Toimintamalli ja toimenpidesuositukset kuntien digi- ja kyberturvallisuuden testaukseen ja kehittämiseen

Tiivistelmä

Kiristyneen kansainvälisen turvallisuustilanteen myötä kuntien tulee varautua yhä vakavampiin kyberuhkiin toiminnoissaan. Tietoturvatestaus mahdollistaa erilaisten puutteiden, heikkouksien ja haavoittuvuuksien tunnistamisen ja korjaamisen kuntien tietojärjestelmistä, toimintatavoista ja elintärkeistä yhteiskunnallisista toiminnoista. Tässä dokumentissa esitetään Kuntien digi- ja kyberturvallisuuden testaus- ja kehittämismenettely -hankkeessa muodostetut toimintamalli ja toimenpidesuositukset kuntien digi- ja kyberturvallisuuden testaukseen ja kehittämiseen. Toimintamalli sekä sen käyttöä tukevat toimenpidesuositukset tarjoavat tietoa ja menetelmätukea jatkuvan tietoturvatestauksen organisointiin osana kuntien tietoturvallisuuden hallintaa. Hankkeessa osallistujakunnissa suoritettiin monipuolista käytännön tietoturvatestausta, jota ohjaavaksi ajankohtaiseksi uhkaskenaarioksi tunnistettiin valtiollinen geopoliittinen aggressio. Uhkaskenaariosta johdetuiksi hyökkäysskenaarioiksi asetettiin: 1) kohdistetut tietojenkalasteluhyökkäykset, 2) web-sovellushyökkäykset, 3) sisäverkon hyökkäykset, 4) toimitiloihin tunkeutuminen, ja 5) kriittisen infrastruktuurin kyberhyökkäykset. Toimenpidesuositukset muodostettiin tukemaan kuntien testaustoimenpiteitä erityisesti em. hyökkäysskenaariohin varautumisen tason testaamisessa. Toimenpidesuositukset sisältävät mm. hyökkäyskuvauksen, hyökkäysvektorit, testausmenetelmät, mittarit, hyödyt, sekä yleiset kehitystoimenpiteet. Lisäksi niissä käsitellään hankkeen käytännön kokemuksia sekä testauksissa huomioitavia asioita, teknologioita ja materiaaleja. Toimintamalli ja toimenpidesuositukset muodostettiin kirjallisuuden ja hankkeessa kertyneiden kokemusten perusteella hankkeen päätteeksi. Toimintamallin käyttöönotosta sekä soveltamisesta jatkuvana prosessina tarvitaankin lisätietoa ja käytännön kokemuksia kuntakentältä.

Sisällysluettelo

Tausta

Hanke toteutettiin ajanjaksolla 1.3.2022 - 31.1.2024. Hankkeen lähestymistapa kuntien digi- ja kyberturvallisuuden testaukseen ja kehittämiseen oli skenaariomainen, eli testaustoimenpiteille muodostettiin toimintaa ohjaava uhkaskenaario, jonka tavoitteena oli motivoida, johdonmukaistaa ja tarinallistaa testausta ajankohtaisten teemojen kautta. Tietoturvatestaukseen tuotiin siis elementtejä ns. Red Teaming -tyyppisistä tunkeutumisharjoituksista. Skenaarioiden ja testaustoimenpiteiden suunnittelua tukemaan kehitettiin Skenaariovetoisen penetraatiotestauksen mallinnusmenetelmä.

Hankkeen alkumetreillä Euroopan turvallisuustilanne muuttui merkittävästi. Ohjausryhmä valitsikin hankkeen toimintaa ohjaavaksi uhkaskenaarioksi valtiollisen geopoliittisen aggression, mistä johdettiin viisi hyökkäysskenaariota: 1) kohdistettu tietojenkalasteluhyökkäys, 2) web-sovellushyökkäys, 3) sisäverkon hyökkäys, 4) toimitiloihin tunkeutuminen ja 5) kriittisen infrastruktuurin kyberhyökkäys. Hyökkäysskenaarioiden tavoitteena oli kattaa käytännön toimenpiteiden tasolla tyypilliset tilanteet sekä kybermaailmassa että rakennetussa ympäristössä, joissa vihamielinen valtiollinen toimija voisi yrittää tunkeutua kunnan kriittisiin tietojärjestelmiin, tietovarantoihin ja yhteiskunnan elintärkeisiin toimintoihin.

Hankkeessa tietoturvatestaustoimenpiteitä tehtiin seitsemässä kunnassa; Akaan kaupunki, Alavuden kaupunki, Eurajoen kunta, Kankaanpään kaupunki, Lapuan kaupunki, Loimaan kaupunki ja Seinäjoen kaupunki. Hankkeen hallinnoinnista vastasi Kankaanpään kaupunki ja hankkeen projektipäällikkönä toimi Ari Peltoniemi. Yhteistyökumppaneina hankkeessa olivat Suomen Kuntaliitto ja Kyberturvallisuuskeskus. Hanke rahoitettiin pääosin Valtiovarainministeriön hallinnoimasta Kuntien digitalisaation kannustinjärjestelmästä. Hankkeessa laadittiin toimintamalli ja toimenpidesuositukset kuntien digi- ja kyberturvallisuuden testaukseen ja kehittämiseen, jotka esitetään tässä dokumentissa. Dokumenttia hallinnoi Kankaanpään kaupunki ja se on tarkoitettu kuntien vapaasti hyödynnettäväksi.

Toimintamalli

Tässä osiossa esitetään toimintamalli kuntien digi- ja kyberturvallisuuden testaukseen ja kehittämiseen.

Esittely

Toimintamallin tarkoituksena on tarjota kunnille tietoa ja menetelmätukea jatkuvan tietoturvatestauksen organisointiin osana kuntien tietoturvallisuuden hallintaa. Toimintamallin käyttöönotto auttaa kuntia tunnistamaan tietoturvaan liittyviä heikkouksia tietopohjaisesti sekä korjaamaan niitä ennen kuin kyberhyökkäyksiä pääsee tapahtumaan. Tunnistamattomat ja siten hallitsemattomiksi jäävät haavoittuvuudet sekä tietojärjestelmien ja käytänteiden puutteet muodostavat kunnille huomattavia riskejä, jotka voivat realisoituessaan jopa lamauttaa niiden yhteiskunnallisesti elintärkeät toiminnot. Tietoturvatestaus tukeekin paitsi kunnan riskienhallintaa myös pitkän aikavälin turvallisuuden ja vakauden ylläpitämistä sekä jatkuvuutta kriittisessä infrastruktuurissa ja kansalaisten palveluissa.

Toimintaympäristö

Kansainvälisen turvallisuustilanteen kiristyessä vakavien kyberhyökkäysten uhka kasvaa myös kuntien toimintaympäristössä. Kuntienkin tulisi valmistautua kasvaviin kyberuhkiin proaktiivisesti mm. tietoturvatestausta jalkauttaen. Siitä on hyötyä myös arvioitaessa EU:n säädöspohjan (kuten NIS2-direktiivin) kansallisen toimeenpanon määrittelemien vaatimusten merkitystä kunnille - velvoitteitten osalta. Kuntien tulisikin panostaa tietoturvatestaukseen, koska se auttaa suojaamaan arkaluonteisia tietoja, turvaamaan kriittisten julkisten palveluiden saatavuuden, rakentamaan luottamusta kansalaisten ja sidosryhmien keskuudessa, varmistamaan lainsäädännön ja standardien noudattamisen, tuottamaan kustannussäästöjä välttämällä tietoturvahyökkäysten seuraukset sekä kasvattamaan kyberturvallisuustietoisuutta ja -osaamista kunnissa.

