla palvelimilla taukoamatta 9 Gb sekunnissa.
- Analyysi voi paljastaa muun muassa organisaation kyberturvallisuuden puutteita, vuotaneita tietoja ja muita mahdollisia ongelmakohtia.
- Analyysin avulla tuotetaan näkemys siitä, miltä organisaatio näyttää kyberrikollisen ja vihamielisten toimijoiden silmin katsottuna.

Haavoittuvuuspinta-alan kartoitus

- Haavoittuvuuspinta-alan kartoituksessa analysoidaan kohteen verkkoinfrastruktuurin rakennetta ja sen verkon kyberturvallisuuden tilaa kuudessa eri riskitekijäryhmässä.
- Haavoittuvuuspinta-alan osalta raportoidaan, miltä kohteen verkko näyttää ulkopuolisen tarkastelijan silmissä ja se kokoaa yhteen organisaatioon liittyvät verkko-omaisuuden osat kuten palvelimet, avoimet portit, sovellukset ja verkkosivut.
- Luokittelemme kyberaltistumiset kahdeksaan havaintokategoriaan ja jaamme havainnot vakavuuden perusteella kolmeen tasoon.
- Keskeisimmät havainnot raportoidaan johdon yhteenvetoraportissa päätöksenteon tueksi.
- Raportti sisältää havaintojen yksityiskohtaisemman esittelyn sekä suositukset korjaavista toimista ja strategisen tason kehityskohteista.

MONITOROINTI

Lähtötilannekartoituksen pohjalta voidaan sopia syvän ja pimeän verkon monitoroinnista toimenpiteiden vaikuttavuuden selvittämiseksi ja uusien uhkien havaitsemiseksi. Monitoroinnissa havaittuja uusia löydöksiä tarkastellaan suhteessa aiempiin havaintoihin ja analysoidaan syitä havaintomäärien muutoksiin. Monitoroinnin tulokset raportoidaan sovituin väliajoin.

- Säännöllinen monitorointi: sovituin aikavälein toimitettava raportti, esimerkiksi kuukausittain, kvartaaleittain, puolivuosittain tai vuosittain.
- Jatkuva monitorointi: 24/7 seuranta uusista havainnoista, joista tieto suoraan asiakkaalle sekä kuukausittainen raportointi.

Toimitusketjujen turvallisuus

NIS2 HALLINTATOIMENPIDE

Toimitusketjun toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt.

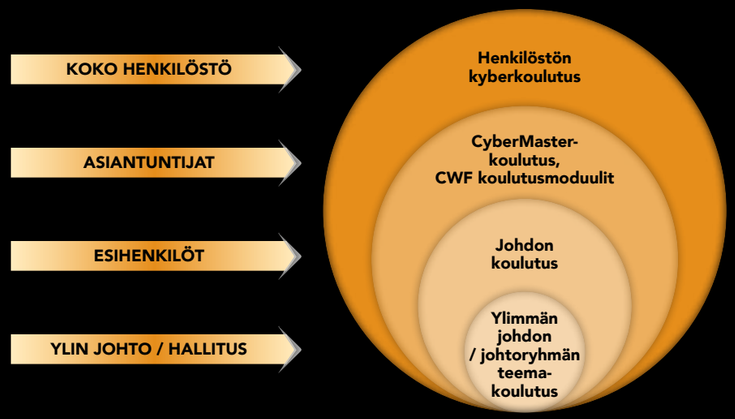
Analyysi voidaan tehdä valituille toimitusketjun organisaatioille (edellyttäen sopimusta). Havainnot jalkautetaan toimitusketjun organisaatioille, jotka vastaavat korjaavien toimenpiteiden suorittamisesta sekä raportoi tilaajalle, kun korjaavat toimenpiteet on tehty.

Palvelun sisältö esimerkiksi:

- Verkkoanalyysin esikartoitus toimitusketjun osille
- Verkkoanalyysi valituille toimitusketjun osille
- NIS2 käyttöönottokoulutus

Toimitusketjun kyberturvallisuuskäytäntöjen tarkastaminen lisää asiakasorganisaation omaa kyberkypsyyttä ja auttaa yritystä vastaamaan paremmin kyberturvallisuuslain vähimmäisvaatimuksiin. Mahdollistaa asiakkaalle esimerkiksi yritysostotilanteessa potentiaalisten yhteistyötahojen kybermaturiteettien selvittämisen ja riskiarvion tekemisen.

