Cyberwatch Finland

MAGAZINE 1/2026

Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

Tavoitteena kyberkyvykkäämpi maailma

Cyberwatch Finland

SISÄLTÖ

Cyberwatch Finland
MAGAZINE 1/2026

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)

Cyberwatch Finland

Onko meillä riittävä kyberuhkatiedustelukyvykkyys?

Maailman tilanne näyttää päivä päivältä hullummalta, epävarmuus lisääntyy, globaali talouskriisi kiihtyy ja sotatoimet jatkuvat Lähi-idässä sekä Ukrainassa. Kykymme muodostaa luotettava strateginen tilannekuva on puutteellinen. Media uutisoi, jokaisesta kriisistä erikseen, mutta keskinäisriippuvaisen maailman kokonaisuus on entistä vaikeammin ennakoitavissa. Kyberaseiden merkitys eri kriisipesäkkeissä kasvaa erityisesti tekoälyn nopean kehittymisen myötä. Toisaalta tekoälyn lisääntynyt käyttö lisää disinformaation määrää, helppo analyysi tuottaa myös vääriä johtopäätöksiä ja heikentää käytössä olevan datan luotettavuutta. Samaan aikaan uusi kyberlainsäädäntö ja sitä täydentävä EU-regulaatio velvoittaa yritysten hallitusten jäsenten ja operatiivisen johdon hankkimaan riittävän hyvän tilannekuvan kybermaailmasta, jotta heillä on kyky riskiperusteiseen päätöksentekoon. Haasteellinen tilanne – mikä siis neuvoksi?

Kykyämme kokonaisuuden hallintaan on parannettava. Kybermaailman ymmärtäminen perustuu edelleenkin ihmisten toiminnan, toimintaprossien sekä teknologian muodostamaan ekosysteemiin sekä tietenkin kyberuhkatoimijoiden toimintatapojen ymmärtämiseen. Tästä kokonaisuudesta on pystyttävä muodostamaan luotettava ja ennakoiva tilannekuva, jossa otetaan huomioon organisaation eri tasoilla tarvittavat tiedon tarpeet. Ne voidaan karkeasti jakaa ylimmän johdon tarvitsemaan strategiseen näkymään, operatiivisen johdon operatiiviseen tilannekuvaan ja asiantuntijoiden tarvitsemaan tekniseen tilannekuvaan. Kaikki tämä edellyttää luotettavaa dataa ja parempaa kykyä datan analysoimiseen. Kyberuhkatiedustelu on noussut arvoon arvaamattomaan. Kysymys kuuluukin, miten yksittäiselle yritykselle tai organisaatiolle luodaan riittävä uhkatiedustelukyky, onko se oltava itsellä vai voiko sen saada ostettua ulkoiselta palveluntuottajalta. Tämä on tärkeä päätöksenteon paikka, joka vaatii harkintaa ja oman organisaation tiedon tarpeiden ja kyberkypsyyden ymmärtämistä. – mistä sen ymmärrys syntyy?

Velvoite kyberriskianalyysin tekemiseen onkin hyvä työkalu, jos se tehdään huolellisesti ja perusteena on oman organisaation nykytilakartoitus ja perusteellinen pohdinta siitä millaisia kyberriskejä meihin kohdistuu – mikä on niiden todennäköisyys ja vaikutus? On tunnettava kyberuhkakuvat ja pystyttävä seuraamaan niissä tapahtuvia muutoksia. Samalla on pystyttävä arvioimaan miten fyysiset ja digitaaliset riskitekijät ovat keskinäisriippuvaisia toisistaan – tarvitaan siis kokonaisvaltainen riskianalyysi, joka perustuu luotettavaan tietoon. Prosessi opettaa tekijöilleen tiedontarpeet ja luotettavan analyysin merkityksen. Samalla se auttamatta johtaa johtopäätökseen, että luotettavaa kyberriskianalyysia ei voi tehdä ilman hyvää kyberuhkatiedustelutietoa.

Julkaisemme yhdessä DNV Cyberin kanssa uhkatiedustelun käsikirjan myöhemmin keväällä. Sen tavoitteena on avata kyberuhkatiedustelun kokonaisuutta ja helpottaa päätöksentekoa oman organisaationne kannalta. Tuote tulee kaikille vapaasti saataville ja on syntynyt hävittäjähankintaan liittyvän epäsuoran teollisen yhteistyön tuloksena. Yksi tämän tutkimus- ja tuotekehitykseen tähtäävän yhteistyön keskeinen tavoite on kyberosaamisen lisääminen suomalaisessa yhteiskunnassa ja siihen tämäkin käsikirja tähtää.

AAPO CEDERBERG
Toimitusjohtaja
ja perustaja
Cyberwatch Finland

Kyberturvasääntelyn uusi aalto

Euroopan unionin kyberturvasääntely on kokenut historiallisen murroksen. Vuonna 2016 voimaan tullut alkuperäinen verkko- ja tietoturvadirektiivi (NIS)[1] oli ensimmäinen yritys harmonisoida kyberturvallisuusvaatimuksia EU-tasolla, mutta se jäi vaikutuksiltaan vaatimattomaksi. Venäjän hyökkäyssota Ukrainaan vuonna 2022, kiihtyneet kyberhyökkäykset EU:n kriittistä infrastruktuuria vastaan ja digitaalisten toimitusketjujen haavoittuvuuksien paljastuminen pakottivat lainsäätäjän uusimaan lähestymistapansa perusteellisesti. Tuloksena on ollut kyberturvasääntelyn hyökyaalto, jota organisaatioiden on tullut oppia hallitsemaan.

Viimeisten neljän vuoden aikana EU:ssa on annettu tai valmistunut useita kyberturvallisuuden kulmakivisäädöksiä, kuten NIS2-direktiivi[2], kyberkestävyyssäädös (CRA)[3], kriittisten toimijoiden häiriönsietokykyä koskeva direktiivi (CER)[4], finanssialan digitaalista häiriönsietokykyä koskeva DORA-asetus[5] ja kybersolidaarisuussäädös[6]. Tuloksena on uusia velvoitteita, valvontarakenteita ja sääntelyn ulottuminen entistä syvemmälle yritysten johtamisrakenteisiin, toimitusketjuihin ja sisäisiin prosesseihin.

Vuonna 2026 sovellettavaksi tulevaa sääntelyä

Syyskuu 2026 on käänteentekevä hetki EU:n digimarkkinoilla toimiville organisaatioille, kun CRA:n asettamat haavoittuvuuksia ja poikkeamia koskevat raportointivelvoitteet tulevat sovellettaviksi. Kyseiset velvoitteet koskevat huomattavan monia organisaatioita.

Mikä on kyberkestävyyssäädös (CRA)?

Toisin kuin EU:n nykyinen digisääntely, joka koskee pääasiassa palveluntarjoajia ja järjestelmätoimittajia, CRA asettaa kyberturvallisuusvaatimuksia suoraan digitaalisia elementtejä sisältäville tuotteille. Näin ollen lähes kaikki ohjelmistoja laitteistotuotteet, jotka voivat muodostaa yhteyden internetiin tai muihin laitteisiin, kuuluvat CRA:n soveltamisalaan. Tällaisia tuotteita ovat esimerkiksi reitittimet, älykotilaitteet, teolliset anturit, mobiilipelit, käyttöjärjestelmät ja useimmat yritysohjelmistot. Jotta tällaiset tuotteet voidaan saattaa EU-markkinoille, niiden on täytettävä CRA:n olennaiset kyberturvallisuusvaatimukset ja valmistajan käytäntöjen on oltava CRA:n haavoittuvuuksien käsittelyä koskevien säännösten mukaisia.

Keihin kyberkestävyyssäädöstä sovelletaan?

CRA ei koske vain suuria teknologiayrityksiä, vaan laajasti monenlaisia toimijoita, jotka valmistavat digitaalisia elementtejä sisältäviä tuotteita tai asettavat tuotteen saataville EU-markkinoilla osana kaupallista toimintaa. Velvoitteet koskevat siis tuotteiden valmistajia, maahantuojia ja jakelijoita.

CRA:ta ei sovelleta tiettyihin tuotteisiin, kuten lääkinnällisiin laitteisiin, tyyppihyväksynnän alaisiin moottoriajoneuvoihin ja ilmailualan turvallisuustasoa koskevien vaatimusten mukaisesti sertifioituihin tuotteisiin silloin, kun niistä säädetään jo alakohtaisesti. Lisäksi yksinomaan kansallisen turvallisuuden ja maanpuolustuksen käyttöön tarkoitetut tuotteet jäävät soveltamisalan ulkopuolelle. Mikäli tuote ei lukeudu edellä mainittuihin poikkeuksiin, CRA mitä todennäköisimmin soveltuu siihen.

Syyskuussa 2026 sovellettaviksi tulevat raportointivelvoitteet

Vaikka suurinta osaa CRA:n velvoitteista aletaan soveltaa vasta joulukuussa 2027, digitaalisia elementtejä sisältäviin tuotteisiin sisältyviä aktiivisesti hyödynnettyjä haavoittuvuuksia ja tietoturvaan vaikuttavia vakavia poikkeamia koskevat raportointivelvoitteet tulevat sovellettaviksi 11.9.2026. Tästä lähtien tuotteiden valmistajilla on lakisääteinen velvollisuus ilmoittaa edellä mainituista tapauksista asianomaisille kansallisille kyberturvallisuusviranomaisille (CSIRT) ja Euroopan unionin kyberturvallisuusvirasto ENISAlle.

Valmistajien on ilmoitettava kaikista aktiivisesti hyödynnetyistä haavoittuvuuksista eli tapauksista, joiden osalta on luotettavaa näyttöä siitä, että pahantahtoinen toimija on hyödyntänyt järjestelmän haavoittuvuutta ilman järjestelmän omistajan lupaa. Tämä ei kuitenkaan kata teoreettisia riskejä tai tunnettuja mutta hyödyntämättömiä virheitä, vaan nimenomaan tilanteita, joissa on luotettavaa näyttöä siitä, että jokin pahantahtoinen toimija on hyödyntänyt haavoittuvuutta.

Valmistajien on lisäksi ilmoitettava vakavista poikkeamista, jotka vaikuttavat tuotteen tietoturvaan. Tällaiset poikkeamat vaikuttavat tai voivat vaikuttaa kielteisesti tuotteen kykyyn suojata arkaluonteisten tai tärkeiden tietojen tai toimintojen saatavuutta, aitoutta, eheyttä tai luottamuksellisuutta taikka johtavat tai voivat johtaa haitallisen koodin sisällyttämiseen tai ajamiseen tuotteessa tai tuotteen käyttäjän verkko- ja tietojärjestelmissä.

Ennakkovaroitusilmoitus on toimitettava 24 tunnin kuluessa haavoittuvuuden tai poikkeamana havaitsemisesta ja varsinainen ilmoitus 72 tunnin kuluessa. Ellei asiaankuuluvia tietoja ole jo toimitettu, lopullinen raportti aktiivisesti hyödynnetystä haavoittuvuudesta on toimitettava viimeistään 14 päivän kuluessa siitä, kun korjaava tai lieventävä toimenpide on käytettävissä ja kuukauden kuluessa vakavan poikkeaman ilmoittamisesta. ENISA vastaa keskitetyn raportointialustan perustamisesta ja ylläpitämisestä, jotta arkaluonteiset haavoittuvuustiedot pysyvät luottamuksellisina.

Raportointivelvollisuus ei kuitenkaan rajoitu vain viranomaisilmoituksiin, vaan valmistajien on ilmoitettava myös käyttäjilleen aktiivisesti hyödynnetyistä haavoittuvuuksista tai vakavista poikkeamista. Tarpeen mukaan käyttäjäilmoitukseen on lisättävä myös tieto korjaavista toimenpiteistä, joita käyttäjät voivat toteuttaa haavoittuvuuden tai poikkeaman vaikutusten lieventämiseksi.

Entä tekoäly?

CRA ei ole ainoa merkittävä vuonna 2026 sovellettavaksi tuleva säädös, sillä suurinta osaa EU:n tekoälysäädöksen[7] velvoitteista aletaan pääosin soveltaa 2.8.2026. Soveltamisen aikatauluun on ehdotettu osittaista lykkäystä erityisesti suuririskisten tekoälyjärjestelmien velvoitteiden osalta niin kutsutun AI Omnibus -ehdotuksen myötä, joten on mahdollista, että soveltamisen aikatauluun tulee muutoksia lähitulevaisuudessa.

Tekoälysäädös sääntelee tekoälyjärjestelmiä ja -malleja asettamalla vaatimuksia ja velvoitteita niille, jotka saattavat ne markkinoille, ottavat ne käyttöön tai käyttävät niitä EU:ssa.[8] Tekoälysäädöksen soveltamisala on laaja ja se koskee EU:ssa toimivien tekoälyjärjestelmien tarjoajien ja käyttöönottajien lisäksi myös EU:n ulkopuolisia tarjoajia, joiden järjestelmiä käytetään EU:ssa sekä maahantuojia, jakelijoita ja valmistajia.

Myös tekoälysäädös asettaa erityisiä kyberturvallisuusvaatimuksia, kuten asianmukaisen kyberturvallisuustason varmistaminen suuririskisissä tekoälyjärjestelmissä, joita ovat muun muassa rekrytointiin, luottokelpoisuuden arviointiin, biometriseen tunnistamiseen ja useat kriittiseen infrastruktuuriin käytettävät tekoälyjärjestelmät. Tähän sisältyy kyky ehkäistä ja rajoittaa kolmansien osapuolten yrityksiä manipuloida järjestelmän käyttöä, tuloksia tai suorituskykyä hyödyntämällä sen haavoittuvuuksia.

Hyvä uutinen on, että nämä kaksi säädöstä on suunniteltu täydentämään toisiaan kyberturvavaatimusten osalta. Kun esimerkiksi suuririskinen tekoälyjärjestelmä kuuluu CRA:n piiriin, voidaan CRA:n asettamien kyberturvallisuusvaatimusten noudattamisella täyttää myös monet tekoälysäädöksen asettamat kyberturvallisuusvaatimukset.

Tekoälysäädökseen sisältyy myös raportointivelvoitteita. Suuririskisten tekoälyjärjestelmien tarjoajien

on ilmoitettava vakavista vaaratilanteista niiden jäsenvaltioiden markkinavalvontaviranomaisille, joissa kyseinen vaaratilanne tapahtuu. Tietyissä tilanteissa myös suuririskisten tekoälyjärjestelmien käyttöönottajien on ilmoitettava vakavista vaaratilanteista ensin tarjoajalle ja sen jälkeen maahantuojalle tai jakelijalle sekä asianomaisille markkinavalvontaviranomaisille. Suomessa markkinavalvonnasta vastaavat kunkin toimialan nimetyt valvontaviranomaiset.

Valmistautuminen uusiin velvoitteisiin

Kokonaisuutena CRA:ssa asetetut velvoitteet ovat merkittäviä ja koskevat myös tuotteiden valmistusvaihetta. Ajankohtaisin tehtävä on kuitenkin luoda sisäiset prosessit, joita tarvitaan aktiivisesti hyödynnettyjen haavoittuvuuksien ja vakavien poikkeamien havaitsemiseksi ja ilmoittamiseksi, sillä raportointia koskevat velvoitteet tulevat sovellettavaksi edellä todetussa aikataulussa jo syksyllä 2026. Tällaisten prosessien luontia ei kuitenkaan tulisi pitää kertaluonteisena toimenpiteenä organisaatioissa, vaan alkuponnistuksena jatkuvalle kyberturvallisuutta koskevalle maturiteettitasolle, joka kattaa CRA:n vaatimukset kuten riskinarvioinnit, tukijaksoa koskevat sitoumukset ja ilmoituskanavat haavoittuvuuksille. Tekoälypohjaisia tuotteita kehittäville tai käyttöönottaville organisaatioille tekoälysäädöksen soveltamisen alkaminen elokuussa 2026 lisää uuden kerroksen kyberturvallisuusvelvoitteisiin.

Kyberturvasääntelyä korjataan uusien sääntelyehdotusten avulla

Digital Omnibus: Poikkeamaraportoinnin yhdenmukaistaminen

Euroopan komissio on ehdottanut kyberturvallisuuteen liittyvien poikkeamien raportointivelvoitteiden uudistusta, jonka tavoitteena on keventää raportoinnista yrityksille aiheutuvaa taakkaa. Yksi digitaalista sääntelyä koskevan marraskuussa 2025 annetun laajan Digital Omnibus -ehdotuksen keskeisistä uudistusehdotuksista on **eri sääntelyyn perustuvan poikkeamaraportoinnin keskittäminen yhteen keskitettyyn ilmoituskanavaan**. Tämän ilmoituskanavan kautta raportoitaisiin useaan eri säädökseen (ainakin GDPR[9], NIS2, CER, CRA, DORA ja eIDAS[10]) perustuvat poikkeamailmoitukset toimivaltaisille viranomaisille. Kanavan kehittäisi ja sitä ylläpitäisi ENISA. Tällä olisi vaikutuksia erityisesti niille toimijoille, jotka ovat usean päällekkäisen ja ajallisesti tiukan raportointivelvollisuuden piirissä.

Lisäksi Digital Omnibus -ehdotus toteutuessaan **pidentäisi GDPR:n mukaisen henkilötietojen tietoturvaloukkausta koskevan ilmoituksen antamisen aikarajaa nykyisestä 72 tunnista 96 tuntiin**. Tämän uudistuksen vaikutukset koskisivat laajasti kaikenlaisia organisaatioita, sillä käytännössä kaikki toimijat ovat joissain tilanteissa henkilötietojen rekisterinpitäjän roolissa eli velvollisia ilmoittamaan henkilötietojen tietoturvaloukkauksista tässä roolissaan.

Komission uusi kyberturvallisuuspaketti: CSA2 ja NIS2 -sääntelyn päivitykset

Tammikuussa 2026 komissio antoi ehdotuksen uudesta kyberturvallisuuspaketista, jolla päivitettäisiin ja täydennettäisiin olemassa olevaa Euroopan unionin keskeistä kyberturvasääntelyä.[11]

Kyberturvallisuusasetuksen uudistuksella (CSA2)[12] komissio pyrkii ratkaisemaan neljä ydinhaastetta: EU:n kyberpolitiikan ja sidosryhmien tarpeiden yhteensopimattomuuden, eurooppalaisen kyberturvallisuuden sertifiointikehyksen toimeenpanon epäonnistumisen, kybersääntelyn pirstaleisen ja monimutkaisen vaatimustenmukaisuuskentän sekä kasvavat ICT-toimitusketjuriskit.