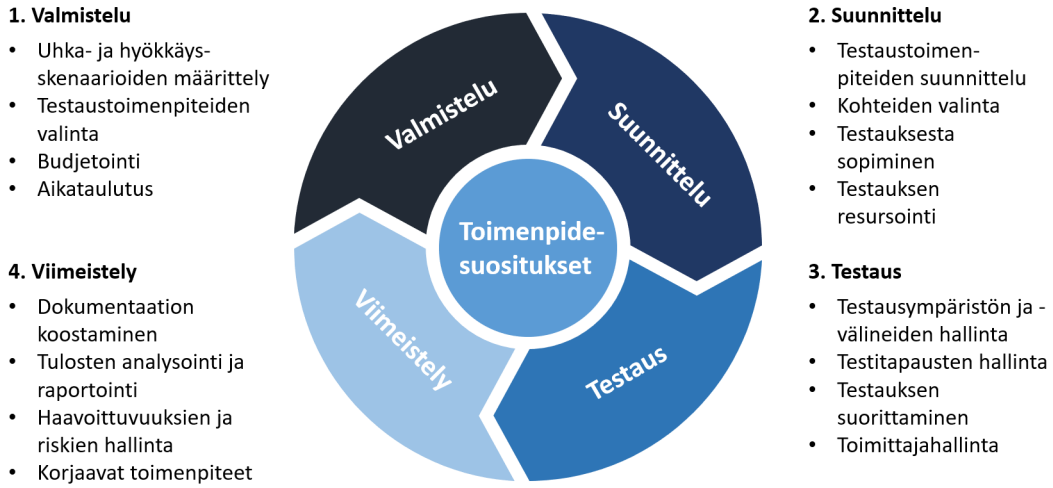
Kohderyhmä

Toimintamalli on kehitetty kunnan tietohallinnon ja erityisesti tietoturvasta vastaavien henkilöiden käyttöön. Ainakaan pienemmissä kunnissa tietoturvallisuuden hallintaan ei tavallisesti ole osoitettu kokoaikaista henkilöä ja mm. siksi niissä tehdään tietoturvatestaustakin usein vain satunnaisesti. Toimintamalli pyrkii ketterän ohjelmistokehityksen periaatteisiin pohjautuvana viitekehyksenä olemaan kevyt ja helposti hallittavissa oleva kokonaisuus. Sen on myös tarkoitus integroitua osaksi kunnan tietoturvallisuuden hallintaa. Varsinaisen testaustyön suorittaminen voi vaatia syvällistäkin teknistä perehtymistä ja/tai ulkoista näkökulmaa testauksen tulosten laadun ja realistisuuden varmistamiseksi. Tämän vuoksi osa toimintamallin vaiheiden tehtävistä on tapauskohtaisesti ulkoistettavissa tietoturvatestauspalveluita tuottaville asiantuntijaorganisaatioille.

Prosessin kuvaus

Toimintamalli on esitetty Kuviossa 1 jatkuvana nelivaiheisena prosessina, jota ohjaavat tässä dokumentissa jäljempänä esitetyt Toimenpidesuositukset kuntien digi- ja kyberturvallisuu-

den testaukseen ja kehittämiseen. Toimintamallin vaiheet ovat 1) *valmistelu*, 2) *suunnittelu*, 3) *testaus* ja 4) *viimeistely*, jotka kuvataan alla. Vaiheiden ydintehtävät on listattu Kuviossa 1. Prosessista voi olla samanaikaisesti käynnissä useita eri vaiheissa eteneviä ilmentymiä. Toimintamalli on muodostettu tilannekohtaisen menetelmäkehityksen periaatteita ja hankkeen käytännön kokemuksia soveltaen. Toimintamallin ns. metamalliin voi tutustua tästä. Esimerkin tietojenkalastelusimulaation organisoinnista voi nähdä täällä.



Kuvio 1: Toimintamalli kuntien digi- ja kyberturvallisuuden testaukseen ja kehittämiseen

Valmistelu Valmisteluvaiheessa tulevan tarkasteluajanjakson tietoturvatestaustoimenpiteet määritetään esim. osana kunnan vuosisuunnittelua. Skenaariosuunnittelussa tunnistetaan aluksi yksi tai useampi uhkaskenaario, joka kuvaa ajankohtaista yleistä kyberuhkaa, jota kunta pyrkii minimoimaan. Tämän jälkeen määritetään hyökkäysskenaarioita, joiden kautta tunnistettu kyberuhka voisi käytännön tasolla kohdistua kuntaan. Seuraavaksi valitaan soveltuvimmat tietoturvatestauksen toimenpiteet, joilla hyökkäysskenaarioihin varautumisen tilaa voidaan testata. Valituille testaustoimenpiteille arvioidaan kustannus ja ne viedään budjetointiprosessiin. Investointeja testaustoimenpiteisiin voidaan perustella esim. vertaamalla testaustoimenpiteiden kustannuksia tunnistetun kyberuhkan realisoitumisen potentiaalisiin vaihtoehtokustannuksiin ja muihin negatiivisiin vaikutuksiin. Lopuksi toimenpiteet aikataulutetaan esim. kunnan tietoturvallisuuden hallinnan vuosikelloon. Vaiheen lopputuloksena on dokumentaatio siitä, mitä testauskokonaisuuksia tarkasteluajanjaksolla tehdään, milloin ne tehdään, mikä on niiden budjetti ja miksi ne tehdään.

Suunnittelu Suunnitteluvaiheessa testauskokonaisuuksien toimenpiteet määritetään tarkemmalla tasolla, valittavien testauskohteiden erityispiirteet huomioiden. Toimenpiteiden ja kohteiden yksityiskohtaisempi määrittely kannattaa tehdä kullekin hyökkäysskenaariolle hieman ennen aikataulutettua testausajankohtaa, jotta esim. mahdollisiin turvallisuustilanteen muutoksiin pystytään reagoimaan ajoissa. Suunnittelussa tulee selvittää myös mahdolliset ulkoiset ja sisäiset vaatimukset, jotka pitäisi huomioida testauksessa.

