TOTEUTETTAVUUSTUTKIMUS: YRITYSTEN TIETOTURVAA VOI PARANTAA HELPOSTI!

Sisältö

1 Alkusanat ja keskeisten havaintojen esittely

Sanat "kyberturvallisuus" ja "helppo" esiintyvät harvoin samassa lauseessa. Tämä oli yksi keskeisistä ongelmista, mitä Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen TONTTU-lempinimen saanut toteutettavuustutkimus lähti muuttamaan. Tekemisen helppous on keskiössä, kun yhteiskunnan kokonaisturvallisuutta halutaan parantaa laajemmassa skaalassa.

Ylivoimaisesti suurin osa suomalaisista yrityksistä on pieniä tai keskisuuria. Sadat jopa tuhannet niistä ovat mukana toteuttamassa yhteiskuntamme kriittisiä toimintoja. Suuryrityksille suunnatut turvallisuusratkaisut harvemmin toimivat pienemmissä yrityksissä, joissa ei ole kyberturvallisuudelle erillistä resurssia tai erityisosaamista. Toisaalta suurten yritysten tietoturvahenkilöstön kalenterit ovat täyttyneet olemassa olevista hankkeista, joka vaikuttaa olemassa olevien resurssien käytettävyyteen.

Olipa organisaatio iso tai pieni, resurssit ovat todennäköisesti vähissä. Helpot tavat kehittää kyberturvallisuutta kiinnostavat. Onko sellaisia olemassa? TONTTU-hanke tutki tätä 11 huoltovarmuuskriittisen organisaation kanssa – ja tulokset eivät jättäneet kylmäksi.

Hanke osoitti, että yhteiskunnan kriittisten palveluiden kyberturvallisuutta voidaan parantaa kevyesti käyttöön otettavilla menetelmillä. Organisaatiot itse kokivat pilotin tuovan heille välittömiä ja suoria hyötyjä.

Toteutettavuustutkimuksessa kävi ilmi, että:

- Yhdeksässä organisaatiossa löytyi vuotoja eristetyistä tietoverkoista.
- Seitsemän organisaation omista tai toimittajien palveluista löytyi mahdollisia haavoittuvuuksia.
- Kahdessa tapauksessa haavoittuvuuksin liittyi myös hyväksikäyttöepäilyjä, joista yksi vahvistettiin työryhmälle. Tietomurtoepäilyt eivät liittyneet operatiivisiin verkkoihin.
- Internet-palveluiden tietovuotojen yleistyminen näkyi myös hankkeen osallistujilla.
- Seitsemän organisaatiota tunnisti henkilöstönsä olleen uhreina tietovuodoille. Osa osallistujista oli jo aiemmin tunnistanut tietovuodon uhrit ja alkanut kouluttaa säännöllisesti henkilöstöään suojaamaan itseään ja työympäristöään vuotojen haittavaikutuksilta.

Hankkeen osallistujat tunnistivat automaattisesti suojattavia kohteitaan, vastaanottivat kohteisiin liittyvää tietoturvatietoa automaattisesti ja testasivat verkkojen eristysten toimintaa. Hankkeen havaintojen valossa on kannustavaa, että kaikki vastaajat harkitsevat vastaavien kyvykkyyksien hyödyntämistä jatkossa. Ilahduttavaa oli, että kolme osallistujaa otti edellä mainitut toimenpiteet käyttöön välittömästi.

Osana hankkeen havaintoja nousi esille, että organisaatioiden tulisi lisätä näkyvyyttään kolmansien osapuolten tuottamiin palveluihin, jotta ne voivat vaatia toimittajilta toimia turvallisuuden parantamiseksi. Konkreettiset havainnot parantavat organisaatioiden kykyä arvioida toimittajien kyberturvallisuuden tasoa ja toimittajat puolestaan voivat saada kilpailuetua toimimalla kyberturvallisesti.