- **Toimitusketjuturvallisuutta koskevat ehdotukset** ovat CSA2:n kenties merkittävin uudistuskokonaisuus, joka ilmentää vallitsevan geopoliittisen tilanteen vaikutuksia lainsäädäntöön. CSA2 loisi EU-tasoisen kehyksen niin kutsuttujen ”ei-teknisten” toimitusketjuriskien hallintaan. Kehys koskisi NIS2-sääntelyn alaisia kriittisiä toimialoja, ja se perustuisi EU-tason riskinarviointeihin, joiden pohjalta komissio voisi määrätä erityisiä vaatimuksia ja jopa kieltoja tiettyjen kolmansien maiden toimittajien ja niiden tarjoamien komponenttien käyttöön. Jos kolmas maa todettaisiin kyberturvallisuuden kannalta riskimaaksi, kyseisten maiden toimittajille säädettäisiin rajoituksia muun muassa EU-sertifiointiin, vaatimustenmukaisuuden arviointiin, julkisiin hankintoihin sekä EU-rahoituksen piiriin. Viestintäverkkojen osalta korkean riskin toimittajien komponenttien alasajo perustuisi suoraan asetukseen sen mukaisine aikarajoineen. Toimijat, joilla on kytköksiä kyberturvallisuusriskimaiksi todettuihin maihin, voisivat hakea poikkeusta vaatimuksiin tai kieltoihin tietyin edellytyksin.

- Lisäksi CSA2:n keskeisenä tavoitteena on tuoda **uudistettu kyberturvallisuuden sertifiointikehys,** joka tekisi kyberturvallisuuden sertifioinnista ennakoitavampaa, johdonmukaisempaa ja ketterämpää. Keskeinen sisällöllinen uudistus olisi sertifiointikehyksen soveltamisalan laajennus – sertifioinnin kohteena voisivat olla ICT-tuotteet, -palvelut, -prosessit ja hallinnoidut tietoturvapalvelut sekä myös organisaatioiden kyberturvallisuusasema kokonaisuutena. Tämä tarkoittaisi, että tulevaisuudessa organisaatiot voisivat hakea sertifiointia kyberturvallisuustasonsa osoittamiseksi – ei pelkästään yksittäisille tuotteille tai palveluille. Kyberturvallisuussertifioinnin roolia on tarkoitus vahvistaa myös vaatimustenmukaisuuden osoittamisen välineenä ja hallinnollisen taakan vähentäjänä eri säädösten velvoitteiden yhteensovittamisessa.

- CSA2-ehdotukseen sisältyy **ENISAn mandaatin kokonaisvaltainen uudistus**, jotta virasto voi tukea politiikan toimeenpanoa ja jäsenvaltioiden operatiivista yhteistyötä aiempaa tehokkaammin. ENISAlle tulisi uusia tehtäviä operatiivisen yhteistyön tukemisessa, tilannekuvan parantamisessa, EU:n kyberturvallisuusreservin operoinnissa sekä raportointialustojen ja haavoittuvuuksien hallinnan kapasiteetin tarjoamisessa.

Komission uusi kyberturvallisuuspaketti sisältää CSA2-ehdotuksen lisäksi erillisen ehdotuksen muutoksista NIS2-direktiiviin.

Keskeiset muutosehdotukset liittyvät soveltamisalan tarkennuksiin, täytäntöönpanosääntelyyn, vaatimustenmukaisuuden osoittamiseen, haittaohjelmia koskevaan EU:n laajuiseen raportointiin sekä rajat ylittäviä palveluja tarjoavien toimijoiden valvontaan:

- NIS2-sääntelyn **soveltamisalaa selkeytettäisiin ja laajennettaisiin**. Terveydenhuollon tarjoajia, sähköntuottajia, vetyalan yrityksiä ja kemianteollisuuden toimijoita sekä DNS-palveluntarjoaja koskevia soveltamisalasäännöksiä selkeytettäisiin. Eurooppalaisten digitaalisten identiteettilompakoiden ja eurooppalaisten yrityslompakoiden tarjoajat ja merenalaisen tiedonsiirtoinfrastruktuurin operaattorit tulisivat sääntelyn soveltamisalan piiriin. Sääntelyyn otettaisiin uusi pienten ja keskisuurten yritysten luokka komission suosituksen[13] mukaisesti. NIS2-direktiivin liitteeseen I kuuluvat pienet midcap-yritykset (small mid-caps) tulisivat pääsääntöisesti tärkeiksi toimijoiksi (keskeisen toimijan sijaan), mikä vähentäisi sääntelyn valvonnasta aiheutuvaa taakkaa.

- Sääntelyn **soveltamisen yhdenmukaisuutta parannettaisiin täytäntöönpanosäädöksellä** avulla. Komission tulisi laatia tarkentavat suuntaviivat toimitusketjun turvallisuusvaatimuksista sääntelyn oikeusvarmuuden ja suhteellisuuden parantamiseksi. Lisäksi otettaisiin käyttöön entistä pidemmälle menevä harmonisointi kyberturvallisuuden riskienhallintatoimenpiteitä koskevien vaatimusten tarkentamiseksi.

- **Kyberturvallisuussertifioinnin avulla helpotettaisiin vaatimusten noudattamisen osoittamista** (hyödyntäen edellä mainittua sertifiointikehystä).

- Ehdotuksen mukaisesti otettaisiin käyttöön Euroopan unionin

laajuinen **kehys kiristysohjelmahyökkäyksiä koskevien tietojen keräämiselle**. Tavoitteena on antaa viranomaisille tarvittavat tiedot kiristysohjelmaryhmien toiminnan häiritsemiseksi ja lakkauttamiseksi.

- **ENISAlle annettaisiin uusi rooli jäsenvaltioiden tukemisessa** sellaisten toimijoiden valvonnassa, jotka tarjoavat palveluja useammassa jäsenvaltiossa. ENISA suorittaa kattavan analyysin rajat ylittävistä kyberturvallisuusriskeistä ja laatii vuotuisen riskinarviointiraportin. Raportin perusteella ENISA voisi suositella toimivaltaisille viranomaisille yhteisten tarkastusryhmien perustamista, kehittää yhteisiä valvontasuuntaviivoja ja avustaa yhteisissä valvontatoimissa.

- Ehdotuksen mukaan jäsenvaltioiden edellytettäisiin ottavan käyttöön **politiikat kvanttiturvalliseen salaukseen (PQC)** siirtymiseksi osana kansallisia kyberturvallisuusstrategioitaan. Ehdotetussa aikataulussa tavoitellaan PQC-siirtymää vuoteen 2030 mennessä kriittisten käyttötapausten osalta ja vuoteen 2035 mennessä keskitason ja matalan tason käyttötapausten osalta. Suomen voimassa olevan kyberturvallisuusstrategian mukaan Suomen yhtenä strategisena tavoitteena on olla kriittisten salausteknologioiden osalta omavarainen ja kvanttiuhkaan varautunut valtio 2030-luvun alkuun mennessä.

Kuinka navigoida muuttuvassa sääntely-ympäristössä?

Tämän vuosikymmenen alkupuolella kyberturvallisuuslainsäädännön ensimmäinen aalto kuvattiin usein tsunamiksi, mutta nykyistä tilannetta voidaan paremmin luonnehtia sääntelyn nousuvedeksi. Kaiken kaikkiaan kyberturvallisuuslainsäädäntö on ollut ennennäkemättömän myllerryksen kohteena. Joissakin tapauksissa sääntelykehyksen päivittäminen on alkanut huomattavan aikaisin, mikä korostaa kehityksen aktiivisen seurannan tärkeyttä. Seuraavassa kuvatut lähestymistavat voivat auttaa navigoimaan muuttuvassa sääntely-ympäristössä.

Ensinnäkin on tärkeää tunnistaa omaan toimintaan suoraan vaikuttavat säännökset sekä muiden säännösten mahdolliset välilliset vaikutukset, esimerkiksi toimitusketjujen kautta. Eri lainsäädäntövälineiden velvoitteiden välisten synergioiden tunnistaminen voi auttaa velvoitteiden jalkauttamisessa mielekkäällä tavalla. Velvoitteiden seuranta kategorioittain (kuten poikkeamien havaitseminen ja hallinta, toimitusketjujen turvallisuus) voi olla käytännöllisempää kuin velvoitteiden seuranta säädöksittäin. Organisaatiosta riippuen esimerkiksi poikkeamien ja haavoittuvuuksien hallinta voi olla useiden, osittain päällekkäisten velvoitteiden alainen.

Kyberturvallisuuden riskienhallintaa koskevan lainsäädännön soveltaminen on nostanut kyberturvallisuuden kirjallisen dokumentoinnin merkityksen aivan uudelle tasolle. Dokumentaatio toimii sisäisen viestinnän ja toiminnan välineenä, mutta se on myös tärkeä keino osoittaa velvoitteiden noudattaminen oikeusvarmuuden turvaamiseksi poikkeamien, valvontatoimenpiteiden tai riitojen sattuessa. Koska kyberturvallisuuden sääntely on riskipohjaista, riskien arvioinnin ja riskienhallintatoimenpiteiden dokumentointi sekä tällaisen dokumentaation pitäminen ajan tasalla on riskienhallintatyön perustavia lähtökohtia. Sääntely kannustaa organisaatioita omaksumaan proaktiivisen lähestymistavan kyberturvallisuuden hallintaan.

Tehtävien ja vastuiden selkeä määrittely on välttämätöntä velvoitteiden onnistuneen jalkauttamisen kannalta. Riskienhallinta muuttuu uhka- ja sääntely-ympäristön vuoksi yhä vaativammaksi ja haastavammaksi, joten on tärkeää varmistaa, että tiimit ovat riittävät ja tunnistavat tehokkaan yhteistyön merkityksen kestävän kyberturvallisuusriskien hallinnan saavuttamisessa.

KIRJOITTAJAT:

JOHANNA TUOHINO
Dittmar & Indrenius

JUKKA LÅNG
Dittmar & Indrenius

ROOPE FREDMAN
Dittmar & Indrenius

VIITTAUKSET/LÄHTEET

1 Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa.

2 Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa.

3 Euroopan parlamentin ja neuvoston asetus (EU) 2024/2847, annettu 23 päivänä lokakuuta 2024, digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista.

4 Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557, annettu 14 päivänä joulukuuta 2022, kriittisten toimijoiden häiriönsietokyvystä.

5 Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554, annettu 14 päivänä joulukuuta 2022, finanssialan digitaalisesta häiriönsietokyvystä.

6 Euroopan parlamentin ja neuvoston asetus (EU) 2025/38, annettu 19 päivänä joulukuuta 2024, toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberuhkien ja poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten.

7 Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689, annettu 13 päivänä kesäkuuta 2024, tekoälyä koskevista yhdenmukaistetuista säännöistä.

8 Tekoälysäädöksen osalta huomattava, että sen sisältämät vaatimukset ovat riippuvaisia Euroopan komission keskeneräisestä aloitteesta yksinkertaistaa ja osittain lykätä tekoälysäädöksessä asetettujen velvoitteiden soveltamispäivää.

9 Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta.

10 Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla, jota on muutettu asetuksella (EU) 2024/1183.

11 Proposal for a Regulation for the EU Cybersecurity Act, COM(2026) 11; Directive Proposal for simplification measures and alignment with the Cybersecurity Act, COM(2026) 13.

12 CSA2-ehdotuksella pyritään tarkistamaan Euroopan parlamentin ja neuvoston asetusta (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista.

13 Komission suositus (EU) 2025/1099 pienten midcap-yritysten määritelmästä.

CYBERWATCH FINLAND
& DNV CYBER

Kyberuhka-tiedustelun käsikirja

Cyberwatch Finland on laatinut yhteistyössä DNV Cyberin kanssa kyberuhkatiedustelun käsikirjan tavoitteinaan lisätä suomalaisten kriittisten alojen organisaatioiden ymmärrystä ja kykyä hyödyntää kyberuhkatietoa.” Käsikirjasta on tehty tähän lehteen lyhennelmä. Käsikirja tullaan julkaisemaan 2026 keväällä sekä suomeksi että englanniksi ja tuote tulee kaikille vapaasti saataville.

Johdanto:

Kyberuhkat muuttuvat ja kehittyvät jatkuvasti, ja organisaatioilta on alettu edellyttämään yhä enemmän kykyä omaksua ja hyödyntää kyberuhkia koskettavaa tietoa. Tämä korostuu paitsi nykyisissä käytännön tarpeissa kuin myös lainsäädännön vaatimuksissa. Vaikka EU:n verkko- ja tietoturvadirektiivi NIS2-direktiivi (EU2022/2555) ja sen kansallisesti sovellettavat versiot (Kyberturvallisuuslaki, Laki julkisen hallinnon tiedonhallinnasta ja Laki sähköisen viestinnän palveluista) eivät suoraan velvoita kyberuhkatiedon hankintaan tai hyödyntämiseen, velvoittaa se arvioimaan ja hallitsemaan kyberuhkia, muodostamaan näiden pohjalta organisaation kyberriskienhallinnan toimintamallin ja raportoimaan merkittävistä poikkeamista valvovalle viranomaiselle. Yrityksen johto onkin uuden kyberturvallisuuslain myötä entistä velvoittavammassa roolissa, ja uusissa velvoitteissa korostuu johtohenkilöstön henkilökohtaisen vastuun kasvaminen riskienhallinnan toimenpiteiden toteuttamisessa – ja toteuttamatta jättämisessä. Kyberriskienhallinnan toimenpiteitä on lähes mahdotonta toteuttaa ilman reaaliaikaista uhkatietoa, jolloin näkyvyys uhkakuvaan on hyvin rajallinen ja epätodenmukainen. Mitä kattavampi kyberuhkatieto yrityksellä on, sen paremmin valmistautumisaikaa sillä on.

Modernissa tietoyhteiskunnassa jokainen organisaatio joutuu varautumaan kyberuhkiin – joko suoraan tai välillisesti. Kyberuhka on potentiaalinen tilanne, tapahtuma tai toiminta, joka voi vahingoittaa tai häiritä viestintäverkkoja ja tietojärjestelmiä, tällaisten järjestelmien käyttäjiä ja muita toimijoita. Liian usein organisaatioiden varautumisen aste ei ole sillä tasolla, että kyberuhkan realisoitumiseen osattaisiin suhtautua riittävällä vakavuudella. Edelleen toimintamalleissa korostuu reaktiivinen ote proaktiivisen sijaan ja toimenpiteitä toteutetaan vasta, kun kyberuhka on tapahtunut, mainehaittaa on ehtinyt syntymään ja viranomaiset ovat kiinnostuneet tapahtuneesta. Merkityksellinen ja oikea-aikainen uhkatieto pyrkii tuomaan toimenpiteisiin ennakoitavuutta ja tehokkuutta, samalla minimoiden vahinkojen kustannukset. Kyberuhkatiedolla on pyrkimys saada aika ja taustatieto päätöksentekoon. Jotta uhkatiedosta on organisaatiolle hyötyä, pitää organisaation johdolla olla myös riittävä kyky tehdä siihen pohjautuvia päätöksiä viedäkseen organisaatiota oikeaan suuntaan. Kyberuhkatieto on edellytys entistä kehittyneempään ja tarkempaan tiedolla johtamiseen, kun suunnitellaan ja toimeenpannaan kybersuojausta.

Kyberuhkatiedon tasot

Kyberuhkatiedolla tarkoitetaan toimintaympäristöstä hankittua tai sitä koskevaa tietoa siitä, mitkä tai minkälaiset uhkat ovat kaikkein todennäköisimpiä ja miten niiltä voidaan suojautua. Käytännössä se on tietoa, joka ohjaa organisaation päätöksiä kyberturvaan tehtävistä investoinneista, toimintamalleista tai teknisistä ratkaisuista. Kyberuhkatieto, ja sen tuottamisen prosessi, on hyvin samankaltainen tiedusteluprosessin kanssa. Perinteinen tiedusteluprosessi on jatkuva, vaiheittainen toimintamalli, jolla kerätään, analysoidaan ja toimitetaan tietoa päätöksenteon tueksi. Organisaatioiden ja etenkin ylimmän johdon on tärkeä ymmärtää, minkälaista erilaista uhkatietoa on saatavilla. Kyberuhkatieto jaetaan usein kolmeen tasoon auttamaan hahmottamista: strateginen, operatiivinen ja tekninen (joskus myös taktinen) uhkatieto.

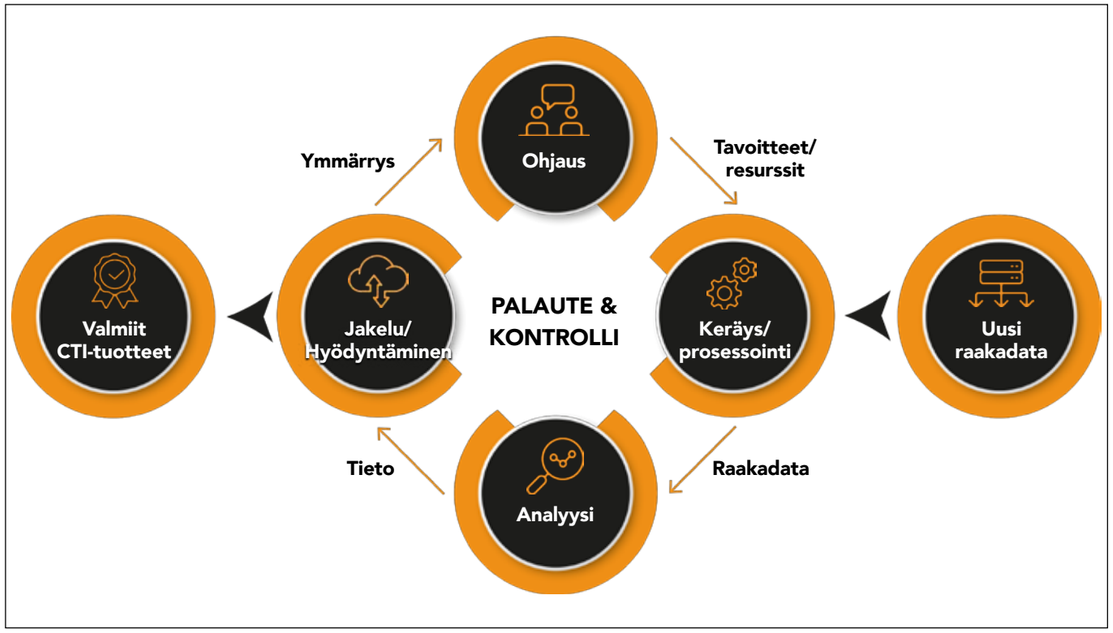
Uhkaprosessin kehittäminen ja arviointi

Tärkein kriteeri, jota uhkatiedolle voidaan määrittää, on sen käyttökelpoisuus. Tällä tarkoitetaan sitä, että uhkatieto, jota organisaatio tuottaa tai hankkii, on luonteeltaan ja sisällöltään sellaista, että se vastaa tarpeisiin, johtaa suoriin toimenpiteisiin tai vahvistaa jo tehtyjen toimenpiteiden oikeellisuutta. Jokaisella organisaatiolla on omat resurssit ja tavoitteet, jotka määrittävät sen, minkä laajuiseen uhkatietoprosessiin pyritään, ja missä suhteessa oma toiminta ja kumppanien hyödyntäminen tapahtuu. Organisaation kyberkypsyyden kasvattaminen on prosessi, jossa organisaatio siirtyy sattumanvaraisesta tietoturvasta systemaattiseen, riskipohjaiseen ja ennakoivaan toimintatapaan, jossa yhdistyy ihmiset, prosessit ja teknologia.