Arvioidaan myös voidaanko testaus suorittaa tuotantoympäristössä vai vaaditaanko esivalmisteluja, jotta testauksesta ei koituisi mahdollisia haittoja esim. tietojärjestelmien toimintaan. Testaukselle määritetään vastuuhenkilö, arvioidaan tarvittava työmäärä ja muut kustannukset sekä valitaan suoritusajankohta. Jos testauksessa hyödynnetään ulkopuolisia asiantuntijoita, toimenpiteisiin voi kuulua myös esim. toimittajien kanssa viestintä sekä testauksen kilpailuttaminen ja tilaaminen. Suunnitteluvaiheeseen kuuluu myös testauksen suorittamisesta tiedottaminen ja käytännöistä sopiminen esim. johdon ja muiden mahdollisten tahojen, kuten tietohallinnon ja henkilöstöhallinnon kanssa. Jos henkilöstö on testauksessa osallisena, tiedottaminen kannattaa kohdistaa huolellisesti rajattuun joukkoon, jotta testauksen tulokset eivät pääse vääristymään tiedon leviämisen myötä. Vaiheen lopputuloksena on dokumentaatio siitä, miten testaus tehdään, mihin kohteisiin testausta tehdään, mitkä ovat testauksen vaatimukset, keitä testauksesta on tiedotettu, mikä taho on testauksesta vastuussa, mikä taho käytännön testaustyön suorittaa sekä mitkä ovat testauksen kustannukset.

Testaus Testausvaiheessa suoritetaan varsinainen tietoturvatestaustyö sekä siihen liittyvät toimenpiteet. Testauksen jalkauttamisessa hyödynnetään edellisen vaiheen suunnitelmia. Aluksi varmistetaan ovatko suunnitelmat ajan tasalla ja tehdään mahdolliset tarvittavat viime hetken muutokset. Jos testausta hoitaa ulkopuolinen asiantuntija, pidetään tavallisesti aloituspalaveri, jossa lyödään lukkoon testauksen käytännön järjestelyt. Testauksen suoritusympäristö valmistellaan testausta varten. Testauksessa käytettävät välineet, menetelmät ja testitapaukset saatetaan käyttövalmiiksi. Testauksen suorittaminen tapahtuu sovittuna ajankohtana. Mahdollisen ulkopuolisen asiantuntijan kanssa käydään tarpeen mukaan viestintää testauksen etenemisen yksityiskohdista. Vaiheen lopputuloksena on dokumentaatio siitä, miten testaus käytännössä suoritettiin ja mitkä ovat testauksen tulokset.

Viimeistely Viimeistelyvaiheessa tietoturvatestauksessa kerätty tieto dokumentoidaan, analysoidaan ja jalostetaan haavoittuvuuksiksi, riskeiksi ja edelleen niitä minimoimaan pyrkiviksi toimenpiteiksi. Tekniseen dokumentaatioon kerätään testauksen lähtökohdat, tavoitteet, menetelmät, kohteet, tulokset, opit ja kehitysehdotukset. Testauksen tuloksista raportoidaan tilannekohtaisesti esim. tietohallintopäällikölle ja johdolle. Ulkoistetun testauksen tapauksessa materiaalin koostamisen analysoinnin ja raportoinnin hoitaa tavallisesti ulkopuolinen asiantuntija. Tuloksista ja kehitystoimenpiteistä voidaan tiedottaa myös henkilöstöä. Testauksesta nousevia haavoittuvuuksia tulisi hallita kuntien tietoturvallisuuden hallinnan toimenpiteiden tasolla. Siihen kuuluu tunnistettujen haavoittuvuuksien käsittely ja tarvittavien toimenpiteiden toteuttaminen dokumentoidusti koskien kaikkia niitä järjestelmiä ja käytänteitä joita ko. haavoittuvuus koskee. Haavoittuvuuksia ja niihin kohdistuvien uhkien realisoitumisen todennäköisyyksiä ja vaikutuksia voidaan tarkastella myös kunnan riskien käsittelyn ja hallinnan toimenpiteiden tasolla. Korjaavat toimenpiteet jalkautetaan hallitusti löydösten vakavuuden mukaisella aikataululla. Vaiheen lopputuloksena on valmis dokumentaatio suoritetusta testauksesta, sen tuloksista, löydetyistä haavoittuvuuksista, niiden vakavuudesta sekä suunnitelluista ja suoritetuista korjaustoimenpiteistä. Vaiheen lopuksi testauksesta kertyneet opit viedään prosessin seuraavaan sykliin ja prosessia kehitetään tarpeen mukaan.

Käyttöönotto

Toimintamalli on koostettu kirjallisuuden ja hankkeen kokemusten perusteella, eikä sitä ole vielä koeponnistettu jatkuvana prosessina kunnissa. Toimintamallin yksittäiset osat on kuitenkin suoritettu osana hankkeen testaustoimenpiteitä. Kokemuksia ja tuloksia hankkeen testauksista on dokumentoitu karkealla tasolla osaksi toimenpidesuosituksia. Toimintamallin käyttöönottoa kannattaakin lähteä valmistelemaan tutustumalla tähän dokumenttiin sekä etsimällä tarpeen mukaan lisää tietoa. Toimintamallin käyttöönotosta ja esim. sen kustannuksista, kattavuudesta ja soveltuvuudesta erilaisiin käyttötapauksiin tarvitaankin lisää käytännön kokemusta kuntakentältä.

Toimenpidesuositukset

Tässä osiossa esitetään toimenpidesuositukset kuntien digi- ja kyberturvallisuuden testaukseen ja kehittämiseen. Ensimmäisenä esitetään toimenpidesuositusten rakenne ja sisältöjen kuvaukset ja sen jälkeen viisi toimenpidesuositusta sisältöineen.

Toimenpidesuositusten rakenne ja sisältöjen kuvaukset

Suositus	Suosituksen tunniste ja nimi
Hyökkäys-kuvaus	Kuvaus siitä, minkälaisen hyökkäyksen varalta testausta tehdään.
Hyökkäys-vektorit	Hyökkäyksen kohteen ominaisuudet, joiden heikkouksia hyökkääjä pyrkii hyväksikäyttämään tunkeutuakseen kohteeseen.
Testaus	Testausmenetelmän kuvaus.
Mittarit	Testauksessa selvitettävät varautumisen tason tunnusluvut
Hyödyt	Testauksesta saatavat hyödyt.
Hyökkäys-skenaario	Hyökkääjän toimintaa kuvaava skenaario, jota hankkeen testaustoimenpiteillä pyrittiin simuloimaan.
Kokemukset hankkeesta	Kuvaus hankkeessa suoritetuista testaustoimenpiteistä ja sen löydöksistä karkealla tasolla.
Huomioitavat asiat	Hankkeessa kertyneet kokemukset siitä, mitä testauksessa kannattaa ottaa erityisesti huomioon.
Teknologiat	Mitä teknologioita hankkeen testauksissa käytettiin.
Materiaalit	Keskeiset hankkeen testauksissa tuotetut materiaalit.
Kehitys-toimenpiteitä	Yleisiä varautumis- ja korjaustoimenpiteitä hyökkäykseen liittyen.
Lisätiedot	Testausta ohjaavat ja ohjeistavat lähteet.