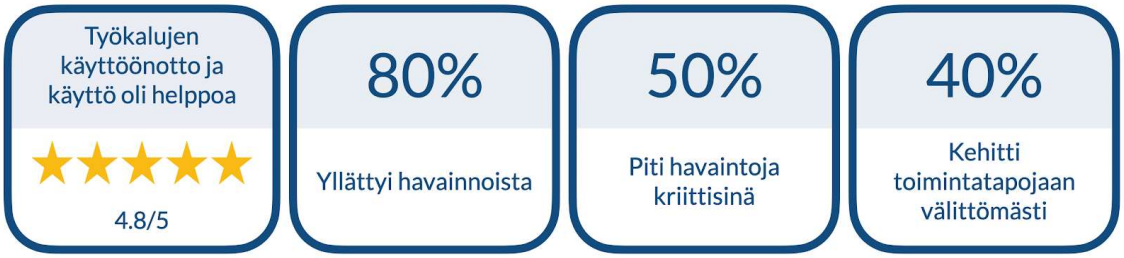
Hankkeen tekemät haavoittuvuushavainnot auttoivat osallistujia ymmärtämään heidän toimittajiensa kyberturvallisuuden reagointikykyä. Konkreettiset, haavoittuvuuksiin ja vuotoihin liittyvät selvityspyynnöt erottivat nopeat toimittajat ja palveluntuottajat niistä, jotka eivät kyenneet reagoimaan havaittuihin asioihin tarpeeksi nopeasti. Osaavat toimittajat ja palveluntuottajat reagoivat nopeasti. Vastaukset olivat selkeitä sekä loogisia. Heikomman reagointikyvyn omaavat toimittajat puolestaan hidastelivat, vastasivat epäselvästi, jos ollenkaan, tai pyrkivät vähättelemään ongelmia.

Toimitusketjun kyberturvallisuuden reagointikykyyn vaikuttamisella voi olla kerrannaisvaikutuksia, koska yksi toimittaja voi palvella useaa huoltovarmuuskriittistä organisaatiota. Kun toimittajat parantavat omaa toimintaansa, huoltovarmuuskriittiset asiakkaat hyötyvät. Huoltovarmuuskriittisten organisaatioiden rooli on tässä olennainen. Yritysten itsensä tai ulkopuolisen toimijan tulisi kyetä tekemään kyberturvallisuuteen liittyviä havaintoja. Vain siten he voivat arvioida toimittajiensa kyberturvallisuuden reagointikykyä ja vaihtaa kokemuksia muiden yhteiskunnan huoltovarmuuskriittisten toimijoiden kanssa. Avoin vertailu antaa kilpailuetua kyberturvallisuudesta huolta pitäville toimijoille.

Kyberturvallisuuskeskuksen tilannekuva rakentuu useista palasista. TONTTU-projektin avulla Kyberturvallisuuskeskus voi parantaa omaa tilannekuvaansa yhteistyössä yritysten kanssa. Yritykset osallistuivat yhteistyöhön mielellään, kunhan se ei kuormita niitä/henkilöstöä liikaa. Automatisointi ja helpot työkalut ovat avainasemassa tämän tyyppisen tilannekuvan rakentamisessa.

Tilannekuvan lisäksi tulokset näyttävät, että kyberturvallisuuden perusasioista huolehtimalla saadaan kestävää hyötyä. Mukana olleet huoltovarmuuskriittiset organisaatiot kokivat TONTTU-projektin tärkeäksi ja toivoivat, että vastaavaa työtä tehtäisiin myös tulvaisuudessa.

Kysyttäessä asteikolla 1-5, kuinka tärkeää on, että Kyberturvallisuuskeskus järjestää vastaavia pilotteja jatkossakin, jokainen osallistuja antoi täydet viisi pistettä.



Kuva: Osallistujat arvostivat työkalujen helppokäyttöisyyttä ja havaintojen hyödyllisyyttä.

2 Aikaisemmat hyvät opit mukaan uuteen työhön

Autoreporter-palvelusta ja HAVAROsta saadut opit

Kyberturvallisuuskeskuksen täysin automaattinen Autoreporter-palvelu ja siihen liittyvä yhteistyö teleoperaattoreiden kanssa on pitänyt Suomen verkot puhtaina jo yli 15 vuotta. Autoreporter-palvelu lähettää verkkojen ylläpitäjille automaattisesti tietoja heidän verkossaan havaituista tietoturvaa vaarantavista ilmiöistä. Palvelun tarkoitus on antaa ylläpitäjille tietoja, joiden avulla he voivat puuttua tietojenkäsittelyä yleisesti vaarantaviin tietoturvapoikkeamiin. Autoreporter on opettanut, kuinka yksinkertaisilla asioilla voi olla suuri vaikutus, kun ne tehdään suuressa mittakaavassa. Suomen verkot ovat vuosittain maailman puhtaimpia.