Kyberuhkatietoprosessin laatua on mahdollista arvioida kybermaturiteetin kautta. Kypsyystaso kertoo sen, millainen kyberkyvykkyys organisaatiolla on suojautua kyberuhilta ja varmistaa liiketoiminnan jatkuvuus häiriötilanteissa. Kyberkypsyys kasvaa sitä mukaan, kun toimintatapoja ja prosesseja kehitetään palautteen ja muuttuvan kybertoimintaympäristön mukaan. Oman kypsyystason mittaaminen voi olla tarpeen toimittajia ja muita yhteistyökumppaneita valittaessa. Alihankkijoiden kohdalla on hyödyllistä arvioida näiden teknologisia valmiuksia, eli mitä järjestelmiä he käyttävät tai minkälaisiin tietolähteisiin heillä on pääsy. Kyberuhkatietoprosessi perustuukin lähes aina tiedon jakamiseen ja yhteistyöhön. Se on luonteeltaan niin laaja ja monipuolinen kokonaisuus, että parhaimminkaan resursoidun organisaation ei ole järkevää pyrkiä tekemään kaikkea itse, vaan tärkeä osa onnistunutta prosessia on oikeanlaisten yhteistyökumppanien hankinta. Kumppanuudet voivat olla niin tasavertaisia tiedonjakoverkostoja kuin alihankkija- tai toimittajasuhteita, joiden kautta hankitaan tietoa tai osaamista. Paras kumppanuus on sellainen, jossa molemmat osapuolet voivat antaa ja saada tietoa. Tämä mahdollistaa molemmin puolisen kasvun ja kehityksen.

Kyberuhkatiedon prosessi:

Kyberuhkatiedon prosessi (CTI-prosessi, Cyber Threat Intelligence -process) jaetaan tässä käsikirjassa ohjauksen, keräyksen, analysoinnin ja jakelun vaiheisiin. Kyberuh-



Kuva 1: Kyberuhkatiedusteluympyrän yksittäinen prosessi.

katiedon kohdalla tavoite on tuottaa lisäaikaa päätöksentekoon ja muuttaa reaktiivinen toiminta proaktiiviseksi eli ennakoivaksi. Syklisen uhkatietoprosessin avulla johdon kyvykkyyksiä ymmärtää kyberuhkatietoa on mahdollista kehittää ja ohjata. Se sisältää kaikki vaiheet ensimmäisestä suunnitelmasta alkaen tiedon keräämiseen ja hyödyntämiseen sekä toiminnasta saatujen kehittämistarpeiden toimeenpanoon seuraavaa keräyskertaa varten. Prosessin aikana kerätty raakadata muokkautuu informaatioksi ja lopulta päätöksentekoa tukevaksi tai ohjaavaksi tiedoksi. Todellisuudessa ympyrän jokainen vaihe on käynnissä samanaikaisesti muiden vaiheiden kanssa rinnakkain, ja useita CTI-prosesseja voi olla samanaikaisesti käynnissä.

Ohjaus

CTI-prosessin ohjaus on usein tärkein vaihe prosessin onnistumisessa. Ohjauksessa johto määrittelee prosessin tavoitteet, resurssit ja mandaatin tavoitteiden saavuttamiseksi. Ilman huolellisesti tehtyä ohjausta, on todennäköistä, että resursseja hukataan vääränlaisen tiedon keräämiseen tai käsittelyyn, tai kaikkea saatavilla olevaa ja tarpeellista tietoa ei kerätä tai hyödynnetä. Johdon vastuulla onkin hyvin tehdyn ohjauksen avulla suojata yrityksen IT omaisuus erilaisilta uhkatoimijoilta, koska jo yksikin laiminlyönti voi johtaa merkittävään tietoturvatapahtumaan. Yksinkertaistettuna ohjausvaiheessa on kyse uhkatiedon keräämisen ja hyödyntämisen suunnittelemisesta sekä suunnitelmien käytännön toteuttamisen valmistelusta. CTI-prosessissa on loppukädessä kysymys turvallisuuteen tehtävästä investoinnista, kuten IT-omaisuuden suojaamisesta, ja mikäli sijoitukselle halutaan vastinetta, on se syytä suunnitella ja valmistella huolella.

Keräys ja prosessointi

Ohjausta seuraava vaihe on tiedon keräys ja sen prosessointi. Keräyksellä tarkoitetaan eri vaiheissa prosessointia olevan tiedon (raakadatan tai valmiiksi analysoidun tiedon) hankkimista edellisessä vaiheessa tehtyjen suunnitelmien mukaisesti. Prosessoinnilla tarkoitetaan kerätyn tiedon muuntamista yhtenäiseksi, käyttökelpoiseksi ja kontekstuaaliseksi uhkainformaatioksi, myöhempää analyysiä ja hyödyntämistä varten. Toisin sanoen, jotta tietoa on mahdollista hyödyntää, tulee se ensiksi löytää ja kerätä. Vasta, kun tämä kerätty tieto on jalostettu, on se käyttökelpoista. Uutta kyberuhkatiedon prosessia käynnistäessä keräysvaiheessa sorrutaan usein keräämään mahdollisimman paljon tietoa monesta eri lähteestä. Vaikka runsas tietomäärä on toisinaan hyvä, johtaa toiminta helposti tilanteeseen, jossa syötettä on liikaa ja tietoturvatiimit lamaantuvat turhien hälytyksien ja manuaalista läpikäyntiä vaativan tietomassan kanssa. Keräysvaiheessa onkin tärkeä muistaa edellisessä vaiheessa määritellyt tarpeet, ja ohjata toimintaa sen mukaan. Liiallinen tietomäärä voi johtaa yhtä herkästi virheisiin kuin puutteellinenkin keräys. Vain edistyneimpien ja eniten resursseja kyberuhkatietoprosessiin sijoittaneiden toimijoiden kannattaa kerätä kaikki mahdollinen saatavilla oleva tieto.

Analyysi

Kolmas vaihe on analyysi. Analyysivaiheessa kerätty raakadata muokataan analyysiprosessin myötä uhkatiedoksi. Riippuen kerätyn datan laadusta, tämä voi olla hyvinkin yksinkertaista tai vaatia paljon työstämistä. Tavoitteena on lisätä raakadataan merkityksiä, yhdistellä eri lähteistä saatavaa tietoa johtopäätösten tekemiseksi ja lopulta tuottaa ymmärrettävää tietoa päätöksenteon tueksi ja siten konkreettisiksi toimenpiteiksi. Oleellista lopputuloksen kannalta on prosessin alkuvaiheessa selkeästi määritellyt tiedustelukysymykset ja tiedon tarpeet. Kyberuhkatiedustelussa analyysistä voi vastata yhtä hyvin niin ihminen kuin järjestelmä. Automaatio ja tekoälyn hyödyntäminen etenkin teknisen datan analysoinnissa ja käsittelyssä kehittyy jatkuvasti, mutta ihmisanalyytikoilla on yhä merkittävä rooli etenkin strategisen tason analyysissä.

Jakelu

Viimeinen jakelun ja hyödyntämisen vaihe on edellytys sille, että työstä on käytännön hyötyä. Tärkein kriteeri sille, minkälaista uhkatietoa organisaation tulee hankkia, on sen käytettävyys. Oli uhkatiedon lopullinen vastaanottaja sitten järjestelmä, henkilö tai organisaation osasto, on tämän vaiheen tehtävä varmistaa, että kerätty ja analysoitu tieto päätyy haluttuun paikkaan ja, että vastaanottaja tietää, mitä on saamassa ja mitä sen kanssa tulee tehdä. Kyberuhkatiedon jakelu koskeekin sekä omaa organisaatiota että ulkoisia kumppaneita. Verkostojen toiminta perustuu siihen, että sen kaikki osapuolet sekä tuottavat että vastaanottavat tietoa, joten kyberuhkatiedon kanssa työskentelevien organisaatioiden tulee varautua myös jakamaan hankkimaansa ja käsittelemäänsä uhkatietoa. Etenkin jaettavan uhkatiedon laadusta tulee olla täysi varmuus tai vaihtoehtoisesti epävarmuus pitää pystyä ilmaisemaan. Pohdittava asia onkin se, minkälaista tietoa organisaatio pystyy jakamaan ja kenelle. Uhkatiedon kriittisyys tulee olla määritetty organisaation sisäisesti, ja eri tiedonjakoverkostot tai kumppanit luokiteltuja sen mukaan, kenelle minkäkin tasoista tietoa voidaan jakaa. Jakelun ja hyödyntämisvaiheen tärkein tehtävä on varmistaa, että suunnitelmat toteutuvat, muokata niitä tarvittaessa.

Kehityksen suunta

Kyberuhkatiedon tärkein tehtävä on tuottaa aikaa ja tietoa päätöksentekoa varten. Aikaa on tarkoitus antaa uhkien ennalta tunnistamiseen ja reagointiin. Tämä aika on jatkuvasti käymässä lyhyemmäksi ja ennakkovaroituksen hankkiminen yhä vaikeammaksi. Uhkatoimijoiden operaatiot ovat nopeutuneet ja uusien haavoittuvuuksien julkaisun ja hyödyntämisen välinen aika lyhentynyt. Tällä hetkellä puhutaan usein minuuteista haavoittuvuusjulkaisun ja sitä hyödyntämään pyrkivien hyökkäysten välillä. Teknologinen kehitys suosii hyökkääjiä, ja esimerkiksi tekoäly on jo nyt tuottanut merkittävää etua kyberhyökkäysten toteuttajille. Yhä intensiivisemmäksi käyneen kybervaikuttamisen seurauksena tarve ajantasaisen kyberuhkatiedon saamiselle on kasvanut entisestään. Organisaation kriittisimmän omaisuuden suojaamiseen tarvittavat kontrollikeinot tarvitaan yhä nopeammin, kuin mitä ihminen pystyy niitä yksin toteuttamaan. Akuutin ja nopealla aikataululla hyödynnettävän tiedon lisäksi strategiselle ja operatiiviselle tiedolle on suurempi tarve yleisen turvallisuustilanteen heikentyessä ja valtiollisen kybervaikuttamisen yleistyessä.

Kyberuhkatiedon tarve koskeekin jokaista organisaatiota, mutta ei samalla tavalla. Jokaisen organisaation käytettävissä olevat resurssit ja tarpeet määrittävät ne yksilölliset olosuhteet, joissa organisaatio toimii. Kyberuhkatiedon hankkimisen ja hyödyntämisen prosessi on varsin laaja ja monipuolinen. Sen toteuttaminen onnistuneesti vaatii motivaatiota, resursseja ja kokemusta. Kyberuhkatiedon prosessi tulee ymmärtää jatkuvasti käynnissä olevaksi ja kehittyväksi toiminnoksi. Ympyrän tulee pyöriä ja palautetta tulee kerätä eri vaiheiden toteutumisesta. Tärkein tekijä kehittyvän prosessin kannalta on intressi kehittää sitä. Kyberuhkatietoprosessi ei tule mieltää vain pakolliseksi toimenpiteeksi, vaan lisäarvoa tuottavaksi sijoitukseksi, joka voi pelastaa organisaation lamauttavalta vahingolta, taloudellisilta menetyksiltä ja mainehaitalta.

Lopuksi

Käsikirja on ensisijaisesti tarkoitettu suomalaisille kyberturvallisuuslain piiriin kuuluville kriittisen- tai puolustusalan toimijoille, mutta sen sisältö on hyödynnettävissä myös laajemmin organisaation toimialaan tai kokoon katsomatta. Käsikirjassa CTI-prosessin vaiheita (ohjaus, keräys, analysointi ja jakelu) käsitellään yksitellen, jakaen ne kolmeen eri näkökulmaan. Kirjassa jokaisen vaiheen alussa käsitellään organisaation johdon vastuita ja toimenpiteitä. Tämän jälkeen käsitellään operatiivisen tason toimenpiteitä ja operatiivisen johdon velvollisuuksia. Lopuksi käsitellään käytännön ja teknisen tason työkaluja, joita kyseisessä vaiheessa on mahdollista hyödyntää. Tarkoituksena on, että jokaisen näkökulman edustajat saavat konkreettista hyötyä niin, että kokonaisuus hahmottaa mahdollisimman laajasti ja läpileikkaavasti koko kyberuhkatiedon prosessia.

Etelä-Kaukasuksen ja Iranin sodan vaikutukset

KIRSTI NARINEN,
SUURLÄHETTILÄS

Etelä-Kaukasus on alue Mustanmeren ja Kaspianmeren välissä — vuosituhantinen kauppareitti idän ja lännen välillä, entinen Silkkitie, nykyinen Middle Corridor. Vuosisatojen/-tuhansien ajan se on ollut kolmen alueellisen valtakeskuksen — Venäjän, Turkin/ottomaanien ja Iranin/Persian — kohde, uhri, kumppani tai vihollinen, riippuen näiden kolmen keskinäisistä suhteista. Alueen ulkopuolisista maista Israel on viime vuosikymmeninä kasvattanut näkyvyyttään ja merkitystään ja Yhdysvallat viimeisen vuoden aikana. Tilanne on siis sekä uusi että perinteinen. Venäjän vaikutusvalta alueella on heikkenemässä useista syistä, ja Iranin ilmeinen heikkous voisi tarjota Turkille mahdollisuuden valtaotteeseen — vaikka Turkki ei vaikuta erityisesti haluavan tätä. Venäjä on alueellinen valtakeskus, jonka kanssa Turkki ei pitkällä aikavälillä halua kilpailla.

EU:n rooli on erityisesti taloudellisesti nouseva, mutta sen poliittinen vaikutusvalta etsii vielä muotoaan. Georgia on EUn ehdokasmaa-asemastaan huolimatta liukumassa demokratian alamäkeä yhä etäämmälle Euroopan arvoista. Azerbaidžan on ensisijaisesti energiantuottaja, mutta EU-suhde on joillain sektoreilla kehittymässä ja Armenia ainoana aidosti tiivistää EU-yhteistyötään.

Azerbaidžan

Muslimi-identiteetistään huolimatta Azerbaidžan on ollut vuosia Israelin läheinen kumppani sotilaallisesti sekä tieteen, kulttuurin ja teknologian aloilla. Modernin asetekнologian vastineeksi Azerbaidžan on tarjonnut Israelille tärkeän alueellisen tarkkailija-aseman. Azerbaidžan on Turkin läheinen kumppani ja on myös pyrkinyt sovittelemaan Israelin ja Turkin kireää suhdetta.

Iranin kanssa Azerbaidžan on pyrkinyt ylläpitämään herkkää (myönteisesti värittynyttä) tasapainoa. Suhde on vaikuttanut vakaalta, mutta jännitteiseltä. Araks-rajajoelle on suunnitteilla uusi silta, ja on ollut presidenttitason vierailuja, puheluita ja tilannekuvan jakamista. Etelä–pohjoinen-kauppareittiä Kaspian meren rannalle on pyritty rakentamaan Venäjän tuella. Iranin presidentti Pezeshkian on azeri-etnisyydeltään ja puhuu azeria. Khamenein suvulla on myös etnisiä azeri-juuria.

Iranissa asuu arviolta 30 miljoonaa etnistä azerbaidžanilaista. Heillä ei ole separatistisia pyrkimyksiä, ja vaikka he asuvat pääosin pohjoisessa, he ovat levittäytyneet ympäri maata. Ulkoinen hyökkäys kotimaahan on todennäköisesti vahvistanut tämän ryhmän iranilaista identiteettiä.

Maaliskuun 5. päivänä Iran ampui neljä dronea Azerbaidžanin Nachichevanin esklaaviin, joka sijaitsee Armenian takana ja rajautuu Iraniin. Hyökkäys oli virhe Iranilta, joka selitti sen olleen Israelin drooni – yksi ehkä mutta ei neljä. Nachichevan on Azerbaidžanin presidentti Alijevin suvun kotiseutu, mutta alue on muutoin poliittisesti ja taloudellisesti periferiaa. Lentokenttä vaurioitui lievästi ja lennot jatkuivat muutaman päivän kuluessa. Mutta poliittinen viesti oli selvä.

Presidentti Alijev oli ymmärrettävästi sekä raivoissaan että huolissaan. Hän oli todennut ja kokenut tehneensä kaiken voitavansa naapuruuden vakauden säilyttämiseksi. Alijev asetti armeijan täyteen valmiuteen ja vaati Iranilta anteeksipyyntöä. Presidentti Pezeshkian soitti, ilmaisi pahoittelunsa kiistäen samalla Iranin osallisuuden. Julkisella anteeksipyynnöllään hän ilmoitti, ettei Iran tule hyökkäämään maihin, joista sitä itseään vastaan ei ole hyökätty. Media tulkitsi tämän olevan osoitettu Persianlahden arabivaltioille, mutta tarkoituksena taisi olla erityisesti Bakun rauhoittaminen.

Iran ei tarvitse uutta vihollista naapurustoonsa. Ja presidentti Alijev on johtanut maansa rauhan polulle Armenian kanssa vuosikymmenien vihamielisyyden jälkeen — uutta avointa konfliktia ei nyt tarvita. Myöskään Turkki ei todennäköisesti halua kumppanistaan sotaan osapuolta.

Tulkinta droneiskusta terrorismina on jäänyt voimaan. Tapauksen katsotaan viittaavan siihen, että Iran käyttää kriisitilanteissa sotilaallisessa päätöksenteossa hajautettua mallia, joka tässä tapauksessa aluepäällikkö teki huonon valinnan. Presidentti Alijev vastasi pidättämällä näyttävästi azeri-shiia-aktivisteja. Pelko terrori-iskuista ei todennäköisesti ole aiheeton.

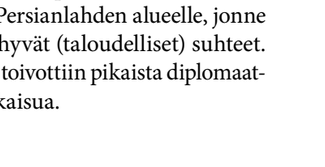
Armenia

Armenialaisilla on luottamukselliset suhteet Iraniin ja yhteyksiä monella tasolla, mutta suhde on enemmän pragmaattinen kuin emotionaalinen. Heille Iran on vakauttava turvallisuuspoliittinen voima molemmilla puolilla olevien turkkilaisten keskellä. Pitkittyneen sodan aiheuttama epävakaus estäisi tai hidastaisi Armenian ja Azerbaidžanin välistä rauhanprosessia, joka otti merkittävän askeleen eteenpäin presidentti Trumpin johdolla Washingtonin huippukokouksessa elokuussa 2025. Rauhanprosessin tärkeänä osana oleva Trump Route for International Peace and Prosperity eli TRIPP yhdistää Azerbaidžanin alueet mutta kulkee aivan Iranin rajalla. Hankkeen eteneminen joutuu odottamaan sodan loppumista.

Armenialaispiireissä ei pidetä ulkoisten voimien aikaansaamaa vallanvaihtoa Iranissa mahdollisena. Muutosvoiman on oltava sisäinen, ja tammikuun mellakoista huolimatta he pitävät antiteokraattisen kansannousun mahdollisuutta pienenä. Järjestelmä on rakennettu kestäväksi ja ulkopuolisen henkilön, kuten Pahlavin, nousu valtaan ei ole todennäköistä. Myös azerit vastustavat häntä — hänen isoisänsä muun muassa kielsi azerbaidžanin kielen käytön tukahduttaessaan väkivaltaisesti azerien kansannousua toisen maailmansodan jälkeen.