Toimenpidesuositus 1: Kohdistetut tietojenkalasteluhyökkäykset

Suositus	S-1 Testaa kohdistettuihin tietojenkalasteluhyökkäysiin varautumisen taso
Hyökkäys-kuvaus	Tietojenkalastelu on yleisin kyberhyökkäystyyppi. Se kohdistuu käyttäjien valmiuksiin tunnistaa huijausviestejä ja väärennettyjä verkkosivustoja. Tavallisesti hyökkäysten tavoitteena on saada käyttäjät luovuttamaan arkaluonteisia tietoja tai asentamaan haittaohjelmia tietämättään. Kohdistetussa tietojenkalastelussa huijaus on räätälöity tietylle kohderyhmälle, mikä kasvattaa hyökkäyksen läpimenon todennäköisyyttä. Noin 40 % kaikista kyberhyökkäyksistä hyödyntää tietojenkalastelua alkuvaiheessaan (IBM, 2022). Tietojenkalastelun motiivina on tavallisesti oikeudettoman taloudellisen hyödyn tavoittelu; esim. pankkitunnusten anastaminen tai kiristyshaittaohjelman levittäminen.
Hyökkäys-vektorit	Henkilöstön valmiudet, sähköpostijärjestelmien ominaisuudet
Testaus	Testaukseen käytetään tietojenkalastelusimulaatiota, jossa organisaatio itse tai ulkopuolinen palveluntarjoaja lähettää henkilöstölle suunniteltuja, haitattomia tietojenkalasteluviestejä ja kerää tilastotietoa henkilöstön reaktioista niihin. Jos organisaatio hoitaa simulaation itse, otetaan käyttöön ohjelmistoratkaisu tietojenkalastelukampanjoiden hallintaan tai se hankitaan palveluna. Tietojenkalastelusimulaatioille on hankittava myös johdon hyväksyntä ennen testauksen aloittamista. Tietojenkalastelukampanjan suunnittelussa määritetään testauksen tavoitteet, kohderyhmät, käytettävät viestit sekä mahdolliset liitteet tai kalastelusivustot. Kampanjat suunnitellaan niin, että ne jäljittelevät aitoja tietojenkalastelukampanjoita, mutta eivät aiheuta todellista vahinkoa vastaanottajille. Ennen kampanjan käynnistämistä viestien lähettämistä ja valvontaa tulee testata kattavasti, jotta voidaan varmistua siitä, että kaikki toimii suunnitellusti. Kampanjan jälkeen tulokset analysoidaan ja tuloksista raportoidaan ryhmätasolla johdolle ja henkilöstölle. Lopuksi reagoidaan mahdollisiin kehitystarpeisiin.
Mittarit	Hyökkäyksen läpimenoprosentti (kalasteluviesti, kalastelusivusto)
Hyödyt	Tietojenkalastelusimulaatiot lisäävät henkilöstön tietoisuutta ja käytännön valmiuksia tunnistaa tietojenkalasteluhyökkäyksiä, mikä vähentää merkittävästi organisaation tietoturvariskejä. Säännöllisesti pidettyinä ne kehittävät jatkuvaa turvallisuuskulttuuria organisaatiossa ja tarjoavat arvokasta tietoa turvallisuuskoulutuksen tehostamiseen. Simulaatiot auttavat myös noudattamaan tietoturvaan liittyviä lainsäädäntöjä ja standardeja, osoittaen proaktiivista lähestymistapaa tietoturvan hallintaan.

Suositus	S-1 Testaa kohdistettuihin tietojenkalasteluhyökkäysiin varautumisen taso
Hyökkäys-skenaario	Hyökkääjä yrittää kalastella kunnan henkilöstön pankkitunnuksia, joiden avulla se voisi esim. vaihtaa salasanan kunnan järjestelmien käyttäjätunnuksiin, siirtää rahaa sekä saada pääsyn arkaluonteisiin henkilötietoihin.
Kokemukset hankkeesta	Hankkeessa testaukset päätettiin hoitaa omatoimisesti avoimen lähdekoodin Gophish-ohjelmistoratkaisulla. Projektipäällikkö valmisteli Gophish-palvelimen, kalasteluviestit ja kalastelusivuston käyttöön sekä ohjasi kuntia testauksessa. Noin vuoden välein suoritettujen tietojenkalastelusimulaatioiden tulokset olivat linjassa globaalien tietojenkalasteluhyökkäysten keskimääräisten läpimenoprosenttien kanssa (IBM, 2022). Keskimäärin n. 18 % prosenttia kuntien henkilöstöstä klikkasi linkkiä kohdennetussa tietojenkalasteluviestissä ja n. 11 % klikkasi linkkiä pankkitunnusten anastamiseen tarkoitetulla kalastelusivustolla. Hankkeessa kalasteluviestinä käytettiin viranomaisviestejä ja kalastelusivustona muokattua kopiota Suomi.fi -tunnistautumissivusta. Kalastelusivuston linkkien klikkaajille suositeltiin ohjelmallisesti DVV:n Digiturvallinen elämä koulutusta. Tuloksista tiedotettiin sekä johdolle että henkilöstölle ja kaikille suositeltiin em. koulutusta. Henkilöstöltä kerätty palaute simulaatioista oli yleisesti ottaen hyvin positiivista ja niille toivottiin jatkoa. Katso myös mallinnus käytetystä testausmenetelmästä.
Huomioitavat asiat	Organisaation johdon ja tietohallinnon tulee olla tietoinen testauksesta etukäteen. Testauksessa tulee myös huomioida tietojasuojaregulaatio, koska simulaatiossa käsitellään henkilötietoja. Tuloksia kannattaa käsitellä ryhmätasolla. Simulaatiosta kannattaa tiedottaa etukäteen vain hyvin rajattua joukkoa, jotta tulosten realistisuus varmistetaan. Niin ikään sähköpostijärjestelmissä ja/tai sähköpostiliikenteen valvontajärjestelmissä on erilaisia toimittaja- ja organisaatiokohtaisia mekanismeja viestien skannaukseen ja luokitteluun, jotka pitää ottaa huomioon tilannekohtaisesti, konfiguroida niihin tarvittavat poikkeukset ja testata kokonaisuus kattavasti, jotta kalasteluviestit saavuttavat kohderyhmän esteittä ja kalastelun valvontaa häiritsemättä.
Teknologiat	Gophish, yleisimmät sähköpostijärjestelmät
Materiaalit	Tietojenkalastelusimulaation tekninen ratkaisu, kalastelusivusto, kalasteluviestit, suoritusohjeet, esittely johdolle, tiedote henkilöstölle, kysely henkilöstölle ja sen tulokset, sähköpostijärjestelmien konfiguraatiot, Iptables-palomuurisäännöt, tulosraportti

Suositus	S-1 Testaa kohdistettuihin tietojenkalasteluhyökkäysiin varautumisen taso
Kehitys-toimenpiteitä	Säännölliset tietojenkalastelusimulaatiot, tietoturvakoulutukset, turvallisuuskulttuurin edistäminen, tietoturvapolitiikat ja -ohjeistukset, johdon ja henkilöstön sitoutuminen, tekniset suojauskeinot
Lisätiedot	Julkri HAL-13, IBM X-Force Threat Intelligence Index 2022