HAVARO eli vakavien tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä on puolestaan suojannut Suomen huoltovarmuuskriittisiä organisaatiota jo vuodesta 2011 lähtien. HAVARO on Kyberturvallisuuskeskuksen erityisesti huoltovarmuuskriittisille organisaatioille ja valtionhallinnolle tarjoama palvelu, jossa eri lähteistä saatavia tietoturvauhkia koskeviin tunnisteisiin pohjautuen organisaation verkkoliikenteestä havainnoidaan haitalliseksi tunnistettua tai normaalista poikkeavaa liikennettä.

HAVARO innovoi mallin, jossa yhteistoiminnan edut sekä viranomaisille että organisaatioille mietitään entistä tarkemmin. Kun ensimmäiset osallistujat kertoivat HAVAROn konkreettisista hyödyistä toisille huoltovarmuuskriittisille organisaatioille, HAVARO alkoi kasvaa vauhdilla. Kasvun myötä sekä Kyberturvallisuuskeskuksen tilannekuva että HAVAROn hyödyllisyys paranivat entisestään, kun yhdestä organisaatiosta saadut havainnot auttoivat muita yrityksiä suojautumaan entistä paremmin.

Maailma muuttuu ja innovaatioilla on vanhenemispäivämäärä

TONTTU-projektia suunniteltaessa Autoreporterista ja HAVAROsta saatuja hyviä oppeja haluttiin hyödyntää. Samalla havaittiin kehitystarpeita, joita lähdettiin parantamaan TONTTU-projektissa. Autoreporter- ja HAVARO-palvelut ovat perustuneet oletukseen, että suojattavat kohteet sijaitsevat Suomessa. Tämä oletus ei pidä enää täysin paikkaansa. Teknologioiden muutos tuo mukanaan muuttuvan toimintaympäristön, joka asettaa uusia vaatimuksia toimintaympäristön havaitsemiselle ja siellä oleville työkaluille.

Pilvipalveluihin liittyvät trendit näkyvät jo edistyksellisimmissä kriittisen infrastruktuurin organisaatioissa. IT siirtyy pilveen vauhdilla. Ensimmäiset merkit operatiivisten toimintojen toteuttamisesta pilvipalveluiden avulla on jo käytössä. TONTTU-projektin yhteydessä testattiin tapoja uudista toimintaa ja vastata uusiin haasteisiin.

Kuva: Palvelut muuttavat pilveen, kuinka käy näkyvyyden?

Vaikuttavuus vaatii skaalautuvuutta, skaalautuvuus vaatii lähes täydellistä automatisointia

TONTTU-projektin aikana testattiin uusia, entistä kevyempiä menetelmiä, joilla yhtäaikaisesti sekä parannetaan yhteiskunnan huoltovarmuuskriittisten organisaatioiden turvallisuutta että lisättiin Kyberturvallisuuskeskuksen tilannekuvaa organisaatioiden suojattavista kohteista. Menetelmät skaalattiin sekä osallistujamäärien että osallistuvien organisaatioiden koon mukaan.

Aikaisemmat havainnot ja opit, joita kuvattiin yllä, loivat kehyksen TONTTU-projektille, jossa nousi viisi väittämään, joiden tulisi toteutua hankkeessa. Näitä voitaisiin soveltaa myös vastaavissa hankkeissa tulevaisuudessa:

1. **Päätös osallistumisesta täytyy olla helppo organisaatiolle**. Osapuolten välisen sopimisen tulee olla yksinkertaista: jos sopimuksia tarvitaan, niiden tulee olla lyhyitä ja selkeitä.

   Tässä selvityksessä osapuolet olivat Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus ja huoltovarmuuskriittinen organisaatio. Hanke vahvisti ennakko-oletusta siitä, että yhteistyön kokeileminen ei myöskään saa vaatia osallistujalta työlästä hankintaprosessia.

2. **Osallistujien aika on arvokasta.** Hanke ei saa viedä merkittävästi osallistujien aikaa. Vähän kokouksia, työkalujen helppo käyttöönotto helppoa, työkalut eivät vaadi jatkuvaa käyttöä, vaan ne tekevät työtä jatkuvasti taustalla.