Koulutus ja osaamisen kehittäminen



CYBERWATCH-KOULUTUSMODUULIT JA LUENNOT

Toteutamme organisaatiollesi myös räätälöityjä koulutuskokonaisuuksia sekä luentoja, joiden avulla vahvistat kyberturvallisuuden osaamista ja valmistaudut kohtaamaan digitaalisen toimintaympäristömme muuttuvia haasteita.

Koulutustarjontamme koostuu moduulikokonaisuuksista sekä yksittäisistä luennoista, joista voit valita organisaatiollesi sen tilanteeseen tai toimintaan parhaiten soveltuvat osat. Koulutukset on mahdollista toteuttaa koulutuspäivinä, hybridikoulutuksina tai verkkokursseina. Koulutusten ja luentojen lisäksi voit tilata myös yrityksellesi skenaariotyöskentelyn, jonka avulla voit kerätä ja jäsentää tietoa, joka mahdollisimman kattavasti auttaa ymmärtämään tulevaa.

Esimerkkejä moduuleista:

Moduuli 1: Kyberturvallisuus ja johtaminen
Moduuli 2: NIS2 ja kyberregulaatiot
Moduuli 3: Kyberturvallisuusprosessi
Moduuli 4: Kyberriskit ja varautuminen
Moduuli 5: OT-turvallisuus
Moduuli 6: Hybridivaikuttaminen ja kybersota
Moduuli 7: Kyberrikollisuus
Moduuli 8: Kyberturvallinen yhteiskunta
Moduuli 9: Yhteiskunnan kriittiset rakenteet
Moduuli 10: Kyberkäsitteet haltuun

Esimerkkejä luennoista:

- Energiasektorin kybertilannekuva
- Logistiikkasektori kyberturvallisuus
- Satelliittien ja paikannus-järjestelmien kyberturvallisuus
- Kriittisen infrastruktuurin kyber-turvallisuus
- Terveyssektorin kyberturvallisuus
- Kybersodankäynti ja Ukrainan sodan vaikutukset kybertoiminta-ympäristöön
- Kyberturvallisuuden johtaminen ja kriisiviestintä
- Kyberhygienia
- Kyberrikollisuus
- Pimeä verkko

HENKILÖSTÖN TILANNEYMMÄRRYKSEN PARANTAMINEN

Voimaan astunut kyberturvallisuuslaki (NIS2) ja sen myötä mukaan tullut kyberriskienhallintavelvoite vaatii, että yritysten henkilöstöille tulee järjestää säännöllisesti koulutusta, jonka pyrkimyksenä on:

1) tietoisuuden parantaminen yleisesti kyberturvallisuudesta,
2) kyberhygieniakäytäntöjen kehittäminen ja
3) ymmärryksen ja tietoisuuden lisääminen ajankohtaisista kyberturvallisuusris-keistä.

Cyberwatchin henkilöstölle suunnattu kybertilannetietoisuus koulutuskokonai-suus vastaa tähän vaatimukseen. Sisältö muodostuu edellisen kuukauden aikana viikko- ja kuukausikatsauksissa käsitellyistä merkittävistä kyberilmiöistä. Koulutus pidetään henkilöstölle kerran kuukaudessa live streamina tai muuna etäkoulutuk-sena ja on kestoltaan noin 60 min.

MIF-KOULUTUSOHJELMAT

Tuotamme yhdessä Management Institute of Finlandin (MIF) kanssa Cyber Mas-ter erikoisammattitutkintokoulutusta. Tällä hetkellä koulutusohjelmissa voi suorit-taa Cyber Master Basics sekä Cyber Master Extended -koulutuskokonaisuudet. Koulutusten tarkoituksena on syventää ymmärrystä kyberturvallisuuden uhista ja tarjota käytännön työkaluja suojaamaan organisaation toimintaa.