Toimenpidesuositus 2: Web-sovellushyökkäykset

Suositus	S-2 Testaa web-sovellushyökkäyksiin varautumisen taso
Hyökkäys-kuvaus	Web-sovellushyökkäykset kohdistuvat verkkopohjaisiin palveluihin, kuten nettisivustoihin, hyödyntäen niiden turvallisuuspuutteita, kuten suunnittelu- ja toteutusvirheitä, vanhentuneita komponentteja tai palvelinympäristön haavoittuvuuksia. Hyökkääjät skannaavat globaalissa mittakaavassa jatkuvasti julkisten tietoverkkojen osoiteavaruuksia erilaisten hyökkäyskohteiden paikantamiseksi. Hyökkäyksiä voidaan myös kohdentaa suunnitellusti tiettyyn palveluun tai organisaatioon, esim. niiden toiminnan häiritsemiseksi tai maineen vahingoittamiseksi. Hyökkäysten tavoitteena on tyypillisesti oikeudettoman pääsyn saaminen arkaluonteisiin tietoihin, haittaohjelmien levittäminen tai sovelluksen toiminnan manipulointi, esim. taloudellisten tai poliittisten intressien edistämiseen.
Hyökkäys-vektorit	Web-sovellusten haavoittuvuudet, palvelinympäristöjen haavoittuvuudet ja virheelliset konfiguraatiot
Testaus	Web-sovellusten tunkeutumistestausta voidaan suorittaa esim. käyttämällä yleisesti saatavilla olevia haavoittuvuusskannereita tai hankkimalla räätälöity testaus palveluna. Testausta käytetään tunnistamaan sovellusten turvallisuusheikkoudet, kuten käyttäjäsyötteiden käsittelyn virheet, istunnon hallinnan puutteet, autentikointi- ja valtuutusongelmat sekä kryptografiset heikkoudet. Testaus voi sisältää myös erilaisten hyökkäysmenetelmien, kuten Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) ja palvelunestohyökkäysten (DoS, DDoS) simuloinnin, sekä rajapintojen turvallisuuden tarkastelun. Testaustyökaluja on saatavilla myös tietyille alustoille ja ohjelmistoille räätälöityinä. Testauksen tavoitteena on arvioida web-sovellusten kykyä suojautua luvattomalta pääsyltä ja toiminnalta, tunnistaa ja dokumentoida turvallisuuspuutteet sekä tarjota tietoa haavoittuvuuksien korjaamista varten.
Mittarit	Löydettyjen haavoittuvuuksien määrä ja vakavuus (korkea, keskitaso, matala)

Suositus	S-2 Testaa web-sovellushyökkäyksiin varautumisen taso
Hyödyt	Web-sovellusten tunkeutumistestaus tarjoaa monipuolisia hyötyjä organisaation tietoturvan parantamiseksi, sillä haavoittuvuuksien tunnistaminen edistää niiden korjaamista, tietoturvariskien vähentämistä, brändin maineen suojaamista, vaatimustenmukaisuusvelvoitteiden täyttämistä, kustannussäästöjä, asiakastietojen suojaamista ja turvallisuuskulttuurin kehittämistä. Se auttaa organisaatioita ehkäisemään tietoturvaloukkauksia proaktiivisesti sekä vahvistamaan asiakkaiden ja sidosryhmien luottamusta, tarjoten samalla pitkän aikavälin säästöjä välttämällä tietoturvaloukkausten aiheuttamia kustannuksia ja mahdollistaa jatkuvan tietoturvan parantamisen uusia uhkia vastaan.
Hyökkäys-skenaario	Hyökkääjä yrittää löytää kunnan julkisista verkkopalveluista haavoittuvuuksia, joista pääsisi tunkeutumaan niihin sisään, tavoitteena saada haltuunsa esim. käyttäjätunnuksia, tietoja tai pääsyn sisäverkkoon.
Kokemukset hankkeesta	Hankkeessa suoritettiin tunkeutumistestausta Wordpressille, joka on yleisesti käytössä kuntien verkkosivustojen julkaisujärjestelmänä. Käytössä olivat vapaasti saatavilla olevat ja avoimen lähdekoodin testaustyökalut. Projektipäällikkö suunnitteli ja ohjasi testausprosessia, joka alkoi kuntien ulkoverkon hyökkäyspinta-alan kartoituksella DNS Dumpster -palvelussa ja jatkui Wordpress-instanssien kevyellä skannauksella Wordpress Security Scan -palvelussa. Tämän jälkeen suoritettiin syvällinen haavoittuvuusskannaus WPScan-työkalulla, joka mahdollistaa mm. käyttäjätunnusten ja heikkojen salasanojen selvittämisen sekä tietoturvakonfiguraation puutteiden tunnistamisen. Testauksessa löydettiin pääasiassa ylläpidettyjä ja ajan tasalla olevia Wordpress-instansseja, joista löydetyt haavoittuvuudet olivat lähinnä nollapäivähaavoittuvuuksia, jotka tultiin korjaamaan seuraavissa päivityksissä. Joissakin kunnissa osallistuttiin myös Kyberturvallisuuskeskuksen tarjoamaan Kansalliseen Hyökkäyspintakartoitukseen Hyökyyn, jossa kuntien ulkoverkon palveluista tunnistetaan tunnettuja heikkouksia ja haavoittuvuuksia.
Huomioitavat asiat	Testauksesta on tärkeää sopia testattavasta palvelusta vastaavan tahon kanssa ja varmistaa, että testauksen eri työvaiheiden/toimenpiteiden osalta noudatetaan olemassa olevaa lainsäädäntöä. Jotkin tunkeutumistestausmenetelmät voivat tehdä oikeaa tuhoakin tuotantosovelluksissa ja niiden datavarannoissa, joten testausta on hyvä koeponnistaa testiympäristössä.
Teknologiat	DNS Dumpster, Wordpress Security Scan, WPScan, Kali Linux, JetPack Protect, Wordpress Vulnerabilities, Hyöky
Materiaalit	Wordpress-testausohjeet, tulosraportti

Suositus	S-2 Testaa web-sovellushyökkäyksiin varautumisen taso
Kehitys-toimenpiteitä	Säännölliset web-sovellusten ja palvelinympäristöjen päivitykset ja kovennukset, web-sovelluspalomuurien (WAF) käyttö, tunkeutumistestaukset, hyvät turvallisuuskäytännöt, tietohallinnon tietoturvakoulutukset
Lisätiedot	Julkri TEK-19, OWASP Top 10