3. **Yhteistyön pitää perustua automaatioon**. Manuaalinen tiedonvaihto toimii poikkeustilanteessa, mutta jatkuva yhteistyö vaatii automatisoitua tiedonvaihtoa.

4. **Tietoturvan kivijalka rakentuu perusasioista.** Hanke tukee perusasioista huolehtimista. Moni etsii ratkaisuja päivänpolttaviin ongelmiin. Huolehtimalla tietoturvan perusasioista, yritys varautuu kattavasti myös tulevaisuuden uhkiin.

5. **Ihmisten aika tulisi käyttää korjausten ja ratkaisujen miettimiseen.** Hanke keskittyy selkeisiin havaintoihin. Hankkeen skaalautuvuustavoitteet eivät täyty kustannustehokkaasti, mikäli itse havainnot vaativat ihmisen analyysiä tai tulkintaa.

3 Kevyet menetelmät tietoturvan parantamiseksi

Suojattavien kohteiden tunnistaminen ja tarpeellisen tiedon jakaminen

Julkiseen verkkoon näkyvät palvelut pitää meidän inventoida tarkemmin."

Järjestelmät, henkilöstön käyttämät palvelut, alihankintaketjut ja näihin liittyvät vastuut ovat monimutkaistuneet siinä määrin, että verkon suojattavien kohteiden tunnistaminen on vaikeaa. Tunnistusta vaativat kohteet vaihtelevat tietovuodoille alttiista käyttäjätiedoista teknisiin pilvipalvelujen resursseihin.

Hankkeessa huoltovarmuuskriittiset organisaatiot tunnistivat suojattavia kohteitaan ja jakoivat tietoa pilvipalveluidensa kriittisistä resursseista avustaakseen Kyberturvallisuuskeskusta kohdistamaan kansallista tietoturvatyötä näiden kohteiden suojaamiseksi. Kun Kyberturvallisuuskeskus tietää automaattisesti ja ajantasaisesti, missä yhteiskunnan huoltovarmuuskriittiset palvelut tarkalleen sijaitsevat, se voi välittää kohteisiin liittyvät tietoturvayhteisön varoitukset automaattisesti suoraan kohteiden omistajille.

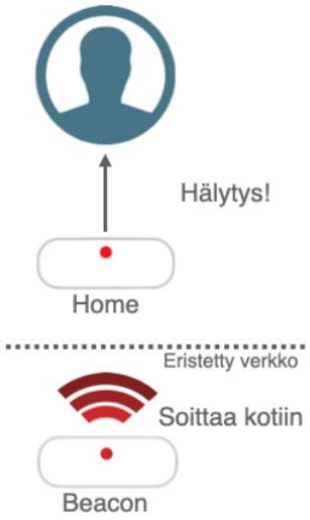
"Tiedonvaihdon tulee olla automaattista, muuten se ei vaan toimi"

Tutkimuksessa teknologiatoimittajien, Badrap Oy ja SensorFu Oy, kehittämiä menetelmiä yhdistettiin Kyberturvallisuuskeskuksen palveluihin. Badrap.io mahdollisti tietoturvatiedon tuottajille ja välittäjille yrityksien tavoittamisen kohdistetulla tietoturvatiedolla. Palvelu itsessään auttaa yrityksiä tunnistettujen ongelmien korjaamisessa. Esimerkiksi kun joku yrityksien käyttäjistä on altistunut käyttäjätietojen vuodolle, voi palvelun tarjoama välitön ja kohdistettu koulutus ja toimintaohjeet ehkäistä vuodon ikävät seuraukset. Käytännössä palvelu kytkee tietoturvan sisällöntuottajat ja yritykset yhteen, sekä varmistaa että tyypillisiin korjauksiin löytyy valmis käsikirjoitus. Yritykset suojaavat palvelun avulla sekä henkilöstöään, että pilvipalveluitaan.

SensorFu Beacon tuote luo kyvykkyyden verkon eristyksen toimivuuden jatkuvalle valvonnalle. Verkkojen eristys on yksi tärkeimmistä tietoturvakontrolleista korkean turvallisuuden tietoverkoissa. Beacon automatisoi normaalisti käsin tehtävän eristyksen testauksen ja tuottaa hälytyksiä löytyvistä vuotokohdista. Hälytykset mahdollistavat verkon omistajan

nopean reagoinnin. Verkon vuotokohtia saattaa syntyä vahingossa, esimerkiksi konfiguraatiomuutoksissa, inhimillisten virheiden johdosta tai vihamielisen toimijan tekeminä.