Armenian suhde Iraniin on myös taloudellinen. Iranin kanssa on voimassa energianvaihtosopimus, joka kattaa Armeniassa tuotetun kaasun ja sähkön, ja sillä on suuri merkitys Armenian energiaturvallisuudelle. Armenian ulkomaankaupasta 25% kulkee Iranin kautta. Intiasta ja Kiinasta saapuvat tavarat kuljetetaan rekoilla Bandar Abbasin satamasta Armeniaan tai edelleen Georgiaan ja Venäjälle. Hormuzinsalmen sulkeminen on pysäyttänyt toimitukset. Armenia on viime vuosina löytänyt uusia vientimarkkinoita Persianlahden alueelta — pääasiassa lentoteitse, mikä on nyt seisahduksissa. Kriisin aiheuttama pelko on siksi ensisijaisesti taloudellinen. Nousevat polttoainehinnat nostavat inflaatiota ja hidastavat muutoin hyvin käyntiin lähtenyttä talouskasvua.

Armenian monivektoraalinen ulkopolitiikka on toiminut hyvin, eikä sillä ole muuta suoraa omaa riskiä kuin miljoonien pakolaisten aalto Iranin sisällissotaskenaariossa. Noin 50 000 armeenia asuu Iranissa — heidän kotiinpaluunsa olisi myös taloudellinen ja sosiaalinen shokki, sillä maa on vasta toipumassa Karabahin armenialaisten pakkosiirtymisestä (syksy 2023).



Georgia

Georgian demokratian ja ihmisoikeuksien rapautuminen on kiihtynyt viime vuosina siinä määrin, ettei se ole enää mitenkään sovitettavissa yhteen sen entisen läntisen suuntautumisen ja EU-ehdokasmaan johtoaseman kanssa – vaikka hallitus edelleen vakuuttaa EU-jäsenyyden olevan sen tavoite. Georgian hallituksen epämääräinen ulkopolitiikka on arvoitus kaikille, todennäköisesti myös heille itsellensä. Hallitseva puolue Georgian Dreamin lähestymistapa ulkopolitiikkaan on kylvää erimielisyyttä sekä vihollisten että kumppaneiden kanssa ja heidän välilleen. Iran ei ole ollut poikkeus. Irania on huomioitu myönteisesti paljon enemmän kuin kuvitteellinenkaan länsisuuntaus soisi. Hyökkäyksen jälkeiseen hallituksen lausuntoon onnistuttiin sisällyttämään surunvalittelut Iranille valtion johtajien ja siviiliuhrien kuolemasta, surunvalittelut juutalaisille ystäville ja Israelille uhreista ja vahingoista ja vielä päälle solidaarisuuden tunteet Persianlahden alueelle, jonne sillä on hyvät (taloudelliset) suhteet. Lopuksi toivottiin pikaista diplomaattista ratkaisua.

Iranin pehmeä vaikutusvalta on vakiintunut. Georgiassa asuu merkittävä määrä iranilaisia, samoin azerbaidžanilais-taustaisista shiia-aktivisteista koostuva vähemmistöryhmä. Georgiassa toimii useita Iraniin kytkeytyvä shiia-yliopistoja, mukaan lukien Yhdysvaltojen pakotteiden kohteena oleva Al-Mustafa, jossa Koraanin ohella opetetaan länsivastaista ajattelua ja ideologiaa.

Taloudellinen hybridi-vaikuttaminen on myös laajaa. Tuhansia iranilaisia yrityksiä on perustettu äskettäin, ja niitä pidetään Iran-pakotteiden kiertämismekanismeina. Useiden yritysten on todettu olevan lähellä hallituksen taloudellista sisäpiiriä. Useat tätä dokumentoivat tutkimukset ovat saaneet hallituksen kutsumaan tutkijat kuulusteluihin maanpetoksellisesta toiminnasta syytettynä. Iraniin liittyvät paljastukset eivät lupaa toivottua käännettä parempaan Yhdysvaltojen suhteissa. Hallituksen arvokonservatismi ei ole vastoin valtapuolueen odotuksia resonoinut presidentti Trumpin MAGA-politiikan kanssa. Epämääräiset kumppanuuden ja vihamielisyyden mallit eivät luo merkityksellistä luottamusta mihinkään suuntaan. Varapresidentti JD Vance vieraili helmikuussa naapurimaissa mutta jätti Georgian väliin.

Epilogi

Venäjä pitää Etelä-Kaukasusta takapihana, johon sillä on luonnollinen hallintaoikeus. Azerbaidžanilla on fossiilitaloutensa ja kieltämättä taitavan ulkopolitiikkansa kautta melko suvereeni ote Venäjään. Armenia on menettänyt luottamuksensa Venäjään turvallisuuspoliittisena kumppanina, mutta Venäjän taloudellinen ote Armeniaan on merkittävä. Kesäkuun parlamenttivaalit Armeniassa ovat muotoutumassa geopoliittiseksi kilpailuksi uuden moniulotteisen läntisen suuntautumisen, rauhanpolitiikan ja vanhan Venäjä-riippuvuuden välillä. Venäjän hybridivaikuttaminen vaaleihin on jopa näkyviltä osin voimakasta.
Georgian asema on epäselvä. Maata johtaa kulissien takaa miljardööri Bidzina Ivanishvili, joka ajaa omia etujaan enemmän kuin kansallista hyvinvointia. Venäjä hallitsee Abhasiaa ja Etelä-Ossetiaa ja on pitkäaikainen vihollinen, vaikka hallitus näyttää myötäilevän Venäjän toiveita. Valtarakenne toimii omista lähtökohdistaan Venäjän etujen mukaisesti — Venäjälle riittää tarkkailu. Sen vaikutusvalta tulee suoraan hybridiuhkien käsikirjasta, jonka mukaan hybridivaikuttamisen päätavoite on luoda sille suotuinen päätöksentekorakenne. Georgiassa valtapuolue on tehnyt tämän itse. Georgian kansa vaikuttaa ymmärtävän tilanteen paremmin kuin valtarakenne, pitäen demokratian liekkiä elossa vaikeissa olosuhteissa.

Sota on aiheuttanut ja aiheuttaa alueen maille suurta huolta. Vaikka fossiilipolttoaineiden hinnannousú on merkinnyt Azerbaidžanille kohonneita tuloja ja sen asema yhtenä Euroopan vähäisistä luotettavista energialähteistä on vahvistunut, kumppanuussuhde Israeliin on riski, joka saattaa johtaa ennakoimattomiin seurauksiin. USAn ja presidentti Trumpin ailahteleva ja ennakoimaton päätöksentekomekanismi ei lupaa vakaata kehitystä jatkossakaan. Jos Armeniassa Azerbaidžan ja Turkki koetaan hankalina naapureina, Bakun näkökulmasta Venäjä tai Iran ovat vähintään yhtä haastavia.
Rauhanprosessin kannalta positiivista on, että Armenia, Azerbaidžan ja Turkki ovat löytäneet Iranin kriisistä yhteisen sävelen. Yhteydenpito on tiivistynyt. Kaikki toivovat diplomaattisten kanavien avaamista ja nopeaa ratkaisua.

KIRJOITTAJA:

KIRSTI NARINEN
Suurlähettiläs

Suurlähettiläs Kirsti Narinen on ollut ulkoministeriön palveluksessa v.1984 lähtien, ja syksystä 2020 Helsingistä käsin Suomen kiertävänä suurlähettiläänä Armeniassa, Azerbaidzhanissa ja Georgiassa. Hän toimi Tallinnassa lähetystöneuvoksena 1990-luvulla ja suurlähettiläänä 2014-2018, minkä jälkeen kaksi vuotta Hybridiosaamiskeskuksen kansainvälisten suhteiden päällikkönä.

Ajankohtaiset lainsäädäntöhankkeet muokkaavat kyberturvallisuusteollisuuden toimintaympäristöä

RISTO RAJALA
& PETER SUND

Kansainvälinen turvallisuusjärjestys jatkaa murentumistaan. Jo heti alkaneen vuoden ensimmäisinä päivinä Yhdysvallat kohdisti tarkkarajaisen sotilasoperaation Venezuelaan, sieppasi ja poisti vallasta maan presidentti Nicolas Maduron. Onnistuneeksi tulkitsemastaan operaatiosta kenties voimaantuneena Yhdysvallat aloitti kohdistamaan aiempaa voimakkaampaa painostusta Tanskaa ja sen eurooppalaisia kumppaneita vastaan, jotta maa suostuisi myymään sille Grönlannin. Tällä kertaa Eurooppa kuitenkin valitsi jyrkän vastustuslinjan mielistelyn ja joustavuuden sijaan. Kansainvälinen turbulenssi otti uusia kierroksia Yhdysvaltojen ja Israelin aloitettua laajamittaiset ilmaiskut Irania kohtaan, joihin Iran on puolestaan vastannut iskemällä Yhdysvaltoja, Israelia ja Persianlahden arabimaita vastaan sekä uhkaamalla Hormuzinsalmen laivaliikennettä. Samalla useita vuosia käynnissä olevat konfliktit, kuten Venäjän Ukrainaan kohdistama hyökkäyssota, Gazan sota ja Sudanin sisällissota, eivät osoita hiipumisen merkkejä. Informaatio- ja kybervaikuttaminen ovat työkaluina ahkerassa käytössä.

Jatkuva ja kiihtyvä globaali epävakaus heijastuu vahvasti digitaaliseen maailmaan, ruokkien kasvussa olevaa kyberturvattomuutta eli tietoverkkojen kautta toteutettavia laittomia ja kohteelleen vahingollisia tekoja. Erityisesti Yhdysvaltojen ja Iranin välinen sota saattaa nostaa valtiollisten tai valtioihin kytköksissä olevien kyberrikollisten aktiivisuutta entisestään. Vaikeuskerrointa saattaa lisätä entisestään globaalin talouden mahdollinen kriisiytyminen, minkä johdosta yritysten ja organisaatioiden taloudelliset edellytykset tehdä investointeja kyberturvallisuutensa vahvistamiseen voivat vaarantua. Myös Yhdysvaltojen toimet Grönlannin liittämiseksi ovat vahvistaneet jo aiemmin kovaäänisiä vaatimuksia Euroopan digitaalisen suvereniteetin tavoittelemisesta. Digitaalisten palveluiden saatavuusriskin hallinta on kyberturvallisuutta. On vaikea ylikorostaa, kuinka vakavasti Yhdysvaltojen ennennäkemätön poliittinen ja taloudellinen painostus rikkoi eurooppalaisten liittolaisten luottamusta keskeiseen kumppaniinsa.

Geopoliittisen epävarmuuden ja digitaalisten riskien lisääntyessä kyberturvallisuusteollisuuden rooli yhteiskuntien turvallisuuden vahvis-

tajana korostuu. Kyberturvallisuusteollisuuden toimintaympäristöön, kuten koko digitaaliseen talouteen ja elämään, vaikuttaa merkittävästi lainsäädäntö, joka onnistuessaan voi tukea teollisuuden ja koko yhteiskunnan toimintaedellytyksiä ja vahvistaa yhteiskunnan digitaalista resilienssiä. Ajankohtaisia ovat kolme lainsäädäntöhanketta: EU:n kyberturvallisuusasetuksen kokonaisuudistus, kyberkestävyyssäädöksen kansallinen täydentävä lakiehdotus sekä ns. arviointilain kokonaisuudistus, joiden näemme tukevan kyberturvallisuuden edistämistä laajasti.

EU:n Kyberturvallisuusasetuksen uudistaminen herättää toiveita

Euroopan komissio antoi lakiehdotukset koskien kyberturvallisuusasetuksen (CSA2) kokonaisuudistusta sekä siihen liittyvän NIS2-direktiivin muutoksista tammikuussa 2026. Uudistusehdotuksen tavoite on luoda tehokkaampi ja yhtenäisempi EU:n kyberturvallisuusjärjestely uudistamalla EU:n kyberturvallisuusvirasto ENISA:n toimivaltuudet, modernisoimalla ja laajentamalla kyberturvallisuushyödykkeiden sertifiointijärjestelmä ja ottamalla käyttöön EU-tason mekanismi ICT-toimitusketjujen riskien hallintaan. NIS2-direktiivin uudistusehdotus (”NIS2.5”) pyrkii tekemään direktiivistä osin selkeämmän, helpommin noudatettavan ja paremmin yhteen toimivan EU:n kyberturvallisuuslainsäädännön kokonaisuuden kanssa, vähentäen myös yritysten hallinnollista taakkaa.

Lakiehdotuksen kannalta olennaista on, että sääntely tuo selkeyttä ja ennakoitavuutta valvontaan, sertifiointiin ja EU:n ulkopuolisten maiden toimitusketjuriskien hallintaan. Näistä lähtökohdista kummankin lakiehdotuksen päälinjat ovat kannatettavia. Jatkovalmistelussa on kuitenkin huolella varmistettava, että nykyisen lainsäädännön heikkoudet saadaan korjattua.

Uudistuksessa keskeisessä roolissa olevaa ENISAa ja sen oikeusperustaa on arvioitava kriittisesti ja keskityttävä tehtäviin, joissa se voi tuottaa eniten eurooppalaista lisäarvoa – sellaista, jota jäsenvaltiot eivät voi saavuttaa yksin. ENISA:lla on tällä hetkellä liian paljon tehtäviä (määräksi on arvioitu noin 170), ja niitä onkin tarpeen karsia huomattavasti. Monet ENISA:n nykyisistä tehtävistä ovat osin päällekkäisiä muiden virastojen tai jäsenvaltioiden toimintojen kanssa, mikä heikentää viraston kykyä saavuttaa tavoitteitaan ja tuottaa riittäviä tuloksia. ENISA:n toimintamäärärahojen ja henkilöstöresurssien kasvattaminen tulee harkita huolellisesti viraston oikeusperustan ja tehtävien mukaisesti. ENISA:n oikeusperustan muuttamisen ei tule myöskään johtaa jäsenvaltioiden kyberturvallisuusviranomaisten kustannusten lisääntymiseen, vaan pikemminkin kustannussäästöihin – tämä on eritoten Suomelle olennainen asia.

ENISA:n nykyiset tehtävät, kuten teollisuuden tukeminen ja parhaiden käytäntöjen laatiminen, ovat päällekkäisiä kansallisten viranomaisten sekä markkinoiden kanssa. Koulutus-, osaamistoiminnot, kansalaisviestintä sekä standardointiin osallistuminen kuuluvat selvemmin jäsenvaltioille ja eurooppalaisille standardointijärjestöille. Samalla ENISA:n operatiivisia tehtäviä tulee korostaa, painottaen kyberuhkien torjuntaa ja tilannekuvan muodostamista, erityisesti tukien jäsenvaltioiden kansallisia kyvykkyyksiä. ENISA:n tehtävien siirto jäsenvaltioilta tulee perustua siihen, että se tuottaa enemmän lisäarvoa tai merkittäviä säästöjä, eikä heikennä kansallisten viranomaisten roolia.

Lakiehdotuksessa kaavaillulle eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän uudistukselle on suuri tarve. Kyberturvallisuusasetuksen mukaisen eurooppalaisen kyberturvallisuussertifiointijärjestelmän puitteissa ole neljän vuoden aikana saatu voimaan yhtäkään tuote- tai palvelusertifiointikehystä eikä sellaisia ole näköpiirissä ainakaan lyhyellä aikavälillä. EU:n kyberturvallisuusvirasto ENISA ei ole hoitanut tehtäväänsä EU:n kilpailukykyä edistävällä tavalla. Kyberturvallisuusasetuksen uudistusehdotukseen kuuluva sertifiointijärjestelmän uudistus on tervetullut ja tärkeä askel kohti selkeämpää, ketterämpää ja vaikuttavampaa eurooppalaista kyberturvallisuutta. Houkuttelevuutta tulee vahvistaa sertifioinnin kustannusten hallinnan kautta. Tällöin sertifioinnista voi muodostua hyödyllinen väline yrityksille sisämarkkinoille pääsylle. EU:n laajuinen vaatimustenmukaisuutensa osoittaminen yhdenmukaisesti helpottaa tuotteiden ja palvelujen markkinoillepääsyä ja vahvistaa kilpailukykyä.

Esityksessä ehdotetaan uusia sääntöjä tieto- ja viestintätekniikan toimitusketjujen turvallisuudelle, joka olisi toteutuessaan merkittävä muutos nykytilaan. EU voisi tunnistaa kriittisiä ICT-hyödykkeitä ja niiden korkean riskin toimittajia kolmansista maista, rajata niitä julkisten hankintojen, EU:n julkisen tuen sekä eurooppalaisen standardoinnin ulkopuolelle sekä asettaa niitä käyttökieltoon.

Esitetty ICT-toimitusketjujen turvallisuuden hallinnan mekanismi on tarpeellinen. ICT-toimitusketjujen turvallisuuden hallintamekanismi rakentuisi EU-tasoiselle, riskiperusteiselle ja teknologianeutraalille menettelylle, jonka tavoitteena on tunnistaa kriittiset ICT-hyödykkeet (komponentti, järjestelmä, laite, palvelu tai alusta, joka on olennainen osa kriittistä infrastruktuuria, keskeinen toimitusketjun toimivuudelle ja sen väärinkäyttö voi aiheuttaa merkittävää haittaa) ja niihin liittyvät toimittajariippuvuudet.

Kyberkestävyyssäädöksen toimeenpano etenee

Vuonna 2024 hyväksytyn kyberkestävyyssäädöksen toimeenpano etenee niin Suomessa, kuin EU-tasolla säädettyjen siirtymäaikojen puitteissa. Asetus luo edellytykset turvallisisiksi suunniteltujen ohjelmisto- ja laitteistotuotteiden kehittämiselle ja varmistaa, että tuotteet tuodaan markkinoille perusturvallisina, myös kolmansista maista. Kyberala on korostanut, että asetuksen tavoitteet eivät toteudu ilman tehokasta toimeenpanoa EU-jäsenmaissa. Hallituksen esitys kyberkestävyyssäädöksen toimeenpanoa koskevaksi lainsäädännöksi vastaa osin tähän tarpeeseen ja on parhaimmillaan Eduskunnan käsittelyssä.

Kansallinen toimeenpanolaki on monella tapaa kannatettava. Kyberkestävyyssäädöksen markkinavalvontaviranomaisen tehtävät on järkevää keskittää Liikenne- ja viestintävirastolle (Traficom), viraston osaamisprofiilin ja synergioiden vuoksi. Suomen on pyrittävä varmistamaan myös EU-tasolla, ettei asetuksen soveltamiseen ja markkinavalvontaan synny olennaisia eroavaisuuksia jäsenvaltioiden välillä. Tavoitteena on oltava, että Suomen elinkeinoelämä on kyberkestävyyssäädöksen soveltamisen osalta yhdenvertaisessa asemassa muihin jäsenvaltioihin nähden.