Toimenpidesuositus 3: Sisäverkon hyökkäykset

Suositus	S-3 Testaa sisäverkon hyökkäyksiin varautumisen taso
Hyökkäys-kuvaus	Sisäverkon hyökkäykset ovat organisaation sisäisessä verkossa tapahtuvia kyberhyökkäyksiä, joiden lähteinä voivat olla sekä sisäiset uhkatekijät että ulkoa tunkeutuneet hyökkääjät. Näitä hyökkäyksiä leimaa pääsy arkaluonteisiin tietoihin ja kriittisiin järjestelmiin, ja ne sisältävät esim. sisäverkon konfiguraatioiden heikkouksien ja palveluiden haavoittuvuuksien hyväksikäyttämisen, haittaohjelmien levittämisen, pääsy- ja käyttövaltuuksien hallinnan puutteiden hyväksikäyttämisen, tietojen varastamisen ja manipuloinnin, käyttäjätunnusten kaappauksen, verkkoliikenteen kuuntelun ja palvelunestohyökkäykset. Sisäverkon hyökkäykset ovat erityisen haastavia tunnistaa ja torjua, sillä ne tapahtuvat organisaation sisäisen infrastruktuurin suojissa, eivätkä ne välttämättä erotu helposti normaalista sisäverkon käytöstä. Ne vaativat siksi kattavia toimia niin sisäverkon suojaukseen ja valvontaan kuin turvallisuuskulttuuriinkin liittyen.
Hyökkäys-vektorit	Tietojenkalastelu (käyttäjätunnusten vuotaminen, haittaohjelman leviäminen), sisäverkon konfiguraatioiden heikkoudet, sisäverkon palveluiden haavoittuvuudet, pääsynhallinnan puutteet, käyttövaltuuksien hallinnan puutteet
Testaus	Sisäverkon tunkeutumistestausta suoritetaan käyttämällä erilaisia menetelmiä, kuten sisäverkon kartoittamista ja tiedonkeruuta, sisäverkon palveluiden haavoittuvuusskannausta, salasanojen murtamis- ja sanakirjatestausta, langattomien verkkojen turvallisuuden testausta, sovellustason haavoittuvuuksien testausta ja verkkolaitteiden konfiguraatioiden tarkastelua. Sisäverkon tunkeutumistestaus keskittyy organisaation sisäverkon mahdollisten heikkouksien tunnistamiseen.
Mittarit	Löydettyjen haavoittuvuuksien määrä ja vakavuus (korkea, keskitaso, matala)
Hyödyt	Sisäverkon tunkeutumistestaus tarjoaa organisaatioille monia etuja, kuten kyvyn tunnistaa ja mahdollisuuden korjata verkon haavoittuvuuksia ennen vakavien tietoturvaloukkausten tapahtumista. Testauksen tulosten hyödyntäminen edistää riskienhallintaa, tietoturvakäytäntöjä, paljastaa sisäisiä uhkia, vahvistaa sidosryhmien luottamusta, edistää jatkuvan parannuksen kulttuuria kyberturvallisuudessa ja tukea liiketoiminnan jatkuvuutta. Nämä edut tekevät penetraatiotestauksesta arvokkaan työkalun, joka auttaa organisaatioita välttämään tietoturvauhkat ja ylläpitämään turvallista ja luotettavaa toimintaympäristöä.

Suositus	S-3 Testaa sisäverkon hyökkäyksiin varautumisen taso
Hyökkäys-skenaario	Hyökkääjä on päässyt onnistuneen tietojenkalastelun myötä kunnan sisäverkkoon ja etsi sieltä potentiaalisia kohteita hyökkäyksen jatko-osuudelle.
Kokemukset hankkeesta	Hankkeessa sisäverkon tunkeutumistestaus päätettiin tehdä omin voimin, projektipäällikön suunnittelemana ja ohjaamana. Testausalustaksi valittiin Kali Linux -virtuaalikone, joka on tietoturvatestaajien yleisimmät työkalut sisältämä Linux-jakelu VMBox-ympäristöön. Virtuaalikoneeseen asennettiin GVM (OpenVAS), joka on erittäin monipuolinen haavoittuvuuksien skannaukseen ja hallintaan tarkoitettu avoimen lähdekoodin ohjelmisto. Virtuaalikone ladattiin kuntien saataville ja sen käyttö ohjeistettiin. Testauksessa sisäverkon laitteiden ja palveluiden haavoittuvuuksia kartoitettiin Nmap ja GVM -skannereiden avulla. Testaukseen sisältyi myös vapaaehtoinen osuus, jossa tunkeutumisen havaitsemisjärjestelmä Security Onion asennettiin läpikäymään sisäverkon liikennettä. Nmapia käytettiin sisäverkon laitteiden kartoittamiseen ja löydetyille laitteille tehtiin GVM:ssä perusteellinen haavoittuvuusskannaus. Löydetyt haavoittuvuudet analysoitiin ja niiden viemistä haavoittuvuuksien hallintatyökaluun harjoiteltiin. Tyypillisimmät havaitut korkean tason haavoittuvuudet liittyivät elinkaarensa päässä oleviin palvelinohjelmistoihin, kuten Linux-jakeluihin, joilla ohjataan erilaisia verkkoon liitettyjä oheislaitteita. Joissakin kunnissa osallistuttiin myös Kyberturvallisuuskeskuksen tarjoamaan Havaro-käyttöpilottiin, jossa keskityttiin valtiollisten edistyneiden hyökkäysten havainnointiin verkkoliikenteestä.
Huomioitavat asiat	Sisäverkon testauksesta on aina sovittava ainakin organisaation tietohallinnon kanssa. Perusteellinen haavoittuvuusskannaus saattaa hidastaa kohdelaitteita jonkin verran, eli on suositeltavaa ajastaa skannaukset työajan ulkopuolella ajattaviksi. Myös virtuaalikonetta ajava tietokone tulee olla kohtuullisen tehokas, sillä GVM on melko raskas ajettava. GVM:n haavoittuvuustunnisteiden päivitykseen saattaa kulua tunteja, joten sen käyttöönottoon kannattaa varata aikaa. Ainakin jotkut HP:n verkkotulostimet tulkitsevat perusteelliset skannaukset tulostustöiksi, jolloin ne saattavat alkaa tulostaa erilaisia merkkijonoja suuria määriä, eli ne kannattaa tilanteen mukaan jättää skannausten ulkopuolelle.
Materiaalit	Sisäverkon testausohjeet, virtuaalikone testaukseen
Teknologiat	Kali Linux, VirtualBox, Nmap, GVM (OpenVAS), PCF, DefectDojo SecurityOnion
Kehitys-toimenpiteitä	Sisäverkon segmentointi, laitteiden ja palveluiden koventaminen, säännölliset järjestelmäpäivitykset, MFA-käyttäjätodentaminen

Suositus	S-3 Testaa sisäverkon hyökkäyksiin varautumisen taso
Lisätiedot	Julkri TEK-19