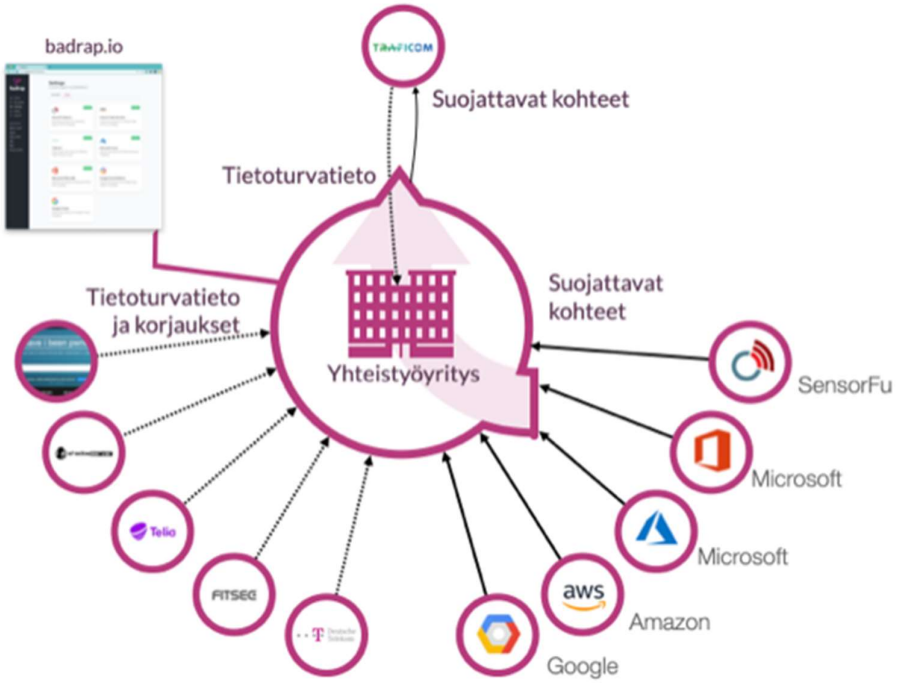
Toimistoverkkojen jatkuva tunnistus toteutettiin sijoittamalla eristettyjen verkkojen testaamiseen tarkoitettu SensorFu Oy:n Beacon-ohjelmisto poikkeuksellisesti avoimeen toimistoverkkoon. Beaconin yhteydenottojen lähdeosoitteet merkittiin automaattisesti suojattaviksi kohteiksi. Osallistujat jakoivat tiedot automaattisesti Kyberturvallisuuskeskukselle Badrapi.io-palvelussa Traficom-sovelluksen avulla.



Kuva: SensorFu Beaconit testaavat ja hälyttävät eristettyjen verkkojen vuodoista.

Hankkeessa Badrap.io-verkkopalvelu toimi sovellusalustana ja kohtaamispaikkana, jossa SensorFu:n kartoituskäyttöön sovittama Beacon-sovellus ja suosittujen pilvipalvelualustojen (Microsoft, Google, Amazon) kohteiden seurannat tuottivat yritykselle reaaliaikaista kohdetietoa. Tämä mahdollisti yrityksille myös kohdetiedon vapaaehtoisen jakamisen Kyberturvallisuuskeskukselle palvelun Traficom-sovelluksen avulla.

Tietoturvatiedon tuottajat, kuten hankkeessa mukana olleet Kyberturvallisuuskeskus ja SensorFu, voivat julkaista Badrap.io-palvelussa integraatiosovelluksia, joiden avulla organisaatiot parantavat turvallisuuttaan. Osallistujat arvostivat muun muassa palvelun helppokäyttöisyyttä ja tiedonjaon automatisointia.



Kuva: Badrap.io-verkkopalvelu toimii kohtaamispaikkana, jonka avulla yritykset tunnistivat suojattavia kohteitaan ja jakoivat vapaaehtoisesti tietoja Kyberturvallisuuskeskukselle.