Cyber Master Basics

Kurssin tavoitteena oppia kyberturvallisuuden perusteet ja rakentaa oman organisaa-tion kestävyyttä. Cyber Master -koulutus syventää ymmärrystä kyberturvallisuuden uhista ja tarjoaa käytännön ei teknisiä -työkaluja, joiden avulla kyetään suojaamaan organisaation toi-mintaa Koulutuksessa opit, kuin-ka rakentaa organisaation kykyä sietää poikkeus- ja häiriötekijöitä sekä hallita kriisitilanteita.

Koulutuksen sisältö:

- Toimintaympäristö ja johtaminen
- Kyberriskien hallinta
- Kyberresilienssi

Cyber Master Extended

Jatkokurssin tavoitteena vahvistaa kyberturvallisuuden osaamista ja viedä organisaation kyberturvallisuus uudelle tasolle. Cyber Master Exten-ded -koulutus tarjoaa syvällisemmän lähestymistavan kyberturvallisuuteen auttaen kehittämään organisaatiosi resilienssiä ja kykyä hallita kyber-uhkia yhdessä johtoryhmän kanssa. Koulutus on suunniteltu niille, jotka haluavat viedä kyberturvallisuuden strategiseen tasoon ja johtaa organi-saation kehitystä kokonaisvaltaisesti

Koulutuksen sisältö:

- Kyberjohtamisen syventäminen ja toiminnan suojaaminen
- Kyberturvan suunnittelu ja kehittäminen

AJANKOHTAINEN KURSSITARJONTAMME

KOULUTUSKOKONAISUUSESIMERKKI, SISÄLTÖ SAMA CYBER MASTER BASIC -KURSSILLA

Koulutuspäivä 1

Teema:
Toimintaympäristö ja johtaminen

1. Toimintaympäristö-analyysi
2. Henkilöön liittyvä kyberturvallisuus
3. Regulaatiovaikutukset
4. Kyberturvallisuuden johtaminen

\+ Etätehtävät

Koulutuspäivä 2

Teema:
Kyberriskien hallinta

1. Kyberriskien hallinta
2. Kyberrikollisuus
3. Teknologian kehittyminen
4. Tuotantoympäristöjen turvallisuus

\+ Etätehtävät

Koulutuspäivä 3

Teema:
Kyberresilienssi

1. Kyberturvallisuus-suunnittelu
2. Jatkuvuuden hallinta
3. Yrityksen kyberkulttuuri ja osaaminen
4. Case – analyysejä tapahtumista

\+ Etätehtävät

KOULUTUSPÄIVÄ KATTAA ISO27001 VAATIMUKSISTA:

Koulutuspäivä 1:
4 Org. toimintaympäristö
5 Johtajuus ja sitoutuminen

Koulutuspäivä 2:
6 Riskienhallinta

Koulutuspäivä 3:
8 Toiminta
7 Tukitoiminnat
(9 Suorituskyvyn arviointi)
(10 Jatkuva parantamien

KOULUTUSKOKONAISUUSESIMERKKI, SISÄLTÖ SAMA CYBER MASTER EXTENDED -KURSSILLA

Koulutuspäivä 1

Teema:
Kyberturvallisuuden varautuminen

1. Kyberturvallisuuden johtaminen
2. Kyberturvallisuuteen varautuminen
3. Riskien hallinnointi ja tunnistaminen
4. Identiteetin hallinta (IAM)

\+ Kehittämisprojekti +Etätehtävät

Koulutuspäivä 2

Teema:
Kyberturvallisuuden vaste

1. Iskujen havaitseminen ja reagointi
2. Kyberturvallisuuden palautuminen
3. Kvanttiteknologia
4. Kyberturvallisuuden muutos

\+ Etätehtävät

KOULUTUS KATTAA NIST- VAATIMUKSISTA:

Koulutuspäivä 1:
Govern, Identify, Protect

Koulutuspäivä 2:
Detect, Respond, Recover

Kyberriskienhallintamalli

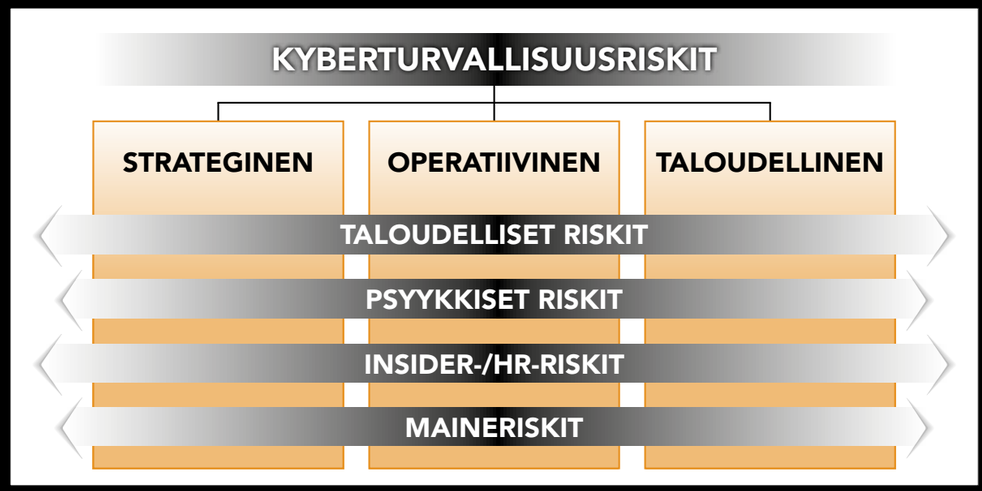
Kyberturvallisuus tulee yhä enemmän ottaa huomioon ennakoiden liiketoimintasuunnitelman eri vaiheissa. Kokonaisvaltaisessa kyber-turvallisuuden riskienhallintasuunnitelmassa laaditaan selkeä tiekartta siitä, miten kyberturvallisuusuhkat huomioidaan entistä paremmin ja miten lisääntyvä EU-regulaatio sekä kansallisen lainsäädännön edellyttämät toimet käytännössä toteutetaan.

Suunnitelma kattaa kyberturvallisuuden neljä osatekijää, johtamisen, tekniset ratkaisut, henkilöstön osaamisen ja toimintaprosessit.

Kyberriskien hallintamallin prosessi koostuu neljästä vaiheesta:

1. **Lähtötilanteen määrittelystä**
2. **Kyberriskianalyysista**
3. **Kyberriskien hallintamallista**
4. **Lopputuloksena toimivasta ja ennakoivasta kyberturvallisuusjärjestelmästä**

ALKUTILANNE	ANALYYSI	HALLINTAMALLI	LOPPUTULOS
1. Tarkastetaan organi-saation kybermaturiteetti -> verkkoanalyysi 2. Määritellään liike-toiminnan kyberuhkat ja riskit	Kyberriskianalyysi: - Henkilöstö - Teknologia - Prosessit Käytetään pohjana verkko-analyysin tuottamaa dataa	Kyberriskien hallinta - Uhkatilanteen jatkuva seuranta - Riskienhallintatoimet: henkilöstö, teknologia, prosessit	Kyberturvallisuusjärjestelmä: toimiva, uskottava & ennakoiva - Ylläpitää johdon tilanne-kuvaa - Liiketoiminnan jatkuvuudenhallinta



NIS2 Yrityskonsultaatio

Kyberturvallisuuslaki (NIS2)

Toimijoiden on toteuttava asianmukaiset ja oikeasuhteiset tekniset, operatiiviset ja organisatoriset toimenpiteet:

- **Hallitakseen riskejä**, joita niiden toiminnoissaan tai palveluntarjonnassaan käyttämien verkko- ja tietojärjestelmien turvallisuuteen kohdistuu.
- **Estääkseen tai minimoidakseen poikkeamien vaikutuksen** palvelujensa vastaanottajiin ja muihin palveluihin.

Toimijat jaetaan keskeisiin ja tärkeisiin.

Voimaan astunut uusi kyberturvallisuusdirektiivi (NIS2) on asettanut uusia velvoitteita yritysten digitaalisten riskien hallintaan. Näitä ovat muun muassa:

1) toimijan johdon kyberriskienhallinnan toteuttaminen ja valvonta
2) toimijaluetteloon ilmoittautuminen
3) koulutuksen järjestäminen jokaiselle henkilöstötasolle
4) toimitusketjussa olevien toimittajien tunnistaminen
5) poikkeamaraportointi.