Valvonta- ja viranomaistehtävien lisääntyessä on huolehdittava toiminnan tehokkuudesta. Huomiota on kiinnitettävä haavoittuvuuksien hallinasta ja pakollisten haavoittuvuusilmoitusten vastaanottamisen edellytyksistä, sillä ilmoittajille on asetettu jo laissa hyvin tiukkoja aika- ja laatumääreitä. Tarvittaessa muita tehtäviä, kuten tietoturvaloukkausten selvitystehtävien sekä teknisten neuvontatehtävien siirtämistä nykyistä laajemmin markkinatoimijoille soveltuvien yhteistyömenettelyiden avulla.

Lain kannalta keskeinen kokonaisuus on tuotteiden ja ohjelmistojen vaatimuksenmukaisuutta arvioivien ilmoitettujen laitosten toiminnan järjestäminen. Näillä arviointilaitoksilla tulee olemaan merkittävä vaikutus paitsi kyberturvallisuusteollisuuden toimintaympäristöön, myös Suomen keskeisimpien vientialojen kilpailukykyyn. Lakiesityksessä Traficom ollaan nimeämässä kyberkestävyyssäädöksessä tarkoitetuksi ilmoittamisesta vastaavaksi viranomaiseksi eli tärkeimmäksi kansallisen arviointitoiminnan järjestäjäksi.

Kyberkestävyyssäädöksen onnistunut kansallinen toimeenpano mahdollistaa kilpailuetuja ja talouskasvua Suomessa toimiville yrityksille, mikä osaltaan tukee myös julkisen talouden tasapainottamista. Ilmoitetuista laitoksista hyötyvät erityisesti Suomessa toimivat vientiyritykset, jotka saisivat asetuksen soveltamisalaan kuuluvat tuotteensa EU:n sisämarkkinoille kansainvälisiä kilpailijoitaan luotettavammin ja nopeammin. On huomattava, että esimerkiksi vuonna 2025 Suomen CRA-liitännäisen tavaraviennin (elektroniikka-, ICT-tuotteet sekä koneet ja laitteet) arvo oli

noin 27,3 miljardia euroa, mikä vastaa noin 37 % koko Suomen tavaraviennistä. Jo yksistään tästä syystä vaatimustenmukaisuuden arvioinnista ei saa muodostua hidastetta kotimaisten tuotteiden markkinoillepääsylle. Lisäksi Suomessa toimivat laitokset mahdollistavat palveluiden tarjoamisen koko EU-alueella toimiville laite- ja ohjelmistovalmistajille sekä maahantuojille palveluvientinä. Kyberkestävyyssäädös mahdollistaa myös viranomaisten fasilitoimien testiympäristöjen perustamisen esimerkiksi erilaisten tuotteiden tai olosuhteiden testaamista varten. Vastaava menettely sisältyy myös EU:n tekoälyasetukseen.

Kansallisen arviointilain uudistus vahvistaa arviointitoiminnan uskottavuutta

Hallitus valmistelee parhaillaan viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointia koskevan lainsäädännön muuttamista. Kyseessä arviointilainsäädännön kokonaisuudistus, joka vahvistaa julkishallinnon kriisinkestävyyttä, selkeyttää viranomaisten vastuita ja parantaa tietojärjestelmien turvallisuusarviointien saatavuutta. Kyberala on pyrkinyt edistämään arviointimenettelyjen selkeyttämistä, arviointiviranomaisten tiivistä yhteistyötä sekä mahdollisuutta hyödyntää yksityisiä toimijoita tehokkaasti arviointityössä.

Arviointilain uudistuksessa on keskeistä, että ns. varautumisen arviointi otetaan osaksi lakia, mikä vahvistaa viranomaisten kykyä turvata toiminnan jatkuvuus häiriötilanteissa ja poikkeusoloissa sekä tukee tiedonhallintalain tavoitteita. Lisäksi turvallisuuskriittisten ratkaisujen ja niiden valmistajien arviointi ja hyväksyntä lainsäädännössä lisää läpinäkyvyyttä, yhdenmukaistaa menettelyt EU- ja NATO-vaatimusten kanssa, ja parantaa kotimaisten toimijoiden kilpailukykyä. Puolustusvoimille esitetty arviointiviranomaisen rooli vastaa kasvaviin tarpeisiin, mutta sen rajaus ja resurssien käyttö tulee suunnitella huolellisesti, jotta järjestely ei rajoita yksityisten arviointilaitosten toimintaa tai aiheuta kestämättömiä kustannuksia julkiselle taloudelle.

Valtionhallinnon viranomaisille ehdotettu oman toiminnan ja riskien arviointivelvollisuus, joka kattaa sekä itsearvioinnin että riippumattoman arvioinnin tietyissä turvallisuusluokissa, parantaa riskienhallintaa ja selkeyttää vastuunjakoa. Arviointimenettelyjen laajentaminen ja täsmentäminen, mukaan lukien viranomaisen toimeksiannosta palveluntarjoajan toteuttama arviointi, lisää arviointien saatavuutta ja tukee elinkeinotoiminnan edellytyksiä. Arviointiperusteiden ajantasaistaminen varmistaa, että kriteerit vastaavat teknologian kehitystä ja kyberturvallisuusvaatimuksia, mikä vahvistaa toiminnan johdonmukaisuutta ja ajantasaisuutta.

Arviointilaitosten pätevyyksien hyväksymismenettelyjen joustavoittaminen edistää markkinoiden toimivuutta, ja yritysturvallisuusselvityksen käyttö lisää luotettavuutta. Arviointiviranomaisten yhteistyön ja tiedonvaihdon vahvistaminen sekä mahdollisuus käyttää yksityisiä toimijoita arviointien tukena parantavat arviointien tehokkuutta ja yhtenäistävät tulkintoja, samalla kun ne tukevat yritystalouden kehitystä.

Aktiivinen vaikuttamistyö toimintaympäristön parantamiseksi jatkuu

Onnistuessaan uudistettu kyberturvallisuusasetus, kyberkestävyyssäädöksen toimeenpanolaki ja arviointilain kokonaisuudistus ovat merkittävä askel kohti parempaa digitaalista elämää, sekä uusien liiketoimintamahdollisuuksien mahdollistamaa talouskasvua. Kyberala ry on ollut vahvasti vaikuttamassa kaikkiin kolmeen lainsäädäntöhankkeeseen niiden eri valmisteluvaiheissa yksityisen ja julkisen sektorin välistä yhteistyötä edistäen ja luottamusta rakentaen.

KIRJOITTAJAT:

PETER SUND

Kyberala ry:n (FISC ry) toimitusjohtaja

Teknologiateollisuus ry

Jukka Rapo

RISTO RAJALA

Kyberala ry:n (FISC ry) neuvonantaja

Teknologiateollisuus ry

Cyberwatch Finland

VIIKKOKATSAUS

9/2026

Teemakatsaus

UKRAINA

Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

Cyberwatch Finland

VIIKKOKATSAUS

9/2026

- Venäjän painopiste kyberoperaatioissa Ukrainassa on ollut tiedustelussa. Samaan aikaan näkyvämpää kybervaikuttamista on kohdistettu Ukrainaa tukeviin maihin.

- Ukraina on jatkuvasti korostanut hyökkäyksellisten kyberoperaatioiden merkitystä, ja viime kesänä niistä nähtiinkin esimerkki Aeroflotin kärsiessä valtavat tappiot kyberhyökkäyksen takia. Venäjä on pyrkinyt puolustautumaan siirtymällä valtion kontrollissa olevaan digitaaliseen ekosysteemiin.

- Tekoälyä vähintään jollain tapaa hyödyntävien kyberhyökkäysten määrä on viimeisen vuoden aikana lisääntynyt eksponentiaalisesti, ja nykyään täysin tekoälystä irrallinen hyökkäys on jo harvinaisuus.

Ukraina-teemakatsaus

Jälleen yksi vuosi on kulunut, ja Ukrainan täysimittaisessa sodassa siirrytään jo viidenteen vuoteen. Huomioidakseen vuosipäivän ja Ukrainan pyrkimykset torjua hyökkäystä Cyberwatch Finland julkaisee jälleen jo perinteeksi muodostuneen teemakatsauksen konfliktin kybertapahtumista viimeisen vuoden ajalta. Sodan neljättä vuotta on leimannut tekoälyn nopeasti lisääntynyt käyttö kyberhyökkäyksissä. Kiovan kansainvälisessä kyberresilienssifoorumissa 2026 ukrainalaiset totesivat, että noin 90 % venäläisistä kyberhyökkäyksistä käyttää tällä hetkellä jollain tavalla tekoälyä hyväkseen. Tämä heijastaa laajempaa maailmanlaajuista trendiä, jossa tekoälyn käyttö kasvaa kaikilla elämän osa-alueilla. Siksi se on ollut kuuma aihe myös kyberturvallisuudessa.

Eräs helmikuun foorumissa esiin noussut mielenkiintoinen seikka oli se, miten yksityinen sektori on noussut yhä suositummaksi kohteeksi kyberhyökkäyksille. Ukrainassa yli 50 % kaikista kyberhyökkäyksistä kohdistuu yksityisiin yrityksiin, ja sama toistuu myös rintaman toisella puolella. Yksityiset yritykset ovat usein helpompia kohteita löyhempien kyberturvallisuuskäytännöiden takia. Samalla niihin kohdistettujen hyökkäysten vaikutukset voivat vaikuttaa tavallisten kansalaisten elämään huomattavalla tavalla. Siksi ukrainalaiset pitävät tällä hetkellä nopeampaa sopeutumista vauhdilla kehittyviin uhkiin suurimpana haasteenaan. Tavallisetkin kansalaiset tarvitsevat koulutusta suojatakseen itseään ja työpaikkojaan kehittyneiltä kyberuhkilta. Tarvittava teknologia on olemassa, mutta henkilöstön koulutus ei pysy vauhdissa mukana.

Eräs mielenkiintoinen tapa ratkaista ongelma on täysin uusi aloite, jonka tarkoituksena on houkutella yhä useampia naisia valitsemaan kyberturvallisuus opintojensa aiheeksi. Ongelma johtuu osittain siitä, että suurin osa IT-ammattilaisista on miehiä, ja merkittävä osa heistä on tällä hetkellä etulinjassa tai vähintäänkin vaarassa joutua sinne lähitulevaisuudessa. Kuten Ukrainan kansallisen turvallisuus- ja puolustusneuvoston toimiston tieto- ja kyberturvallisuusosaston johtaja Nataliya Tkachuk totesi, naisten osuuden kasvattaminen kyberturvallisuuteen liittyvissä ammateissa ei ole tasa-arvokysymys; kyse on selviytymisestä.

Ukrainan valtion erityisviestintä- ja tietosuojapalvelun johtaja Oleksandr Potii totesi foorumissa, että Venäjän kyberhyökkäykset Ukrainan kriittistä infrastruktuuria vastaan keskittyvät yhä enemmän tiedustelutiedon keräämiseen järjestelmien häiritsemisen sijaan. Se koskee myös energia-alaa, joka on ollut kovan paineen alla koko sodan ajan, mutta erityisen koville se on joutunut tänä talvena. Venäjä käyttää kyberkeinoja kerätäkseen tietoa kriittisten laitosten sijainnista ja kohdistaa niihin sitten ohjus- ja drooni-iskuja. Läsnäoloa Ukrainan järjestelmissä hyödynnetään iskujen tehokkuuden ja ukrainalaisten korjaustoimien arviointiin. Tämä on erinomainen esimerkki siitä, miten Venäjä käyttää kyberteknologiaa kineettisten operaatioiden tukielementtinä. Kyseinen trendi on korostunut neljännen vuoden aikana. Kuten Potii totesi: ”Kyberhyökkäykset kriittiseen infrastruktuuriin eivät koskaan tapahdu kaikesta muusta irrallaan, ne ovat aina osa laajempaa toimintaa.”

Syitä painopisteen muutokselle kohti tiedustelutiedon keräämistä voidaan tunnistaa ainakin kaksi. Ensinnäkin Venäjä näyttää ymmärtäneen, että sota tulee kestämään pitkään, ja tiedustelun arvo on siksi kasvanut. Se antaa venäläisille mahdollisuuden suunnitella operaatioita paremmin tulevaisuudessa, sillä nopea voitto on osoittautunut mahdottomaksi. Toiseksi järjestelmien vahingoittaminen on paljon tehokkaampaa kineettisillä keinoilla kuin kyberhyökkäyksillä, sillä Ukraina on ollut menestyksekäs puolustautuessaan vakavia kyberuhkia vastaan. Venäjä yrittää nyt optimoida resurssien käyttöä valitsemalla parhaan työkalun kuhunkin tehtävään sen sijaan, että se edelleen kokeilisi kaikkia vaihtoehtoja umpimähkään.

Venäjä on selvästi suurin kyberuhka Ukrainalle, mutta se ei ole ainoa. Venäjään liittyvien operaatioiden lisäksi toimintaa on raportoitu myös Valko-Venäjältä, Kiinasta ja Pohjois-Koreasta. Tämä ei ole yllätys, sillä nämä maat nähdään usein työskentelemässä yhdessä. Pohjois-Korea on jopa lähettänyt joukkoja taistelemaan Venäjän rinnalle, ja havaintoja maiden välisestä yhteistyöstä kyberrintamalla on pulpahdellut pintaan jo jonkin aikaa. Valko-Venäjä on hyvin todennäköisesti samassa tilanteessa, sillä se on auttanut Venäjää laajasti täysimittaisen hyökkäyksen alusta lähtien, jolloin osa Venäjän joukoista lähti liikkeelle Ukrainan ja Valko-Venäjän rajalta. Kiinan suhteen tilanne on kuitenkin erilainen. On hyvin mahdollista, etteivät kiinalaiset koordinoi toimiaan Venäjän kanssa, vaan heillä on omat yksittäiset operaationsa käynnissä Ukrainassa. Kiina on perinteisesti ollut hyvin haluton tekemään yhteistyötä kyberoperaatioissa, joten äkillinen suunnanmuutos juuri nyt olisi melko yllättävää.

Siirtymä suoraa vahinkoa aiheuttavista hyökkäyksistä vakoiluun pätee myös muihin kohteisiin kuin kriittiseen infrastruktuuriin, sillä se on osoittautunut Venäjän menestyksekkäimmäksi strategiaksi viimeisen vuoden aikana. Venäjän muut kuin tiedusteluun liittyvät kyberhyökkäykset ovat kohdistuneet pääasiassa Ukrainaa tukeviin maihin, koska kineettisen voiman käyttö halutun vaikutuksen aikaansaamiseksi ei ole niiden kohdalla samalla tavalla vaihtoehto. Esimerkkejä tällaisista hyökkäyksistä ovat Norjan Risevatnet-järven vesivoimalan ohjausjärjestelmän haltuunotto viime huhtikuussa sekä hyökkäys Puolan sähköverkkoon joulukuun lopussa. Molemmille kyberhyökkäyksille tunnusomaista oli se, että ne kohdistuivat sähköntuotantoon, johon Venäjä on keskittänyt tuhovoimaansa myös Ukrainassa, tosin kineettisesti. Ukrainan sisällä merkittävimmät häiriötä tai tuhoa tavoittelevat hyökkäykset kohdistettiin maan rautatiejärjestelmiin maaliskuussa ja viljateollisuuteen kesällä.

Ukraina ei ole myöskään jäänyt toimettomaksi, ja viime kesänä pääsimmekin lukemaan suuresta kyberhyökkäyksestä Venäjän kansallista lentoyhtiötä Aeroflotia vastaan. Se oli monille shokki, sillä hakkerit onnistuivat murtautumaan kaikkiin yrityksen järjestelmiin. Hintalappu nousi kymmeniin miljooniin dollareihin, mutta ehkä vielä merkittävämpiä olivat paljastukset yhtiön johtajistosta ja tyytymättömyys, jota venäläiset matkustajat kokivat heidän lentojensa peruuntuessa kesken lomakauden. Venäjän viranomaisille tapaus oli äärimmäisen kiusallinen, ja heidän yrityksensä vähätellä hyökkäyksen vaikutuksia olivat suurelta osin epäonnistuneita.

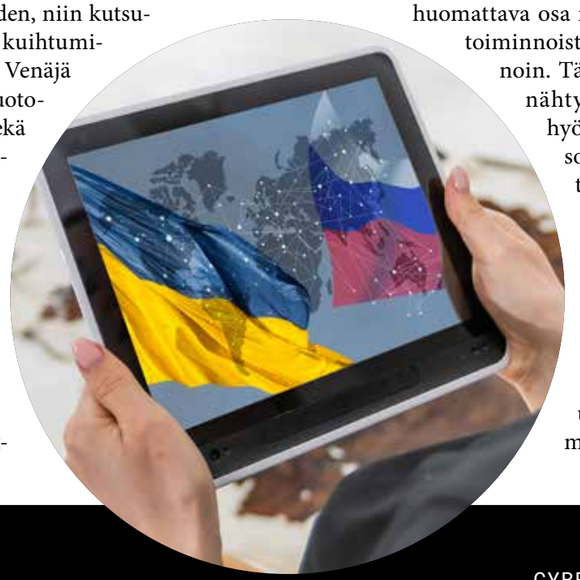
Ukrainan hallitus ei ole virallisesti myöntänyt olleensa hyökkäyksen takana, mutta sen tekijöillä tiedetään olevan vahvat siteet maahan. Ukrainan viranomaisten julkiset lausunnot ovat olleet hyvin rajallisia operatiivisen turvallisuuden vuoksi: hyökkäykselliset kyberoperaatiot ovat tärkeä osa heidän työkalupakkiaan, mutta he kieltäytyvät kommentoimasta yksityiskohtia. Hyökkäysoperaatioiden roolia on korostettu yhä enemmän sodan aikana, ja näyttää siltä, että alamme vihdoin nähdä konkreettisia tuloksia myös mediassa. Vaikuttaa erittäin todennäköiseltä, että täysimittaisen sodan viides vuosi sisältää entistä enemmän kyberhyökkäyksiä Venäjää vastaan, ja joidenkin mielestä Ukraina jopa nousee kiistattomaan asemaan kybersodan hallitsevana osapuolena.

Muutokset Venäjällä

Samaan aikaan Venäjä on ajanut kaupallisia viestintäsovelluksia ahtaalle ja painostanut ihmisiä käyttämään hallituksen kontrolloimaa Maxia. Monet palvelut, kuten WhatsApp, YouTube ja Discord ovat nyt saatavilla enää vain VPN:n avulla. Myös Venäjän suosituimpiin viestintäpalveluihin kuuluva Telegram on kohteena kansalaisten ja jopa joidenkin viranomaisten vastustuksesta huolimatta. Ukrainan rajan lähellä Telegramin välityksellä ilmoitetaan usein hätätiedotteista, ja osa sotilaista käyttää sitä jopa logistiikan järjestämiseen. On melko selvää, että Venäjä etenee aggressiivisesti kohti valtion kontrolloimaa digitaalista ekosysteemiä, jossa hallitus voi Kiinan tapaan valvoa ja hallita kansalaisten kuluttamaa sisältöä.