Tunne mitä suojaat

On tärkeää tuntea oma toimintaympäristö, , jotta osataan välttää sitä uhkaavia tekijöitä tai varautua niihin. Osallistujat arvioivat suojattavien kohteiden tunnistamisen vaikuttavan merkittävästi organisaation turvallisuuteen. Asteikolla 1-5, missä 5 tarkoitti "täysin samaa mieltä", IT-verkoissa vaikutusarvioiden keskiarvo oli 4,3, ja operatiivisten verkkojen osalta 4,6. Vastausten perusteella vastaajat olivat täysin tai lähes samaa mieltä siitä, että suojattavien kohteiden tunnistaminen vaikuttaa merkittävästi organisaation turvallisuuteen. Pieni painotusero saattaa selittyä sillä, että useampi osallistuja oli lähiaikoina tunnistanut OT-verkkojen näkyvyyden kyseisen vuoden kehityskohteeksi.

Parantuneesta näkyvyydestä yllättäviäkin hyötyjä

"Autoitte meitä pääsemään melkoisen hankalan verkkohäiriön jäljille."

Näkyvyys omiin suojattaviin kohteisiin parantaa organisaation kykyä käsitellä odottamattomia poikkeustilanteita. Esimerkiksi hankkeeseen osallistunut organisaatio pääsi kaksi viikkoa kestäneiden verkko-ongelmien juurisyyn jäljille hankkeen tuoman lisänäkyvyyden avulla. Badrapi.io-palvelun suojattavien kohteiden listalla ollut, toimistoverkon IP-osoite oli muuttunut juuri samaan aikaan kun verkko-ongelmat alkoivat. Verkko-osoitteen muutos puolestaan esti pääsyn joihinkin ulkopuolisiin palveluihin, jotka edellyttivät tietoliikenteen lähteeksi tiettyä IP-osoitetta.

Erityissuojattavien verkkojen eristyksen testaus

Verkkojen eristys on yksi tietoturvan kulmakivistä. Tyypillinen tietomurto ei ole erityisen kohdennettu vaan ennemmin opportunistinen ja helpot kohteet kiinnostavat rikollisia. Verkkojen eristämisellä voidaan varmistaa, että liiketoiminnan kannalta keskeiset järjestelmät on suojattu erillisissä verkkosegmenteissään. Mikäli rikollinen pääsee tunkeutumaan organisaation verkkoon, ei koko toiminta vaarannu vaan sen tietty osa-alue. Hanke tarjosi osallistujilleen mahdollisuuden testata eristystensä pitävyyttä.

Pilotin aikana SensorFun Beaconeita toimitettiin 11 organisaation kriittisiin verkkoihin. Verkot olivat luonteeltaan automaatioverkkoja, joiden tulisi olla täysin eristetty Internetistä. Nämä automaatioverkot pitävät sisällään mm. SCADA, ADMS ja HVAC -järjestelmiä. Beacon otettiin käyttöön keskimäärin neljässä verkossa asiakasta kohden.

"Havainnon pohjalta tehtiin kyllä pitkiä keskusteluita, miten tämä korjattaisiin."

4 Onnistunut yhteistyö osallistujien kanssa

Kymmenen yritystä tuotantoon kolmessa kuukaudessa

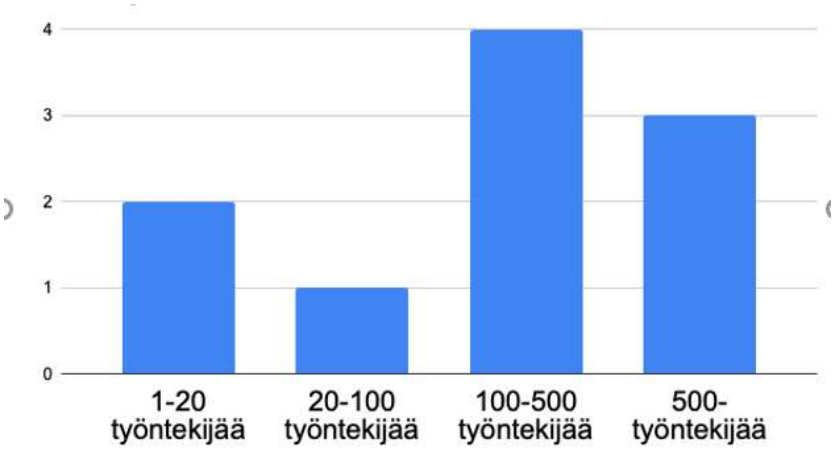
"Käyttöönotot onnistuivat helposti. "

Aloittamiseen, päätöksentekoon, sopimiseen, käyttöönottoon ja käyttöön voiliittyä monta käännettä, joita suunnitelmissa ei ole välttämättä huomioitu. Skaalautuvuudessa on kyse paljon muustakin kuin teknologiasta. Hankkeen ensimmäinen tulikoe oli löytää 10 kiinnostunutta yritystä ja saada kyvykkyydet tuotantoon kolmessa kuukaudessa, jotta kuudennen kuukauden kohdalla hankkeen alustavat tulokset olisivat selvillä.