TUEMME YRITYKSIÄ UUDEN LAINSÄÄDÄNNÖN KÄYTTÖÖNOTOSSA

Autamme muun muassa:

1) Koulutuksen järjestämisessä:
   - kyberturvallisuuslaki ja NIS2 käyttöönottokoulutus (2 h)
   - tilannekuvaseuranta henkilöstölle (1 krt / kk, 1 h)
   - koulutusmoduulit kyberturvallisuudesta 1–10, (3 h/moduuli)
   - MIF: Cyber Master Bascis & Cyber Master Extended (3 pv + 2 pv)
   - muu Cyberwatchin luentotarjoama tai verkkokurssi.
2) Oman toimijuuden määrittelyssä ja ilmoittautumisessa:
   - kuuluuko sääntelyn piiriin
   - keskeinen vai tärkeä toimija.
3) Riskianalyysikonsultaatiossa ja kyberriskienhallintamallin laatimisessa.
4) Toimitusketjun turvallisuuden tarkastamisessa.
5) Muissa NIS2:seen liittyvissä kysymyksissä.

Tarjoamme ilmaisen aloituspalaverin kyberturvallisuuslain vaatimusten esittelystä!

Johdon neuvontapalvelut

Olemme kokenut ja luotettu neuvonantaja ja kyberturvallisuuden asiantuntija. Kyberkonsultoinnissa keskeistä on tuoda esille, mitä organisaation johdon tulee tietää kybermaailmasta, sen ajankohtaisista riskeistä ja niiden vaikutuksista.

Tuemme uhkien torjunnassa, kyberriskien hallinnassa ja toiminnan jatkuvuuden turvaamisessa. Autamme kehittämään kokonaisturvallisuuden, kyberturvallisuuden, sisäisen turvallisuuden asiakokonaisuuksia sekä kumppaniriskien hallintaa. Työskentelymetodeinamme ovat muun muassa teema-alustukset, muistiot, työpajat sekä skenaariotyöskentely.

Cyber Due Diligence

Cyberwatchin kyberturvallisuuden Due Diligence on prosessi, joka auttaa organisaatiotasi tunnistamaan ja arvioimaan kyberturvallisuuteen liittyviä riskejä, jotka voivat vaikuttaa esimerkiksi kaupalliseen sopimukseen, investointiin, rahoitusjärjestelyyn tai yrityskaupan ehtoihin. Cyber Due Diligence toimii myös sopimuspuolien kilpailutilanteissa välttämättömänä työkaluna.

Cyber Due Diligence- projektiin kuuluu yksityiskohtainen verkkoanalyysi ja auditointiprosessi, joka sisältää muun muassa:

- ✔ Kyberturvan ja tietoturvan nykytilan arvioinnin
- ✔ Kolmansien osapuolien kyberturvallisuuden tason tarkastelun
- ✔ Tietoturvaloukkausten ja mahdollisten kyberhyökkäysten historian tarkastelun
- ✔ Kyberturvallisuuskulttuurin tarkastelun
- ✔ Kyberhygienian tason arvioinnin ja kyberturvakoulutuksen järjestelyt
- ✔ Kyberturvallisuuden sääntelyyn ja vaatimuksiin vastaaminen
- ✔ Kyberturvan ja tietoturvariskien hallinnan
- ✔ Kyberturvallisuuskulttuurin integrointi yrityskaupan jälkeen (NIS2 yhteensopivuus sekä sisäisten politiikkojen yhteensopivuus)

MESSUKESKUS
The real social media

FOR A BETTER DIGITAL FUTURE

Politics, economy, reality and the future of cybersecurity.

Technology, digitalisation, and AI are transforming the global landscape at an unprecedented pace. While this shift creates vast opportunities, it also introduces new vulnerabilities affecting businesses and public administration. Cyber Security Nordic explores the critical role of cybersecurity, providing insights from both corporate and governmental perspectives. Connect with the entire Nordic cyber industry, discover the latest solutions, and experience the first-class programme.

SAFETY & COMPETITIVENESS | EUROPEAN SECURITY | TRUSTED DIGITALISATION & INFORMATION SECURITY | DEMOCRACY & DIGITAL POLICIES

CYBER SECURITY NORDIC

28–29 Oct 2026
Helsinki Expo and Convention Centre

cybersecuritynordic.com