Toimenpidesuositus 4: Toimitiloihin tunkeutuminen

Suositus	S-4 Testaa toimitiloihin tunkeutumiseen varautumisen taso
Hyökkäyskuvaus	Toimitiloihin tunkeutumisessa hyökkääjä pyrkii hyväksikäyttämään fyysisen turvallisuuden heikkouksia tavoitteidensa saavuttamiseen. Hyökkääjä pyrkii hyödyntämään erilaisten fyysisten kontrollien puutteita ja/tai sosiaalisia manipulointimenetelmiä. Se kohdistuu lukitusten ja kulunvalvonnan lisäksi myös toimitilojen ICT-infran pääsynhallintamekanismeihin sekä organisaation prosesseihin, toimintatapoihin ja henkilöstön valmiuksiin. Toimitiloihin pääsyn jälkeen hyökkääjä voi esim. anastaa salaiseksi luokiteltuja asiakirjoja, saada pääsyn tietokoneille tai liittää salaa vihamielisen laitteen organisaation verkkoon. Hyökkäyksen motivaationa voi olla esim. tietojen anastaminen, vakoilu tai sabotaasi.
Hyökkäysvektorit	Fyysiset kontrollit, ICT-infran pääsynhallinta, henkilöstön valmiudet
Testaus	Testaukseen käytetään fyysistä tunkeutumisharjoitusta, jossa voidaan hyödyntää monipuolisia menetelmiä kohteen turvallisuusmekanismien testaamiseksi ja mahdollisten heikkouksien tunnistamiseksi. Testaajat voivat hyödyntää sosiaalista manipulointia esittämällä esimerkiksi huoltomiehiä tai tarkastajia päästäkseen huomaamatta kohdealueelle. Fyysinen murtautuminen taas sisältää turvatoimien, kuten lukkojen ja kulunvalvontajärjestelmien ohittamisen. Myös tietotekninen tunkeutumistestaus voi olla osa prosessia, jos testaajat pyrkivät saamaan pääsyn sisäisiin verkkoihin tai järjestelmiin. Testaukseen valmistautumisen aikana kerätään tietoa kohteesta ja luodaan suunnitelma tunkeutumiselle, kun taas seurannan ja havainnoinnin avulla tunnistetaan parhaat lähestymistavat. Lisäksi erilaisia laitteita saatetaan käyttää salaa asennettuina keräämään tietoa tai luomaan etäyhteyksiä. Tämän monipuolisen lähestymistavan avulla pyritään arvioimaan kohteen fyysistä turvallisuutta mahdollisimman realistisesti, tunnistamaan turvallisuuden heikkoudet ja tarjoamaan parannusehdotuksia.
Mittarit	Löydettyjen haavoittuvuuksien määrä ja vakavuus (korkea, keskitaso, matala)

Suositus	S-4 Testaa toimitiloihin tunkeutumiseen varautumisen taso
Hyödyt	Fyysisen tunkeutumistestauksen hyödyt liittyvät organisaation fyysisen turvallisuuden kokonaisvaltaiseen parantamiseen. Se paljastaa turvallisuusheikkoudet, arvioi turvallisuusprotokollien ja -käytäntöjen toteutusta, lisää henkilökunnan turvallisuustietoisuutta ja kouluttaa heitä, parantaa riskienhallintaa, vahvistaa sidosryhmien luottamusta sekä organisaation mainetta, varmistaa regulaatioiden ja vaatimustenmukaisuuden sekä arvioi aiempien turvallisuusinvestointien tehokkuutta. Tämä tekee fyysisestä tunkeutumistestauksesta olennaisen osan organisaation turvallisuusstrategiaa, tarjoten arvokasta tietoa henkilöstön, omaisuuden ja tietojen suojelemiseksi.
Hyökkäys-skenaario	Hyökkääjä yrittää tunkeutua kunnan toimitiloihin ja saada siellä käyttöönsä esim. verkkoyhteyksiä ja arkaluonteisia tietoja.
Kokemukset hankkeesta	Hankkeessa konsulttien suorittamien tunkeutumisharjoitusten valmisteluissa käytettiin kahta erilaista lähestymistapaa 1) testaajille annettiin minimimäärä tietoa toimitiloista etukäteen ja 2) testaajat informoitiin toimitiloista etukäteen. Näistä ensimmäinen on työläämpi ja kalliimpi, mutta antaa realistisemmat tulokset. Toinen vaatii vähemmän tiedustelutyötä ja on edullisempi, mutta tulokset eivät välttämättä vastaa täysin reaalimaailman tunkeutumista. Testauksissa toimitiloihin päästiin usein kulunvalvonnasta huolimatta esim. henkilöstön kanssa samalla ovenavauksella. Erilaisia peitetarinoita käyttäen pääsy järjestyi joissakin toimitiloissa myös eteenpäin muille osastoilla. Lisäksi tietosuojaroskakorien sijoittelussa ja lukituksissa havaittiin puutteita. Myös etäyhteydet mahdollistava laite saatiin eräässä tapauksessa yhdistettyä verkkoon ja piilotettua henkilöstön näköpiiristä. Testauksissa havaitut vakavimmat puutteet liittyvät toimintatapoihin tuntemattomien henkilöiden kanssa, kulunvalvonnan puutteisiin sekä sisäverkkojen suojaukseen.
Huomioitavat asiat	Testauksesta on tärkeää sopia johdon kanssa etukäteen ja varmistaa, että testauksen eri työvaiheiden/toimenpiteiden osalta noudatetaan olemassa olevaa lainsäädäntöä. Testauksesta kannattaa tiedottaa etukäteen vain hyvin rajattua joukkoa ja testaus kannattaa hankkia ulkoisena asiantuntijapalveluna, jotta tulosten laatu ja objektiivisuus varmistetaan.
Materiaalit	Esittely johdolle, tulosraportti, fyysisen turvallisuuden testaus kunnissa -raportti
Teknologiat	Tiirikka, kamera, piilotettavat laitteet, keyloggerit, skannausohjelmistot
Kehitys-toimenpiteitä	Säännölliset tunkeutumisharjoitukset, turvallisuusstrategian kehittäminen, johdon tuki, prosessien vahvistaminen, rakenteelliset esteet, kulunvalvonnan parantaminen ja verkon segmentointi.

Suositus	S-4 Testaa toimitiloihin tunkeutumiseen varautumisen taso
Lisätiedot	Julkri 3.2 Fyysinen turvallisuus

Toimenpidesuositus 5: Kriittisen infrastruktuurin kyberhyökkäykset

Suositus	S-5 Testaa kriittisen infrastruktuurin kyberhyökkäyksiin varautumisen taso
Hyökkäys-kuvaus	Kriittisen infrastruktuurin kyberuhkat kohdistuvat yhteiskunnan elintärkeisiin toimintoihin sekä keskeisiin/kriittisiin toimialoihin, kuten energia- ja vesihuoltoon, terveydenhuoltoon sekä liikenne- ja viestintäjärjestelmiin. Niissä voidaan hyödyntää mm. suosituksissa S-1-4 kuvattuja hyökkäyksiä sekä muita hyökkäyksiä, kuten etävalvontajärjestelmiin tunkeutumista ja droonivakoilua. Hyökkääjäprofiilit vaihtelevat valtiollisista toimijoista ja terroristeista hakkeriryhmiin ja sisäisiin uhkiin, joilla on erilaisia motivaatioita, kuten poliittisen tai taloudellisen vahingon aiheuttaminen, aktivismi tai strategisen etulyöntiaseman tavoittelu. Nämä hyökkäykset pyrkivät häiritsemään, vahingoittamaan tai saamaan luvattoman pääsyn kriittisiin järjestelmiin, mikä voi aiheuttaa merkittäviä häiriöitä, taloudellisia tappioita ja jopa ihmishenkien menetyksiä.
Hyökkäys-vektorit	Suosituksissa S-1-4 kuvatut hyökkäysvektorit, haavoittuvuudet etävalvontajärjestelmissä, alueellisissa tietoverkoissa ja SCADA-järjestelmissä, ilmatilan ja maaston rakenteet
Testaus	Kriittiseen infrastruktuuriin kuten erilaisiin tuotantolaitoksiin ja niiden ohjaus- ja automaatiojärjestelmiin tunkeutumista voidaan testata teknisesti ja fyysisesti esim. suosituksissa S-1-4 kuvatun mukaisesti. Erityisen tärkeää on kuitenkin varmistaa etukäteen, ettei testaus tuota häiriöitä tuotantoon. Kattava ja tuotantojärjestelmiin kajoamaton tapa arvioida kriittisen infran kyberhyökkäyksiin varautumisen tasoa on esim. Kyberturvallisuuskeskuksen julkaisema Kybermittari-arviointityökalu. Kybermittari pohjautuu Yhdysvaltojen energiaviraston tuottamaan C2W2-malliin. Kybermittari-arviointeja suoritetaan usein työpajoissa käymällä läpi organisaation tai sen toiminnon kyberturvallisuuden hallinnan arviointikriteerejä asiantuntijoiden kesken. Kybermittarilla voidaan tunnistaa kyberturvallisuuden hallinnan kypsyystason vahvuuksia ja heikkouksia, ja sen sisältö soveltuu erityisen hyvin kriittisiin toimintoihin. Kybermittari-arvioinnin tulokset tarjoavat kattavan kuvan siitä, missä määrin organisaatio on valmistautunut kohtaamaan kyberuhkia ja kuinka tehokkaasti se voi puolustautua potentiaalisia hyökkäyksiä vastaan.
Mittarit	Suosituksissa S-1-4 kuvatut mittarit, Kybermittarin kypsyystasot (tunnistaminen, suojautuminen, havainnointi, reagointi, palautuminen)