Kyberturvallisuuskeskus tiedotti hankkeesta sähköpostilla omille sidosryhmilleen. Lisäksi työryhmä tunnisti suoraan hankkeen kannalta kiinnostavia kohdeorganisaatioita. Hankkeeseen pyrittiin löytämään sekä suuria että mahdollisimman pieniä osallistujia.

Työryhmä kirjasi yhteydenottojen ja omien tunnistustensa pohjalta 25 organisaatiota, joiden kiinnostus osallistumiseen selvitettiin tarkemmin. Näistä yrityksistä kahta ei tavoitettu ajoissa, kaksi oli valmis osallistumaan myöhemmin, kymmenen kanssa keskusteltiin, mutta osallistumiseen ei saatu vahvistusta ennen paikkojen täyttämistä. Loput 11 otettiin mukaan hankkeeseen.

Alla olevassa kuvassa on kuvattu kymmenen yrityksen osalta niiden kokoluokka. Yhdestätoista mukana olleesta yrityksestä kymmenen vastasivat kyselyyn, jossa kartoitettiin mm. organisaation kokoa.



Kuva: Hankkeeseen osallistuneiden organisaatioiden koko.

Havaintoja heti alusta lähtien

Ensimmäiset havainnot saatiin verkon eristyksen testeistä lähes välittömästi, kun eristystä testaavia Beacon-ohjelmistoja saatiin tuotantoon. Vuotoja löytyi lopulta yhteensä yhdeksässä yrityksessä yhdestätoista.

"Tehtyjä havaintoja ei varmastikaan olisi itse havaittu vaan hankkeen menetelmin havainnot mahdollistuivat."

Ihmiset ovat edelleen turvallisuuden keskiössä. Koska suurin osa verkon hyökkäyksistä kohdistuu käyttäjiin, on tämän seurauksena työntekijä kahdessa roolissa: paitsi suojattava kohde myös yritystä suojaava toimija. Tietovuotojen uhreilla on korottunut riski joutua myös huijausten kohteeksi. Salasanojen uudelleenkäyttö on johtanut vuodettujen salasanojen hyödyntämiseen hyökkäyksissä. Muiden henkilökohtaisten vuodettujen tietojen hyväksikäyttö lisää puolestaan työntekijöihin kohdistuvien huijausten uskottavuutta.

"Aina voi olla haavoja, joita ei omilla tai kumppanin kyvyillä havaita. Tietämys ja asennoituminen muuttuivat kyllä hankkeen vuoksi.

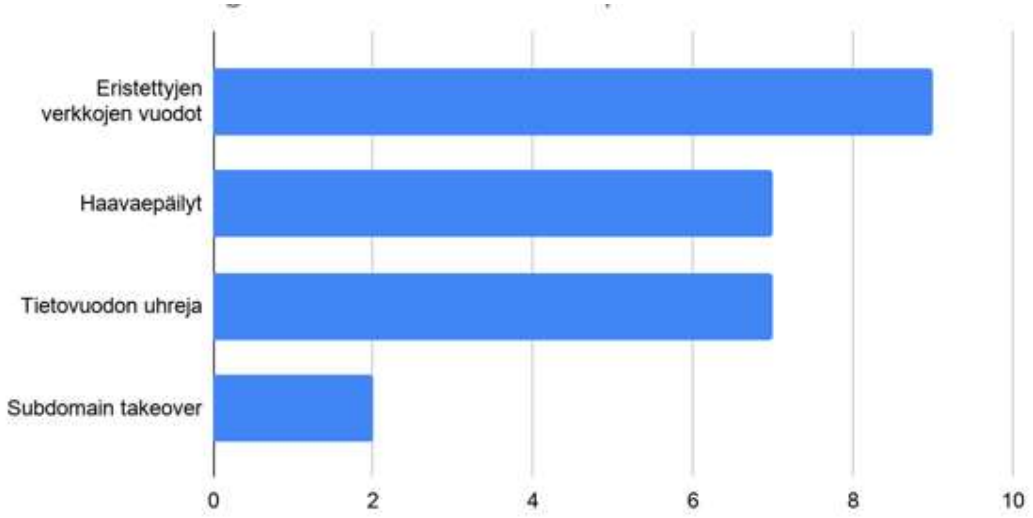
Kun näkyvyys organisaatioiden suojattaviin kohteisiin parani, työryhmä teki kevyitä perustarkastuksia IT-järjestelmiin.