Mobiiliverkkoihin on asetettu laajempiakin rajoituksia, joiden tarkoituksena on estää ukrainalaisten lennokkien toimintaa. Lisäksi viranomaiset ottivat lokakuussa käyttöön 24 tunnin mobiiliyhteyskatkon kaikille, jotka saapuvat maahan ulkomaisella SIM-kortilla. Se on herättänyt merkittävää kritiikkiä henkilöiltä, jotka joutuvat säännöllisesti ylittämään rajan liiketoiminnallisista syistä. Matkapuhelinverkkojen saatavuuden häiriöt ovat luonnollisesti suurempia Ukrainan rajan läheisyydessä. Venäjän armeija on käyttänyt Starlinkia viestinnän tukena, mutta SpaceX ryhtyi helmikuun alussa toimiin estääkseen sen. Telegramin käytön rajoitusten lisäksi Starlink-yhteyksien menetyksellä on ollut merkittävä vaikutus Venäjän sotilaalliseen viestintään, eikä korvaavia vaihtoehtoja ole saatavilla. Venäjä kohtaa vaikeuksia erityisesti viestinnän nopeuden, liikkuvien ryhmien koordinoinnin ja lennokkien kuvasyötteen osalta.

Eräs sodan yllättävä seuraus on ollut Venäjän laittomien datamarkkinoiden, niin kutsutun probivin (пробив) kuihtuminen. Korruption takia Venäjä on ollut data- ja tietovuotojen luvattu maa, jossa sekä kaupallisten että viranomaisten tietojärjestelmien tietoja on myyty pimeässä verkossa. Näitä tietoja ovat hyödyntäneet muun muassa oppositioaktivistit sekä tutkivat journalistit. Yksi suosituimmista kategorioista on ollut niin kutsuttu ”mobiili probiv”, eli haluttuun puhelinnumeroon liittyvien tietojen, kuten puhelin- ja viestilokien laiton ostaminen. Muita yleisesti myytäviä tietoja ovat olleet esimerkiksi henkilöiden passitiedot, pääsy turvallisuuspalvelu FSB:n rajatietokantaan sekä lentoyhtiöiden matkustajalistat.



Juuri probivin on arveltu osaltaan olleen Ukrainan tiedustelun onnistumisten, kuten Venäjän armeijan korkea-arvoisten komentajien salamurhien taustalla. Tämä on johtanut siihen, että Venäjä on alkanut suhtautua tietovuotoihin aiempaa ankarammin. Vuonna 2024 lainsäädäntöä uudistettiin ja datan laittomasta käytöstä, siirrosta, keräämisestä tai tallentamisesta voi nykyään saada jopa 10 vuoden vankeusrangaistuksen. Esimerkkejä pidätyksistä on myös nähty. Kesällä 2025 Moskovassa pidätettiin seitsemän sisäministeriön datakeskuksen työntekijää väärinkäytöksistä epäiltynä. Koventuneet rangaistukset ja pidätykset ovat johtaneet siihen, että laittomilta datamarkkinoilta on poistunut toimijoita, ja vielä jäljellä olevien tietopakettien hinnat ovat nousseet merkittävästi.

Kaiken kaikkiaan neljättä sotavuotta ovat kybernäkökulmasta leimanneet tekoälyn käyttö, venäläisten kyberoperaatioiden painopisteen siirtyminen tiedusteluun sekä ukrainalaisten hyökkäyksellisten kyberoperaatioiden lisääntyminen. Samalla Venäjä on pyrkinyt torjumaan ukrainalaisten operaatioita muun muassa siirtymällä kohti valtion kontrollissa olevaa digitaalista ekosysteemiä Kiinan tapaan. Laajamittaisen hyökkäyksen alussa vuonna 2022 pohdittiin paljon sitä, millaiseksi kyberhyökkäysten rooli sodassa muodostuu. Pahimmissa skenaarioissa käsiteltiin jopa jonkinlaisen “kyberapokalypsin” mahdollisuutta, jossa huomattava osa modernin yhteiskunnan toiminnoista lamautetaan kyberkeinoin. Tällaista ei toistaiseksi ole nähty, mutta käsitys kyberhyökkäysten merkityksestä sodan kontekstissa on toki tarkentunut. Viides sotavuosi tulee todennäköisesti sisältämään lisää ukrainalaisia kyberhyökkäyksiä Venäjän keskittyessä hybridisotaan Ukrainaa tukevien maiden kanssa sekä ukrainalaisten järjestelmien tiedusteluun.

Neljännen sotavuoden merkittävimpiä kyberhyökkäyksiä:

UKRZALIZNYTSIA

AJANKOHTA: 23.3.2025
KUVAUS: Ukrainan valtiollinen rautatieyhtiö koki maaliskuussa 2025 vakavan kyberhyökkäyksen, jonka tavoitteena vaikutti olevan junaliikenteen pysäyttäminen. Rautatieverkko on Ukrainassa keskeisessä osassa paitsi siviilien, myös sotilaiden, haavoittuneiden sekä sotilasmateriaalin kuljetuksessa.
TEKIJÄ: Hyökkäystä ei ole onnistuttu tunnistamaan mihinkään tiettyyn venäläiseen hakkeriryhmään tai turvallisuuspalveluun. Vaikuttaa kuitenkin selvältä, että Venäjä oli hyökkäyksen takana.

VAIKUTUKSET: Hyökkääjä onnistui haittaohjelmalla keskeyttämään rautatieyhtiön verkkosivujen ja mobiilisovelluksen toiminnan useiden päivien ajaksi. Ongelmat alkoivat jo maaliskuun 23. päivä, ja vielä huhtikuun alussa osa palveluista oli poissa käytöstä, vaikka toimintojen kerrottiin palautuneen 90-prosenttisesti. Käytännössä haittaohjelma esti junamatkustajien lippujen ostamisen rautatieyhtiön verkkosivuilta ja mobiilisovelluksesta, minkä lisäksi vaikutuksia oli rahdinlähettäjien verkkopalveluiden toimintaan. Hyökkäyksen tekniset yksityiskohdat eivät ole selvillä, mutta hyökkäys aiheutti jonoja ja sekaannusta rautatiepalveluissa.

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.

VAIKUTUKSET: Ensimmäisen päivän aikana lentoja peruttiin 108 ja pelkästään Moskovan 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.

PUOLAN SÄHKÖVERKKO

AJANKOHTA: 29.12.2025
KUVAUS: Puolan sähköverkkoon kohdistui koordinoituja kyberhyökkäyksiä vuodenvaihteen alla 2025. Tapahtuma on malliesimerkki Venäjän laaja-alaisesta vaikuttamisesta, jonka kohteena ovat Ukrainaa tukevat valtiot. Venäläiset hakkerit ovat hyökänneet kriittistä infrastruktuuria vastaan myös esimerkiksi Norjassa.
TEKIJÄ: Hyökkäys on attribuoitu Venäjän sotilastiedustelu GRU:n Sandworm-ryhmään, joka oli muun muassa Ukrainan sähköinfrastruktuurin vuosien 2015 ja 2016 hyökkäysten takana.

VAIKUTUKSET: Hyökkäys vaikutti sähkön ja lämmön yhteistuotantolaitosten (Combined Heat and Power, CHP) viestintä- ja ohjausjärjestelmiin sekä järjestelmiin, jotka hallinnoivat uusiutuvan energian järjestelmien jakelua tuuli- ja aurinkovoimaloista. Hyökkäys ei johtanut sähkökatkoihin, mikä on voinut antaa valheellisen kuvan heikosta tai epäonnistuneesta iskusta. Tosiasiassa monet järjestelmistä vaurioituivat korjauskelvottomiksi. Kyseessä on arvioitu olevan toistaiseksi laajin venäläinen sabotaasihyökkäys Eurooppaan.

LÄHTEET:

https://carnegieendowment.org/russia-eurasia/politika/2026/02/russia-starlink-telegram-shutdown

https://www.dragos.com/blog/poland-power-grid-attack-electrum-targets-distributed-energy-2025

https://therecord.media/ukraine-cyberattacks-guiding-russian-missile-strikes

https://euromaidanpress.com/2026/01/27/security-service-of-ukraine-blocked-14000-russian-attacks-since-2022/?utm_source=chatgpt.com

https://regard-est.com/ukraine-facing-the-intensification-of-russian-cyber-attacks

https://industrialcyber.co/critical-infrastructure/russian-linked-uac-0219-group-escalates-attacks-on-ukraine-government-critical-infrastructure/#:~:text=CERT%2DUA%2C%20which%20named%20the,agency%20planned%20to%20cut%20salaries.

https://www.reuters.com/world/europe/ukraines-railways-restore-half-it-services-hit-by-cyber-attack-so-far-2025-04-09/

https://therecord.media/russia-sandworm-grain-wipers

https://meduza.io/en/feature/2025/07/29/too-much-is-slipping-through

https://zona.media/news/2025/07/13/probiv

https://www.theguardian.com/world/2025/dec/26/russia-selling-personal-data-leaks-probiv-ukraine-spies

https://therecord.media/whatsapp-russia-blocked-state

https://therecord.media/russia-throttles-telegram-pushes-its-own-messaging-app

Cyberwatch VIIKKOKATSAUS

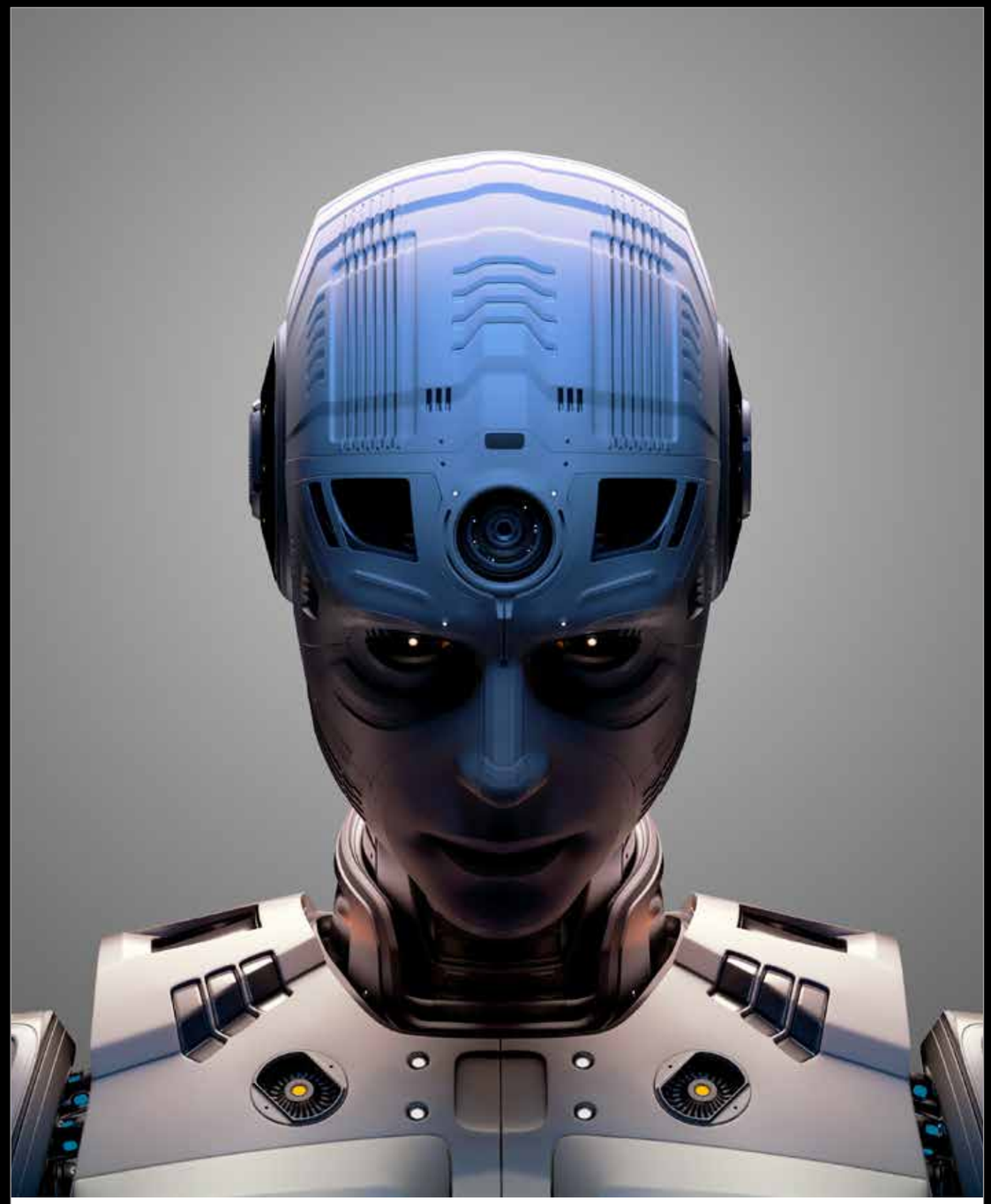
JULKAISIJA Cyberwatch Finland | Nuijamiestentie 5 C, 04400 Helsinki | www.cyberwatchfinland.fi

Cyberwatch Finland

KUUKAUSIKATSAUS

HUHTIKUU/2026

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

Maaliskuu osoitti jälleen kyberuhkien ja geopoliittisten konfliktien kietoutuvan yhteen. Erityisesti Iranin kyberoperaatiot olivat näkyviä ja hyökkäyksiä kohdistui yhdysvaltalaisten sekä israelilaisten kohteiden lisäksi laajasti muihinkin valtioihin varsinkin Lähi-idän alueella. Alankomaiden tiedustelupalvelut taas varoittivat maaliskuussa venäläisestä kybervakoilukampanjasta, jonka tavoitteena olisi toimittajien, viranomaisten ja asevoimien henkilöstön Signal- ja WhatsApp-tilien kaappaaminen. Baltiassa Venäjää on syytetty tahallisesta verkon disinformaatiokampanjasta, jonka mukaan maat sallisivat ilmatilansa käytön ukrainalaisille drooneille. EU vastaavasti asetti pakotelistalleen kaksi kiinalaista ja yhden iranilaisen yhtiön EU-jäsenvaltioihin kohdistuneiden kyberhyökkäysten takia.

Kuukauden konkreettisissa kyberhyökkäyksissä yhdysvaltalainen lääkintälaitteiden valmistaja Stryker joutui kyberhyökkäyksen kohteeksi, jonka seurauksena Microsoft-pohjaiset järjestelmät häiriintyivät ja vaikutukset ulottuivat tuotantoon sekä toimitusketjuihin. Hyökkäyksen takana oli Iraniin kytkeytyvä Handala Hack Team -ryhmä. Myöskään valtioista riippumattomat kyberrikolliset tai hakkerit eivät ole levänneet. Suomessa suosittu kuntosaliketju Elixia joutui tietomurron kohteeksi ja muun muassa asiakkaiden nimiä ja yhteystietoja vaarantui. Globaalisti tietoturvayhtiö Cyber Intelligence Housen tilastojen mukaan pelkästään maaliskuussa kiristyshaittaohjelmaryhmät listasivat sivuilleen yli 2000 uutta uhria.

Teknisten haavoittuvuuksien osalta maaliskuussa havaittu kriittinen haavoittuvuus suositun ohjelmistoyritys Citrixin NetScaler ADC- ja NetScaler Gateway -tuotteissa (CVE-2026-3055, CVSS 9.3) joutui aktiivisen hyväksikäytön kohteeksi. Tapaus korostaa osaltaan haavoittuvuuksien hyväksikäyttösyklien nopeutumista: aikaa haavoittuvuuden julkistamisesta aktiiviseen hyväksikäyttöön on yhä vähemmän.

Tekoälyteknologian riskit olivat niin ikään näkyviä. Internet-jätti Metassa koettiin sisäistä kaaosta, kun tekoälyagentti julkaisi sisältöä sisäisellä foorumilla ilman käyttäjän hyväksyntää liiallisten käyttöoikeuksien vuoksi. Seurauksena arkaluontoisia tietoja paljastui luvattomille henkilöille noin kahden tunnin ajan. OpenAI:n ChatGPT:ssä havaittiin ja korjattiin haavoittuvuus, joka olisi mahdollistanut käyttäjien keskusteludatan varastamisen haitallisen kehotteen avulla. Tätä haavoittuvuutta ei tiettävästi ehditty hyödyntämään kyberhyökkäyksissä.

Geopoliittisiin riskeihin varautuminen vaatii aktiivista tilannekuvan seurantaa sekä huolellista oman verkkoympäristön suojaamista ja päivittämistä. Kuten Citrixin tapaus osoittaa, ovat hyökkääjät varsin ketteriä ja nopeita hyödyntämään tunnettuja haavoittuvuuksia. Tekoälyn yleistyessä sen käyttö ja hallinta voivat nousta elämän ja kuoleman kysymykseksi organisaatioissa. Hyötyjen keräämiseksi koulutusta tekoälyn kyberriskeistä tulisi lisästä ja rajata tekoälyjärjestelmien käyttöoikeudet tiukasti kiusallisten vuotojen välttämiseksi.

2 VALOKEILASSA

2.1 Avainhenkilöt eivät ole immuuneja venäläiselle kalastelulle

Venäläisten valtiollisten hakkereiden laaja ja koordinoitu kampanja Signal- ja WhatsApp-tilejä vastaan on poikinut varoituksia tiedustelupalveluilta Atlantin molemmin puolin. Alankomaiden asevoimien tiedustelupalvelu (MIVD) ja yleinen tiedustelupalvelu (AIVD) vahvistivat, että hollantilaiset valtion työntekijät ovat joutuneet hyökkäysten kohteeksi. Operaatio nojaa tietojenkalastelu- ja sosiaalisen manipuloinnin tekniikoihin, jotka hyödyntävät laillisia todentamisominaisuuksia viestien salaiseen seuraamiseen.

FBI on julkaissut raportin, jossa nämä kampanjat yhdistetään suoraan Venäjän tiedustelupalveluihin. Siinä varoitetaan, että hyökkäykset on suunniteltu päästä päähän -salauksen kiertämiseen tilien kaappaamisen kautta. Kampanja kohdistuu tiedustelullisesti arvokkaisiin henkilöihin, kuten nykyisiin ja entisiin valtion virkamiehiin, sotilashenkilöstöön, poliittisiin toimijoihin ja toimittajiin. Se on jo johtanut tuhansien tilien luvattomaan käyttöön maailmanlaajuisesti. Ranskankin viranomaiset ovat sittemmin yhtyneet näihin varoituksiin.

Hyökkääjät käyttävät kahta ensisijaista menetelmää. Ensimmäinen perustuu ”linkitetty laite” -ominaisuuden väärinkäyttöön. Ensin hyökkääjät tekeytyvät luotetuksi yhteyshenkilöksi ja lähettävät haitallisen linkin tai QR-koodin. Jos uhri avaa linkin, hyökkääjä voi yhdistää oman laitteensa uhrin tiliin saaden jatkuvan pääsyn ilman, että uhri kuitenkaan välittömästi menettää omaansa. Venäläiset hyödynsivät tätä menetelmää jo vuosi sitten ukrainalaisia Signal-käyttäjiä vastaan, mikä on erinomainen osoitus siitä, kuinka tärkeää on seurata Ukrainan sodan kehitystä, sillä se voi antaa organisaatioille mahdollisuuden varautua uusiin uhkiin jo ennen kuin ne realisoituvat.

