HYÖKY PALVELUKUVAUS

Hyöky - kansallinen hyökkäyspintakartoitus
kyberturvallisuuden parantamiseksi
30.10.2023

1 Yleinen kuvaus Hyöky -palvelusta

Hyöky on Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen (jäljempänä Kyberturvallisuuskeskus tai lyhenteenä KTK) tuottama kansallinen hyökkäyspintakartoitus kyberturvallisuuden parantamiseksi. Palvelun tavoitteena on auttaa organisaatioita parantamaan kyberturvallisuuttaan tarjoamalla kohdennettua ja konkreettista havaintoihin perustuvaa tietoa heidän hyökkäyspinnastaan kyberuhkien tunnistamiseksi. Näin organisaatiot pystyvät tunnistamaan ja suojaamaan kohteitaan etukäteen, edistämään toimintakykyään ja kansalaisille tarjottavien palveluiden turvallisuutta ja toimintavarmuutta.

Hyökkäyspinta tarkoittaa heikkouksia ja haavoittuvuuksia, joita asiaton taho voisi hyödyntää esimerkiksi tietomurron tai muun kyberhyökkäyksen toteuttamiseen. Hyökkäyspintatieto auttaa organisaatioita arvioimaan korjaustoimenpiteiden tarvetta ja toteuttamaan niitä kohdennetusti ja ennakoivasti. Hyöky-palvelu tuottaa tilannekuvan asiakkaan ilmoittamien IP-osoiteavaruuksien perusteella julkiseen internetiin näkyvien palveluiden muodostamasta organisaatiokohtaisesta hyökkäyspinnasta.

Palvelu on kohdennettu ensivaiheessa kunnille ja sen käyttö on maksutonta. Tavoitteena on avata palvelu myöhemmin myös muille kohderyhmille kuten julkishallinnon organisaatioille. Hyöky-palvelun tarkoituksena on tukea asiakkaalle asetettujen lakisääteisten tietoturvallisuusvelvoitteiden täyttämistä esimerkiksi Tiedonhallintalakiin (906/2019), yhteiskunnan toiminnan kannalta kriittiseen rooliin tai huoltovarmuuteen perustuen. Palvelun tavoitteena on auttaa asiakkaita parantamaan kyberturvallisuuttaan tarjoamalla organisaatiokohtaista tietoa heidän hyökkäyspinnastaan kyberuhkien tunnistamiseksi, jotta asiakasorganisaatio pystyy suojaamaan kohteitaan etukäteen.

Kyberturvallisuuskeskuksella on kansallisena tietoturvaviranomaisena ainutlaatuinen näkymä suomalaisen yhteiskunnan tietoturvaympäristöön. Kansainvälisen viranomaisyhteistyön kautta Kyberturvallisuuskeskus saa tietoa myös globaaleista tietoturvauhkista ennen niiden julkistamista. Hyöky-palvelua käyttävät organisaatiot pääsevät hyödyntämään Kyberturvallisuuskeskuksen tuottamaa tietoa ja palveluita omassa tietoturvatyössään.

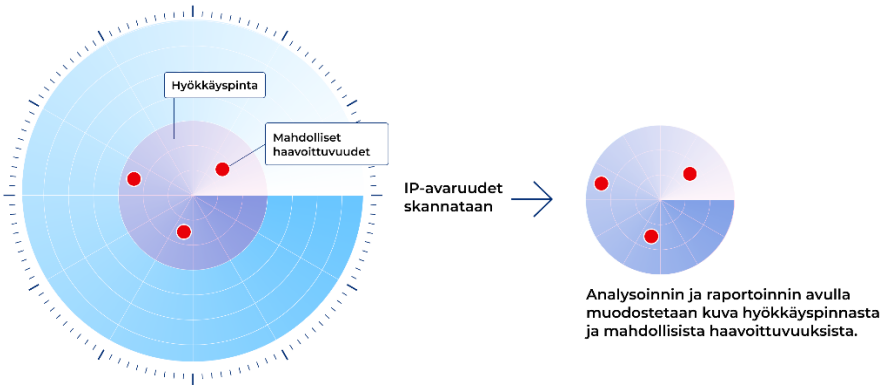
Palvelumallissa asiakas tilaa palvelun Kyberturvallisuuskeskukselta ja hyväksyy palvelun käyttöehdot. Käyttöönoton jälkeen organisaatio saa määräajoin organisaation hyökkäyspintaa koskevan kartoitusraportin. Raportti sisältää ulkopuoliseen julkisen tietoverkon kautta tehtävään havainnointiin perustuvan näkymän tietoturvapuutteisiin ja perustasoisen selvityksen havaituista tietoturvaongelmista. Raportti tarjoaa konkreettista tietoa asiakkaan palveluiden mahdollisista teknisistä heikkouksista, niihin kohdistuvista kyberuhkista ja niihin varautumisesta. Kartoituksia toteutetaan useita kertoja vuodessa, jolloin asiakas voi seurata organisaation hyökkäyspinnan kehittymistä ja varmistaa tehtyjen korjaustoimien onnistumisen. Palveluun ei kuulu esimerkiksi tunkeutumisyrityksiä tietojärjestelmiin tai havaittujen haavoittuvuuksien varmentamista ja korjaamista asiakkaan ympäristössä.