- Seitsemässä tapauksessa organisaation omista tai toimittajien palveluista löytyi haavoittuvuusepäilyjä, joita osallistujat selvittivät toimittajiensa kanssa.
- Kahdesta organisaatiosta paljastui ns. "Subdomain takeover" -haavoittuvuus, joka mahdollistaa yrityksen nimen hyödyntämisen yritykseen tai ulkopuolisiin kohdistuvissa huijauksissa.

Kaksi yllä esitetyistä havainnoista johti myös tietomurtoepäilyihin, joista toiseen saatiin vahvistus hankkeen aikana. Tietomurrot eivät liittyneet operatiivisiin verkkoihin. Eri Internet-palveluiden tietovuotojen yleistyminen näkyi myös hankkeen osallistujilla.

Seitsemän organisaatiota tunnisti henkilöstönsä olleen uhreina tietovuodoille. Osa osallistujista oli jo aiemmin tunnistanut tietovuodon uhrit ja alkanut kouluttaa säännöllisesti henkilöstöään suojaamaan itseään ja työympäristöänsä vuotojen seurauksilta.

Huomionarvoista oli, että yrityksillä, joiden toimintatapoihin kuuluu säännöllinen palveluiden tarkastaminen esimerkiksi nimipalvelutietueiden ja palomuurisääntöjen osalta, ei tehty lainkaan havaintoja poikkeamista hankkeen aikana. Tämä osoittaa sen, että ruohonjuuritason perustyö on siis hyvin tärkeää ja palkitsee turvallisuuden tason paranemisena.



Kuva: Erilaisia poikkeamatyyppejä, joita organisaatioissa havaittiin

5 Tulokset ja johtopäätökset

Hanke osoitti seuraavat asiat:

- Yhteiskunnan kriittisten palveluiden kyberturvallisuutta voidaan parantaa skaalautuvasti kevyesti käyttöönotettavilla menetelmillä. Yritykset kokivat pilotin menetelmien tuovan heille välittömiä hyötyjä.
- Kyberturvallisuuskeskus voi parantaa omaa tilannekuvaansa yhteistyössä yritysten kanssa. Yritykset osallistuvat yhteistyöhön mielellään, kunhan se ei kuormita heitä liikaa. Automaatio ja helpot työkalut ovat avainasemassa.
- Tulokset näyttävät myös, että kyberturvan perusasioista huolehtimalla saadaan kestävää hyötyä.
- Yritysten tulisi panostaa myös tuotantoverkkojen tärkeiden tietoturvakontrollien, kuten verkkojen eristyksen, toimivuuden valvontaan. Tarvetta havainnollistaa projektin löydös, jossa 81 % osallistuvien organisaatioiden eristetyiksi tarkoitetuista verkoista vuotivat odottamattomilla tavoilla.
- Yritysten tulisi parantaa näkyvyyttä heidän yhteistyökumppaneiden tuottamien palveluiden haavoittuvuuksiin. Melkein kaikki ulospäin näkyvät haavoittuvuudet liittyivät toimittajien tuottamiin palveluihin, jotka eivät ole aktiivisessa seurannassa.
- Yritysten tulisi kouluttaa henkilöstöään varautumaan tietovuotoihin sekä niistä seuraaviin mahdollisiin hyökkäyksiin ja huijauksiin. Jos yrityksen täytyy priorisoida koulutustaan, toimenpiteet kannattaa ensiksi kohdentaa avainhenkilöihin ja tietovuotojen uhreihin.

Kaikki osallistujat harkitsevat vastaavien kyvykkyyksien hyödyntämistä jatkossa. Kolme organisaatiota siirtyi suoraan toimeen, hankkien vastaavat kyvykkyydet.