Toinen menetelmä on tilin täydellinen kaappaus. Siinä uhrit saavat virallisilta tuki-ilmoituksilta vaikuttavia viestejä, jotka kehottavat jakamaan vahvistuskoodeja tai kaksivaiheisen todennuksen tunnistetietoja. Erityisen harhaanjohtava piirre kaappaustavan osalta on se, että uhrit voivat uudelleenrekisteröidä puhelinnumeronsa ja saada takaisinpääsyn paikallisesti tallennettuun chat-historiaansa, mikä saattaa johtaa heidät olettamaan, ettei mitään ole vialla. Hollantilaiset viranomaiset kuitenkin korostavat oletuksen voivan olla virheellinen. On helppo ymmärtää, kuinka tuhannet ihmiset ovat saattaneet jo langeta tämänkaltaisiin tietojenkalasteluyrityksiin, mutta samalla uhrien suuri määrä on erittäin huolestuttava etenkin ottaen huomioon kohteiden luonne – he ovat henkilöitä, joilla on pääsy turvaluokiteltuun tai muuten erittäin arvokkaaseen tietoon. Jää nähtäväksi, miten venäläiset aikovat hyödyntää erittäin onnistuneen tietojenkalastelukampanjansa saalista. Hyökkäysten uhreiksi joutuneiden organisaatioiden tulisi pysyä valppaana mahdollisten jatkotoimien varalta.

Alankomaiden sotilastiedustelupäällikkö vara-amiraali Peter Reesink korosti tapauksen pohjalta laajempaa opetusta kaikille: huolimatta päästäpäähän-salauksestaan, viestisovelluksia, kuten Signal ja WhatsApp, ei tulisi käyttää kanavina turvaluokitellulle tai arkaluontoiselle tiedolle. Tästä huolimatta palvelut itsessään ovat edelleen turvallisia. Jälleen kerran tapaus oli mahdollinen ainoastaan inhimillisen virheen vuoksi – viestejä ei tunnistettu tietojenkalasteluksi. Alankomaiden, Ranskan ja Yhdysvaltojen viranomaiset neuvovat käyttäjiä olemaan jakamatta vahvistuskoodeja, tarkistamaan säännöllisesti linkitetyt laitteet ja suhtautumaan epäilyttävästi odottamattomiin tukiviesteihin. Koska Venäjän tiedusteluoperaatiot Euroopassa ovat käyneet huomattavasti haastavammiksi vuoden 2022 jälkeen, kybervakoilun ja kaapattujen tilien merkitys tulee todennäköisesti kasvamaan entisestään tulevaisuudessa.

2.2 Yhdysvaltojen kyberturvallisuudella perusteltu reititinkielto heikentää kyberturvallisuutta

23. maaliskuuta 2026 Yhdysvaltain liittovaltion viestintäkomissio FCC lisäsi kaikki Yhdysvaltojen ulkopuolella valmistetut kuluttajakäyttöön tarkoitetut reitittimet ”katettujen laitteiden listalle” (Covered List), mikä käytännössä kieltää uusien ulkomailla valmistettujen kuluttajareitittimien tuonnin vedoten kyberturvallisuusriskeihin. Päätös seurasi Valkoisen talon koolle kutsuman virastojen välisen paneelin arviota, jonka mukaan ulkomailla valmistetut reitittimet aiheuttavat toimitusketjuhaavoittuvuuksia ja vakavia kyberturvallisuusriskejä, jotka voisivat häiritä Yhdysvaltain infrastruktuuria, mahdollistaa vakoilua ja helpottaa immateriaalioikeuksien varkautta.

Päätöstä vauhdittivat osaltaan kiinalaisiin valtiollisiin hakkereihin yhdistetyt kyberhyökkäykset. FCC viittasi erityisesti Volt, Salt ja Flax Typhoon -kampanjoihin, jotka hyödynsivät reitittimien haavoittuvuuksia kohdistaen iskuja Yhdysvaltain kriittiseen infrastruktuuriin. Kiinan arvioidaan hallitsevan noin 60 prosenttia Yhdysvaltain kotitalouksien reititinmarkkinoista, mikä tekee tästä erityisen laaja-alaisen toimenpiteen. On huomionarvoista, että kielto koskee tuotteen valmistusmaata riippumatta brändin kansallisuudesta – amerikkalaiset yritykset kuten Netgear ja Amazonin omistama Eero eivät ole poikkeuksia, koska niiden tuotteet valmistetaan ulkomailla. Lähes kaikki markkinoilla tällä hetkellä olevat reitittimet valmistetaan Yhdysvaltain ulkopuolella pääasiassa Kiinassa, Indonesiassa, Taiwanissa, Thaimaassa tai Vietnamissa, mikä tarkoittaa, että kyseessä on käytännössä lähes täydellinen kielto uusille reititinmalleille.

Päätökseen liittyy tärkeitä huomioita: kuluttajat voivat jatkaa jo ostamiensa reitittimien käyttöä, ja jälleenmyyjät voivat edelleen myydä malleja, jotka ovat jo saaneet FCC:n hyväksynnän. Valmistajat voivat myös hakea sotaministeriöltä tai kotimaan turvallisuuden ministeriöltä ”ehdollisen hyväksynnän” poikkeusta. Kriitikot ovat esittäneet huolia käytännön seurauksista. Analyytikot varoittavat, että reitittimien saatavuus voi heikentyä ja hinnat voivat nousta. Jotkut kommentaattorit ovat luonnehtineet kieltoa hallituksen puuttumiseksi kuluttajien valinnanvapauteen, kun otetaan huomioon kuinka vähän reitittimiä tosiasiassa valmistetaan kotimaassa. Kiellon pitkän aikavälin tehokkuus riippuu todennäköisesti siitä, miten ehdollisen hyväksynnän prosessi kehittyy.

Jos hyväksyntöjä myönnetään harvoin, kielto johtaa todennäköisesti siihen, että uusimmat reititinmallit loppuvat amerikkalaisilta jälleenmyyjiltä hinnannousuista huolimatta. Pitkällä aikavälillä yhdysvaltalaiset kuluttajat voisivat joutua jatkamaan vanhempien ja siten heikommin suojattujen reitittimien käyttöä – mikä on täysin ristiriidassa kiellon alkuperäisen päämäärän kanssa. On myös huomionarvoista, että koska kielto ei tee eroa maiden välillä, eurooppalaisia yrityksiä pidetään käytännössä yhtä epäluotettavina kuin kaikkia muitakin. Tämä voidaan nähdä jälleen yhtenä särönä transatlanttisissa suhteissa. Kiina tulee tämän seurauksena etsimään vaihtoehtoisia markkinoita uusille reititinmalleilleen, ja sen katse todennäköisesti kohdistuu ensimmäisenä Eurooppaan. Euroopassa käydään jo valmiiksi vilkasta keskustelua kiinalaisten laitteiden turvallisuudesta, ja EU kohtaakin pian vaikean päätöksen siitä, salliako yhä suurempi kiinalaisen teknologian tulva unionin alueelle vaiko ei.

Tässä mielessä Yhdysvaltain päätös istuu hyvin laajempaan globaaliin digitaalisen suvereniteetin trendiin. Muita esimerkkejä tästä ovat Kiinan asettama kielto länsimaisille kyberturvallisuusyrityksille sekä Venäjän siirtyminen kohti Kiinan kaltaista autoritääristä digitaalista ekosysteemiä. Molemmat perustuivat ”turvallisuushuoliin”, mutta ainakin Venäjän tapauksessa todellinen tavoite on, että hallituksella olisi vahvempi ote venäläisten kansalaisten digitaalisesta viestinnästä.

Vaikka kyberturvallisuushuolet Yhdysvaltain tapauksessa ovat varmasti perusteltuja, vaikuttaa silti todennäköiseltä, että toimitusketjuhaavoittuvuudet nähtiin huomattavasti vakavampana ongelmana kieltoa suunniteltaessa. Yhdysvallat yrittää selvästi saada aikaan kotimaista reititintuotantoa välttääkseen katastrofaaliset seuraukset tilanteessa, jossa Kiina päättäisi tulevaisuudessa lopettaa toimitukset Yhdysvaltoihin. Euroopankin tulisi todennäköisesti ottaa tällaiset riskit huomioon. Toisaalta Yhdysvaltain mallin seuraaminen kaikkien uusien reititinmallien kieltämisessä johtaisi väistämättä heikompaan kyberturvallisuuteen lyhyellä aikavälillä, joten vaihtoehtoisten ratkaisujen etsiminen on tärkeää.

3 SEURAA NÄITÄ

3.1 Clauden kyky ymmärtää vanhoja ohjelmointikieliä on turvallisuusuhka

Anthropicin lippulaivatekoäly Claude on viime aikoina ollut uutisissa pääasiassa liittyen yrityksen kannanottoon, jossa se kieltää Clauden käytön automaattisissa asejärjestelmissä. Kyberturvallisuuden näkökulmasta mallin ominaisuus, jonka tarkoituksena on helpottaa vanhan koodin päivittämistä, on kuitenkin huomattavasti kiinnostavampi. 70-luvulla kirjoitettuun koodiin perustuvia järjestelmiä on edelleen varsin paljon, ja monissa tapauksissa ne käyttävät ohjelmointikieltä, jota juuri kukaan ei enää ymmärrä. Claude pyrkii ratkaisemaan tämän ongelman tarjoamalla työkalun, joka hallitsee esimerkiksi COBOL:in kaltaisia kieliä ja voi siten auttaa ohjelmoijia päivittämään järjestelmiään modernimpiin.

Claude voi käytännössä hoitaa modernisointiprosessin työläimmän ja eniten aikaa vievän osan kartoittamalla koko järjestelmän ja sen riippuvuudet dokumentoiden samalla prosessin tavalla, joka on helpommin ymmärrettävissä moderneille ohjelmoijille. Se pystyy automaattisesti havaitsemaan ja merkitsemään haavoittuvuuksia kiinnittääkseen huomion koodin tärkeimpiin ongelmiin. Se saattaa helposti kuulostaa kyberturvallisuuden kannalta erinomaiselta uutiselta, kunnes ymmärtää, että samat ominaisuudet ovat myös kaikkien uhkatoimijoiden käytettävissä. Haavoittuvuuksien automaattinen havaitseminen ja merkitseminen ei enää olekaan yhtä hienoa, kun tarkoituksena on järjestelmän korjaamisen sijaan sitä vastaan hyökkääminen.

Tilannetta pahentaa se, että monet COBOL:in kaltaiset vanhat ohjelmointikielet ovat itse asiassa osittain nojanneet juuri tuntemattomuuteensa. Jos uhkatoimijat eivät ymmärrä järjestelmän käyttämää kieltä, heidän on huomattavasti vaikeampaa löytää siinä olevia haavoittuvuuksia hyödynnettäväksi. Tekoäly muuttaa nyt tämän perusoletuksen. Jos edelleen vanhaan koodiin nojaavat organisaatiot eivät tee asialle mitään, rikolliset ja muut pahantahtoiset toimijat varmasti käyttävät tilaisuuden hyväkseen. Tuntemattomuus ei enää tarjoa suojaa samalla tavoin kuin ennen, joten perintökoodin modernisoimisesta on tullut huomattavasti aiempaa kiireellisempi tehtävä.

Tällaisia järjestelmiä on myös Suomessa runsaasti, ja varsin usein niitä löytyy kriittisen infrastruktuurin toiminnoista. Niin kauan, kun kaikkia niistä ei ole perusteellisesti päivitetty, on hyökkääjillä merkittävä etu Clauden ansiosta. Toki on olemassa mekanismeja, jotka estävät ihmisiä käyttämästä mallia haitallisiin tarkoituksiin, mutta kuten malli itse totesi kysyttäessä uhkatoimijoiden mahdollisuuksista käyttää sitä COBOL-pohjaisia järjestelmiä vastaan hyökkäämiseen: ”Kyllä, rehellisesti sanottuna – juuri tässä skenaariossa osaamiseni voisi olla merkittävä mahdollistava tekijä.”

On hyvä muistaa, että malli ei edelleenkään toimi automaattisena hyökkäystyökaluna. Se voi ainoastaan auttaa hyökkääjää ymmärtämään tuntemattomalla kielellä kirjoitettua koodia tai analysoimaan sitä haavoittuvuuksien varalta. Monissa tapauksissa tämä voi kuitenkin olla ratkaiseva tekijä, joka mahdollistaa hyökkäyksen. Tässä yhteydessä merkittävimpiä uhkia saattavatkin olla sisäpiiririskit. Tyytymätön tai vihainen työntekijä, jolla on perustason ohjelmointiosaaminen, voisi aiheuttaa vakavia ongelmia Clauden avulla niin halutessaan. Työntekijöillä nimittäin voi olla huomattavasti helpompi pääsy koodiin, jota Claude voisi auttaa analysoimaan. Helposti saatavilla olevien ransomware-as-a-service-työkalujen määrän huomioon ottaen tällaisen henkilön tarvitsisi nähdä hyvin vähän vaivaa tehokkaan sisäisen hyökkäyksen toteuttamiseksi.

Vaikka Anthropic on markkinoinut ominaisuutta kyberturvallisuutta parantavana, se saattaa ainakin lyhyellä aikavälillä osoittautua täysin päinvastaiseksi, kun järjestelmiä ei ole vielä päivitetty. Kyynisesti asiaa voi ajatella näin: Anthropicin ei tarvitse välittää siitä, käyttävätkö Claudea järjestelmiään modernisoimaan pyrkivät organisaatiot vai niitä vastaan hyökkäävät uhkatoimijat, sillä he ansaitsevat rahaa joka tapauksessa. Kuten kaiken muunkin kohdalla, tekoäly vaikuttaa kiihdyttävän kehityksen tahtia nopeasti myös tällä alalla. Valitettavasti on todennäköisesti vain ajan kysymys, ennen kuin näemme uutisia Clauden osallisuudesta hyökkäyksessä COBOL-pohjaiseen järjestelmään, joka ei olisi ollut mahdollinen ennen tätä.

3.2 Tekoälytilien kysyntä pimeän verkon markkinapaikoilla lisää kyberrikollisten kiinnostusta tunnusten varastamiseen

Tutkijat julkaisivat äskettäin havaintoja, joiden mukaan tekoälytilien käyttäjätunnuksista on tulossa yhä halutumpi hyödyke sekä myyjille että ostajille pimeän verkon markkinapaikoilla. Viime vuonna kyberrikolliset myivät noin 400 varastettua generatiivisen tekoälyn tilin käyttäjätunnusta päivässä venäjänkielisillä pimeän verkon markkinapaikoilla, ja monet näistä tunnuksista oli kerätty infostealer-haittaohjelmilla saastuneista yrityskäyttäjien koneista. Eräässä tapauksessa jopa yli 100 000 ChatGPT-tilin käyttäjätunnusta listattiin myyntiin useilla pimeän verkon alustoilla.

Luvut ovat sen jälkeen ainoastaan kasvaneet, samoin kuin tuotevalikoima. Varastettujen tilien lisäksi myyntiin on ilmaantunut tarkoituksenmukaisesti rakennettuja haitallisia tekoälytyökaluja. WormGPT:n ja FraudGPT:n kaltaisia työkaluja markkinoidaan maanalaisten foorumien ja Telegram-kanavien kautta. Ne tarjoavat ominaisuuksia, kuten haitallisen koodin kirjoittaminen, haavoittuvuuksien tunnistaminen ja tietojenkalastelusivujen luominen – kaikki ilman valtavirta-alustojen eettisiä rajoituksia. Hinnoittelu vaihtelee suuresti. Premium-pääsy tekoälyalustoille kuten ChatGPT:hen voi maksaa noin 8–500 euroa käyttörajoista riippuen, ja automatisoidut palvelut voivat tuottaa jopa 1 000 väärennettyä tiliä päivässä varastettuja henkilötietoja käyttäen.

Epävirallisen pääsyn kysyntään tekoälytileille on useita syitä. Yksi merkittävimmistä on pakotteiden kiertäminen. Esimerkiksi Venäjällä, Iranissa ja Pohjois-Koreassa pääsy joihinkin suosituimpiin tekoälytyökaluihin on rajoitettu paikallisten maksuvaihtoehtojen estämisellä. Pimeän verkon markkinapaikat mahdollistavat näin ollen rajoitusten kiertämisen VPN-yhteyksien ja kryptovaluuttojen avulla. Niitä voidaan käyttää myös palvelun todellisen käyttäjän salaamiseen. Monet tarjouksista lupaavat täyden pääsyn tekoälyn rajapintaan (API) mahdollistaen käyttäjille kyberrikollisuuden kaltaisen haitallisen toiminnan estävien rajoitteiden ohittamisen. Koska kyseiset tilit ovat yleensä varastettuja, kaikki kustannukset laskutetaan uhrille, ei käyttäjälle.

Seuraukset ovat vakavia monilla eri tavoilla. Vaarantuneet käyttäjätunnukset voivat antaa hyökkääjille pääsyn yrityksen tekoäly-ympäristöihin paljastaen mahdollisesti asiakkaiden henkilö- ja taloustietoja, omistusoikeudellista aineetonta omaisuutta ja muita arkaluontoisia tietoja. Pahimmassa tapauksessa pääsy yrityksen tekoälytilille voisi jopa mahdollistaa laajemman tunkeutumisen organisaation järjestelmiin. Jos tekoälyn asetuksia ei ole turvallisesti konfiguroitu, hyökkääjä voisi käyttää työkalua haittaohjelmien asentamiseen tai käyttöoikeuksien laajentamiseen. Koska yhä useammat ovat valmiita maksamaan tileistä, niiden varastamisen kannattavuus on kasvanut, mikä puolestaan houkuttelee yhä suurempaa joukkoa rikollisia.

Näiltä uhkilta puolustautuminen vaatii monikerroksista lähestymistapaa. Työntekijöiden tekoälykäytön seuranta, salausavaimiin tai monivaiheiseen tunnistautumiseen perustuvan todentamisen käyttöönotto tekoälyalustoille sekä pimeän verkon seurantapalveluiden hyödyntäminen varastettujen käyttäjätunnusten varhaiseksi havaitsemiseksi ovat kaikki tärkeitä askelia, joilla voidaan estää uhkatoimijoita käyttämästä yrityksen omia tekoälytilejä sitä itseään vastaan. Ydinviesti on selvä: mitä keskeisempi rooli tekoälyllä on liiketoiminnassa, sitä tärkeämpää on näiden alustojen käytön turvaaminen – se on kriittinen osa jokaisen organisaation kyberturvallisuutta.