Suositus	S-5 Testaa kriittisen infrastruktuurin kyberhyökkäyksiin varautumisen taso
Hyödyt	Teknisen ja fyysisen testausten osalta suosituksissa S-1-4 kuvatut hyödyt. Kybermittari-arvioinnin suorittaminen kriittiselle infrastruktuurille tuottaa merkityksellistä tietoa organisaation tai sen toiminnon johdolle sekä auttaa edistämään elintärkeiden palveluiden toiminnan jatkuvuutta, yhteiskunnallista luottamusta, riskienhallinnan priorisointia, vaatimustenmukaisuuden varmistamista sekä resilienssiä ja toipumiskyvyn parantamista kyberuhkien edessä. Se auttaa myös kehittämään organisaation turvallisuuskulttuuria sekä mahdollistaa strategisen suunnittelun ja päätöksenteon kyberturvallisuuden parantamiseksi. Se tarjoaa perustan jatkuvalle parannusprosessille, jolla varmistetaan, että kriittinen infrastruktuuri pysyy suojattuna ja ajan tasalla suhteessa jatkuvasti kehittyviin kyberuhkiin ja -hyökkäysmenetelmiin.
Hyökkäys-skenaario	Hyökkääjä yrittää tunkeutua kunnan vesihuollon toimintoihin monelta hyökkäyspinnalta pysäyttääkseen kunnan vedenjakelun.
Kokemukset hankkeesta	Hankkeen aikana puhkesi kansainvälisiä konflikteja ja esim. Suojelupoliiisi tiedotti useasti kohonneesta kyberuhkatilanteesta kotimaankin kriittisen infrastruktuurin toiminnoissa. Tilanteessa hankkeessa tehtäväksi testaustoimenpiteeksi valittiin kriittisen toiminnon kyberturvallisuuden hallinnan kokonaisarviointi, jolla ei ole suoraa toiminnallista vaikutusta ja siten keskeytysriskiä kriittisiin tuotantojärjestelmiin. Hankkeessa päädyttiinkin Kybermittari-arviointien suorittamiseen kuntien vesihuollon toiminnoissa. Arviointien ohjaus ja raportointi hankittiin palveluna ja arviointiosuus käsitti aloituspalaverin jälkeen 2 - 3 kuntakohtaista etätyöpajaa, jotka pidettiin pääosin yhden kuukauden aikana. Arviointien tuloksena muodostetut kyberturvallisuuden hallinnan kypsyystasot kuntien vesihuollossa olivat keskimäärin matalalla tasolla. Korkein kypsyystaso oli kyberuhkilta suojautumisessa ja heikoin kyberhyökkäyksestä palautumisessa. Yleisiä kehityskohteita nousi mm. riskienhallinnasta, kyberturvallisuuden edustuksesta johtoryhmässä, dokumentoinnista sekä tilannekuvatietoisuudesta ja jatkuvuuden hallinnasta. Tekniset suojauskeinot ja henkilöstön osaaminen olivat hyvällä tasolla. Vesihuollon toimintojen tieto- ja automaatioteknistä kokonaisuutta hoitaa kunnissa usein yksityinen teknologiakumppaniyritys. Kuntien tiedossa ei kuitenkaan useinkaan ollut yksityiskohtaisella tasolla, miten kumppanit hallitsivat kriittisten järjestelmien kyberturvallisuutta.

Suositus	S-5 Testaa kriittisen infrastruktuurin kyberhyökkäyksiin varautumisen taso
Huomioitavat asiat	Jos teknistä tai fyysistä testausta tehdään kriittiseen tuotantoympäristöön, asiasta tulee sopia johdon kanssa ja toimenpiteet on valmisteltava huolellisesti etukäteen. Vesihuollossa on usein käytössä vuosikymmeniä tuotannossa olleita SCADA-järjestelmiä, jotka ohjaavat esim. veden pumppausta. Ne ovat kyberturvan kannalta lähtökohtaisesti haavoittuvaisia järjestelmiä, joihin ei ole saatavilla korjauksia, joten testaus- ja arviointitoimenpiteet kannattaakin suunnata siihen, miten kyberturva on järjestetty niiden ympärille suojaamaan niitä hyökkäyksiltä. Teknologiakumppaneiden kanssa kannattaa sopia kyberturvallisuuden hallinnasta yksityiskohtaisesti osana ylläpitosopimuksia. Kybermittarin työpajoissa on hyvä olla edustusta ainakin tietoturvaosaamisesta, johdosta sekä itse kriittisestä toiminnosta. On myös hyvä tiedostaa, että Kybermittari-arviointi perustuu subjektiivisiin arvioihin, kun taas tekniset ja fyysiset testaukset antavat lähtökohtaisesti objektiivisia tuloksia.
Materiaalit	Tulosraportti
Teknologiat	Suosituksissa S-1-4 kuvatut teknologiat, Kybermittari-arviointityökalu
Kehitys-toimenpiteitä	Suosituksissa S-1-4 kuvatut kehitystoimenpiteet. Kybermittarin kypsyystasojen kasvattaminen. NIS2:n siirtymäajan päättymisen ja sen tiedonhallintalakiin tuomien muutosten myötä ainakin pienten kuntien vesihuollossa vaikuttaisikin olevan runsaasti kehitettävää niiden vaatimusten täyttämiseksi. Toimenpiteisiin luo painetta myös kansainvälisen turvallisuustilanteen kiristyminen.
Lisätiedot	Julkri, Kybermittari

Versionhallinta

Versio	Muutokset	Tekijä	Pvm
0.1		Ari Peltoniemi	19.1.2024
0.2	Lisätty toimenpidesuositukset	Ari Peltoniemi	30.1.2024
0.3	1) Lisätty toimintamallin yksityiskohtaisempi kuvaus, 2) huomioitu Kuntaliiton kommentit	Ari Peltoniemi	6.2.2024
0.4	Lisätty tiivistelmä ja viimeistelty ulkoasua	Ari Peltoniemi	15.2.2024