LÄHTEET:

Tapahtumia kybermaisemassa

https://thehackernews.com/2026/03/openai-patches-chatgpt-data.html

https://techcrunch.com/2026/03/18/meta-is-having-trouble-with-rogue-ai-agents/

https://www.theguardian.com/technology/2026/mar/20/meta-ai-agents-instruction-causes-large-sensitive-data-leak-to-employees

https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300

https://www.cybersecuritydive.com/news/citrix-netscaler-exploitation-vulnerabilities/816097/

https://therecord.media/cisa-tells-federal-agencies-to-patch-citrix-netscaler-bug

https://yle.fi/a/74-20218659

https://www.mtvuutiset.fi/artikkeli/wsj-iraniin-kytkeytynyt-ryhma-teki-historian-merkittavimman-sota-ajan-kyberiskun/9311120

https://www.reuters.com/world/china/eu-sanctions-chinese-iranian-companies-cyber-attacks-2026-03-16/

https://www.reuters.com/world/europe/russia-backed-hackers-breach-signal-whatsapp-accounts-officials-journalists-2026-03-09/

Avainhenkilöt eivät ole immuuneja venäläiselle kalastelulle

https://www.bleepingcomputer.com/news/security/dutch-govt-warns-of-signal-whatsapp-account-hijacking-attacks/__

https://therecord.media/russian-hackers-target-signal-whatsapp-warn-dutch-intelligence-agencies__

https://therecord.media/russia-iran-cyber-fbi-hacks__

https://www.bleepingcomputer.com/news/security/fbi-links-signal-phishing-attacks-to-russian-intelligence-services/__

https://www.cert.ssi.gouv.fr/uploads/20260320_NP_C4_Alerte_Ciblage_messagerie_instantanee.pdf

https://www.politico.eu/article/russian-hackers-snoop-ukrainian-signal-accounts-google-report/

Yhdysvaltojen kyberturvallisuudella perusteltu reititinkielto heikentää kyberturvallisuutta

https://reason.com/2026/03/25/fcc-bans-nearly-all-wireless-routers-sold-in-the-u-s/

https://www.aarp.org/personal-technology/fcc-foreign-router-ban-explainer/

https://www.fcc.gov/document/fcc-updates-covered-list-include-foreign-made-consumer-routers

https://www.reuters.com/sustainability/boards-policy-regulation/fcc-banning-imports-new-chinese-made-routers-citing-security-concerns-2026-03-23/

Clauden kyky ymmärtää vanhoja ohjelmointikieliä on turvallisuusuhka

https://claude.com/blog/how-ai-helps-break-cost-barrier-cobol-modernization

https://www.linkedin.com/feed/update/urn:li:activity:7436235669938614272/?originTrackingId=1epJL9ZY7DcKI2LBHV6BNQ%3D%3D

Claude Sonnet 4.6

Tekoälytilien kysyntä pimeän verkon markkinapaikoilla lisää kyberrikollisten kiinnostusta tunnusten varastamiseen

https://www.bleepingcomputer.com/news/security/paid-ai-accounts-are-now-a-hot-underground-commodity/

https://outpost24.com/blog/dark-ai-tools/

https://www.csoonline.com/article/3479476/hottest-selling-product-on-the-darknet-hacked-genai-accounts.html

https://www.group-ib.com/media-center/press-releases/stealers-chatgpt-credentials/

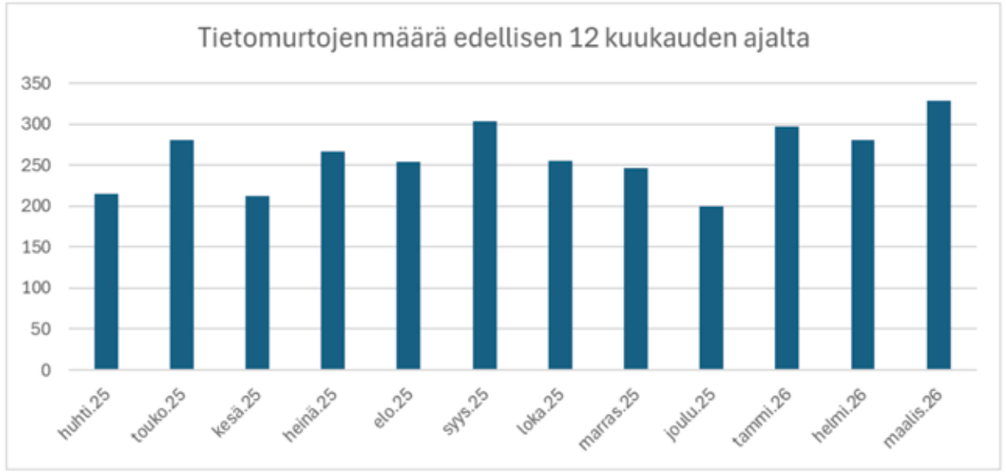
Cyberwatch KUUKAUSIKATSAUS

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)

EU-KOMISSION TIETOMURTO

AJANKOHTA: 24.03.2026
KUVAUS: EU-komissio ilmoitti kohdanneensa kyberhyökkäyksen, joka kohdistui komission Amazon Web Services (AWS) käyttäjätileihin. Kyseessä on jo toinen EU-komission kokema kyberhyökkäys kuukauden sisään. Edellisen kerran helmi-maaliskuun vaihteessa sen mobiililaitteiden hallinta-alustaan kohdistui kyberhyökkäys.
TEKIJÄ: ShinyHunters. Komissio itse ei ole vahvistanut hyökkääjää.
MOTIIVI: Ei tiedossa
VAIKUTUKSET: Komissio tutkii edelleen tapausta, mutta iskun tekijäksi ilmoittautunut ShinyHunters kyberrikollisryhmä on kertonut saaneensa haltuunsa 350 gigatavun edestä dataa komission AWS-tietokannasta. Hyökkääjät väittävät tietojen sisältävän ainakin työntekijädataa, mutta vuotaneena voi olla myös muita tietoja.

PUERTO DE VIGON SATAMAN LUNNASHAITTAOHJELMAHYÖKKÄYS

AJANKOHTA: 24.03.2026
KUVAUS: Espanjan Atlantin rannalla sijaitseva satama Puerto de Vigo koki lunnashaittaohjelma-hyökkäyksen. Satama on ajoneuvojen, ajoneuvologistiikan, kalan ja metallin tärkeä käsittelypiste. Satamasta kulkee rahtia etenkin Kiinaan sekä Etelä- ja Pohjois-Amerikkaan.
TEKIJÄ: Ei tiedossa
MOTIIVI: Taloudellinen
VAIKUTUKSET: Lunnashaittaohjelmahyökkäys pysäytti osan sataman digitaalisista järjestelmistä. Muun muassa logistiikanhallintajärjestelmät olivat käyttämättömissä ja satama siirtyi tämän takia osittain paperiin ja kynään pitäen näin sataman toiminnassa. Hyökkäys alleviivaa jälleen kriittiseen infrastruktuurin globaalisti kohdistuvia kyberuhkia.

PUERTO RICON LIIKENNEVIRASTON KYBERHYÖKKÄYS

AJANKOHTA: Maaliskuu 2026
KUVAUS: Puerto Ricon liikennevirasto kyberhyökkäyksen kohteena. Puerto Ricon hallinnon virastot toimielimineen ovat olleet jatkuvien kyberhyökkäysten kohteena etenkin kuluneen vuoden aikana.
TEKIJÄ: Ei tiedossa
MOTIIVI: Ei tiedossa
VAIKUTUKSET: Liikennevirasto joutui sulkemaan osan viraston toiminnoista kyberhyökkäyksen takia. Muun muassa ajokortti-, lupa- ja ajoneuvorekisteripalvelut jouduttiin pitämään alhaalla hyökkäyksen kohdistuttua niiden tietojärjestelmiin. Myös kaikki näiden palveluiden fyysiset palveluajat peruttiin ja uusien aikojen varaaminen keskeytettiin.

FBI:N JOHTAJAN SÄHKÖPOSTIIN MURTAUDUTTIIN

AJANKOHTA: 27.03.2026
KUVAUS: Yhdysvaltojen keskusrikospoliisin FBI:n pääjohtajan, Kash Patelin henkilökohtaiseen sähköpostiin murtauduttiin ja sen sisältöä jaettiin iranilaisen hakkeriryhmän verkkosivuilla.
TEKIJÄ: Handala. Kyseessä on iranilainen hakkeriryhmä, joka on viime aikoina kunnostautunut kyberhyökkäysten tekijänä Iranin sodan kontekstissa. Patelin sähköpostin hakkeroimisen lisäksi ryhmä oli muun muassa sairaalalaitevalmistaja Strykerin tietomurron takana.
MOTIIVI: Poliittinen
VAIKUTUKSET: FBI:n pääjohtaja Kash Patelin henkilökohtaiselta gmail-tililtä julkaistiin muun muassa kuvia, dokumentteja ja keskusteluita iranilaisen Handala-hakkeriryhmän verkkosivuille. Handala ilmoitti hyökkäyksen syyksi muun muassa FBI:n operaatiot Handalaa vastaan sekä Iranin sota-aluksen upottamisen Intian valtamerellä. Hyökkäyksellään Handala pyrki nolaamaan FBI:n julkisesti ja kirjoittikin verkkosivuillaan "FBI:n olevan pelkkä nimi, jonka takana ei ole lainkaan todellista turvallisuutta" ja "Mitä FBI:n alemman tason työntekijöiltä voidaan vaatia, jos heidän pääjohtajansakin on näin alttiina murroille".

Merkittäviä sekä nousevia uhkatoimijoita

BEARLYFY

KUVAUS: Bearlyfy on ukrainamielinen hakkeriryhmä, joka on kohdistanut hyökkäyksiään etenkin venäläisiin yrityksiin.
VIIME AIKOJEN TOIMINTA: Vuonna 2025 ensimmäisiä kertoja havaittu haktivisti-/kyberrikollisryhmä Bearlyfy on tehnyt jo reilut 70 kyberhyökkäystä venäläisiä organisaatioita kohtaan. Uhreiksi on päätynyt muun muassa konsultti- ja teollisuusyrityksiä. Bearlyfy ei itse pidä ääntä toiminnastaan, eikä esimerkiksi ylläpidä haittaohjelmatoimijoille tyypillistä uhrien "häpeälistaa".
TOIMINTATAVAT JA TAKTIIKAT: Bearlyfy on ideologisesti motivoitunut hakkeriryhmä, joka haluaa tehdä maksimaalista vahinkoa venäläisille organisaatioille. Tämän haitanteon lisäksi ryhmällä on kuitenkin motiivinaan myös kerätä mahdollisimman paljon rahaa hyökkäyksillään muun muassa kehittääkseen omaa toimintaansa. Kehityskaarta onkin jo nähty, sillä alkuun ryhmä tunnettiin hyvin nopeasti kasaan kyhätyistä hyökkäystyökaluistaan. Ryhmä osti käytännössä valmiita työkaluja kyberrikollisilta markkina-alustoilta ja hyödynsi lisäksi samanmielisten haktivistiryhmien tukea hyökkäyksissään. Viime aikoina ryhmän työkalujen ja menetelmien on havaittu kehittyneen ja alkuaikojen kotikutoinen toiminta on karissut kauas taakse. Ryhmän uhreista jopa joka viides on maksanut ryhmälle vaaditut lunnaat. Alun pienemmät lunnasvaatimukset ovat nousseet jo satoihin tuhansiin euroihin. Bearlyfy on hyökkäyksissään hyödyntänyt usein uhriorganisaatioiden alihankkijoille luotuja käyttäjätilejä. Näiden haltuun saatujen käyttäjätunnusten avulla Bearlyfy toimittaa uhrin järjestelmään tietoja kryptaavan haittaohjelman. Kryptauksen jälkeen se uhkaa tuhota tietoja pyyhkivällä haittaohjelmalla koko uhrin tietojärjestelmän, mikäli lunnaita ei makseta.

HANDALA

KUVAUS: Handala on iranilainen haktivistiryhmä, jonka useat eri lähteet ovat yhdistäneet Iranin tiedustelu- ja turvallisuusministeriöön (Ministry of Intelligence and Security, MOIS).
VIIME AIKOJEN TOIMINTA: Handala on iskenyt viime aikoina muun muassa FBI:n johtajan henkilökohtaiseen sähköpostitiliin sekä Yhdysvaltalaislähtöiseen globaaliin terveydenhuoltoalan yritykseen Strykeriin tuhoten Strykerin tietojärjestelmiä ympäri maailman.
TOIMINTATAVAT JA TAKTIIKAT: Handala hyödyntää hyökkäyksissään usein toimitusketjujen haavoittuvuuksia. Se kohdistaa huomionsa hyökkäyksen alkuvaiheessa uhrin IT-palveluntarjoajaan saadakseen haltuunsa käyttöoikeuksia uhrin järjestelmiin. Handala käyttää hyökkäyksissään usein omaa tietoja tuhoavaa haittaohjelmaansa "Handala Wiperia" tai tietoja kryptaavia ohjelmia. Ryhmä pyrkii kohteista riippuen usein joko tuhoamaan kohdejärjestelmiä tai varastamaan ja julkaisemaan niistä kriittistä tietoa.

AKIRA

KUVAUS: Maaliskuussa 2023 ensimmäisen kerran tavattu kyberrikollisryhmä. Toimii lunnashaittaohjelmapalvelu-periaatteella (Ransomware as a Service, RaaS).
VIIME AIKOJEN TOIMINTA: Maaliskuun 2026 aikana Akira on yhdistetty noin 140 kyberhyökkäykseen globaalisti. Sen uhreiksi on joutunut viimeisimpänä muun muassa teknologiayhtiöitä, lakifirmoja, työnvälitysalustoja sekä ruoan tuotannon yhtiöitä. Akira on ollut pitkään yksi tunnetuimmista ja aktiivisimmista kyberrikollisryhmistä.
TOIMINTATAVAT JA TAKTIIKAT: 80 % Akiran uhreista on pieniä tai keskisuuria yrityksiä pääosin Pohjois-Amerikasta tai Euroopasta. Akira käyttää toiminnassaan niin sanottua kaksoiskiristystä; varastaa uhrin dataa, kryptaa sen ja uhkaa julkaista datan, mikäli lunnaita ei makseta.

ANUBIS RANSOMWARE

KUVAUS: Vuoden 2024 lopulla ensimmäisiä kertoja havaittu venäjänkielinen lunnashaittaohjelmia palveluna tarjoava ryhmä (RaaS).
VIIME AIKOJEN TOIMINTA: Anubis on aktivoitunut maaliskuun aikana merkittävästi. Cyber Intelligence Housen datan mukaan Anubiksella oli maaliskuun aikana 24 vahvistettua uhria, kun joulukuun aikana 2025 niitä oli vain kolme ja tammi- sekä helmikuun 2026 aikana ei lainkaan. Viimeisimpien uhrien joukossa ovat muun muassa ranskalainen IT-yritys ja yhdysvaltalainen asianajotoimisto.
TOIMINTATAVAT JA TAKTIIKAT: Anubis tarjoaa lunnashaittaohjelmatyökaluja affiliaatio-sopimuksilla muille kyberrikollisille kolmella eri mallilla. Haittaohjelmaa se tarjoaa käyttöön yhteistyökumppaneilleen ottamalla tuotoista 20 % itselleen. Tietojen varastamiseen käytettävien työkalujen tarjoamisesta ryhmä pidättää itselleen 40 % tuotoista. Yhteistyöoperaatioissa, joissa Anubis tarjoaa mm. apua uhrin järjestelmiin sisälle pääsyyn, se pidättää 50 % operaatioiden tuotoista. Etenkin tässä viimeisessä menetelmässä Anubis on säätänyt uhreja koskevia sääntöjä kuten että uhrin on oltava Pohjois-Amerikassa, Euroopassa tai Australiassa ja uhri ei saa olla koulutuksen, hallinnon tai voittoa tavoittelemattoman sektorin edustaja.

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.

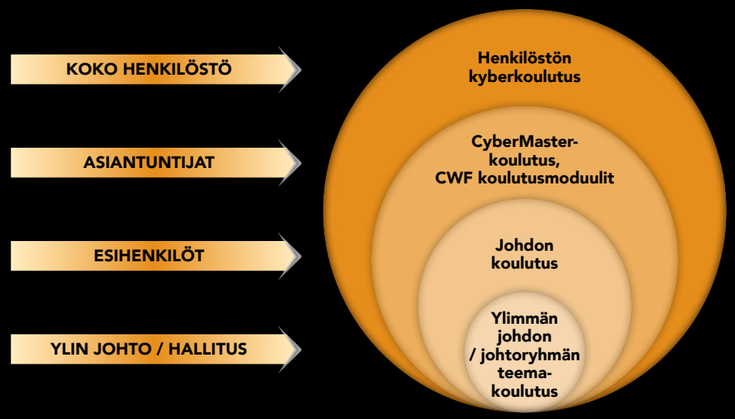
Analyysi voidaan tehdä valituille toimitusketjun organisaatioille (edellyttäen sopimusta). Havainnot jalkautetaan toimitusketjun organisaatioille, jotka vastaavat korjaavien toimenpiteiden suorittamisesta sekä raportoi tilaajalle, kun korjaavat toimenpiteet on tehty.

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

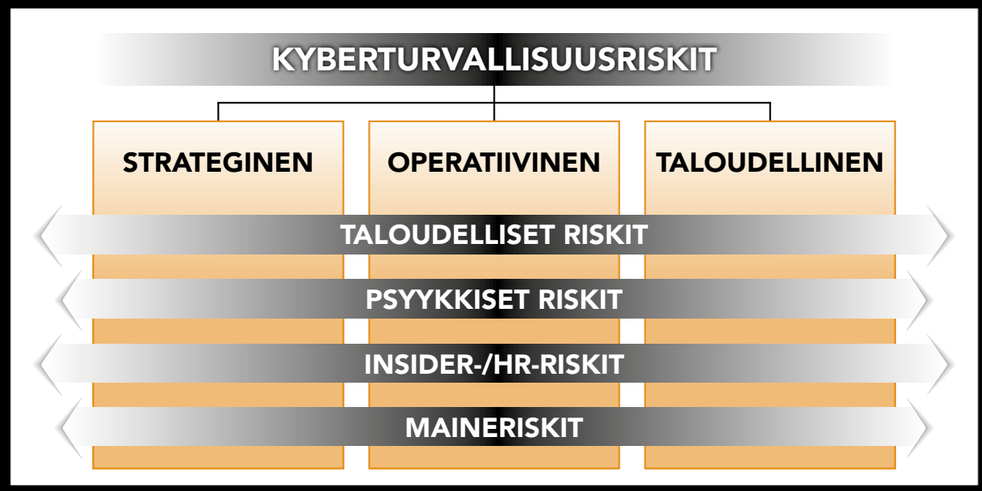
Kyberturvallisuus tulee yhä enemmän ottaa huomioon ennakoiden liiketoimintasuunnitelman eri vaiheissa. Kokonaisvaltaisessa kyber-turvallisuuden riskienhallintasuunnitelmassa laaditaan selkeä tiekartta siitä, miten kyberturvallisuusuhkat huomioidaan entistä paremmin ja miten lisääntyvä EU-regulaatio sekä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