Asiakas vastaa itse kartoituksessa havaittujen puutteiden tarkemmasta arvioinnista ja selvittämisestä sekä korjaamiseen liittyvistä päätöksistä ja kustannuksista, tarvittaessa ulkopuolisten palveluntarjoajien avulla.

2 Kansallinen hyökkäyspintakartoitus yleisesti

Kyberturvallisuuskeskus kartoittaa kansallisesti julkisiin tietoverkkoihin näkyvää hyökkäyspintaa koko Suomea koskien osana lakisääteisiä tehtäviään. Toiminnan tarkoituksena on haavoittuvien tai turvattomasti konfiguroitujen verkkolaitteiden ja tietojärjestelmien havainnointi, niistä ilmoittaminen asianomaisille tahoille sekä kyberturvallisuuden tilannekuvan ylläpitäminen. Kerättyä havaintotietoa voidaan hyödyntää kyberturvallisuuden tilannekuvan ja tilastollisten koosteraporttien lisäksi myös organisaatiokohtaisten näkymien koostamisessa niiden julkisesti näkyvästä hyökkäyspinnasta, jonka kautta organisaatio voi altistua tietoturvaloukkauksille.

Hyökkäyspintakartoitusten toteutustapa perustuu ei-intrusiivisiin menetelmiin. Se tarkoittaa, että käytettävillä menetelmillä ei yritetä tunkeutua asiakkaan järjestelmiin, joten kartoituksista ei aiheudu haittaa sen kohteena olevien järjestelmien tai palvelujen toiminnalle. Käytännössä toimintamalli tarkoittaa teknisiä kyselyjä tai konekielisiä yhteydenottoja yleisesti saatavilla olevaan viestintäverkkoon tai tietojärjestelmään, palveluun, sen palvelimelle tai palvelimen sovellukselle. Yleisessä viestintäverkossa lähetettyjen automatisoitujen teknisten kyselyjen avulla kerätään tietoa esimerkiksi teknisistä ratkaisuista ja niiden avulla tarjotuista palveluista, kuten ohjelmistoista, joita viestintäverkoissa ja tietojärjestelmissä käytetään. Analysoimalla kyselyihin saatuja palvelimien lähettämiä vastauksia voidaan tunnistaa puutteellisesti suojattuja tai haavoittuvia ratkaisuja (kuva 1), minkä avulla niihin kohdistuvia kyberuhkia voidaan torjua ennakoivasti.



Kuva 1. Kyberturvallisuuskeskus kartoittaa kansallisesti julkisten tietoverkkojen hyökkäyspintaa.

Kartoituksissa käytetään useita työkaluja ja tietolähteitä havaintojen tekemiseen, rikastamiseen, analysointiin ja tulosten esittämiseen. Tällaisia datalähteitä voivat olla esimerkiksi erilaiset haavoittuvuuksiin ja niiden vakavuuteen liittyvät tiedot.

Kansallisia hyökkäyspintakartoituksia suoritetaan IP-osoitteista, jotka kuuluvat verkkoalueeseen: 93.190.98.0/24.

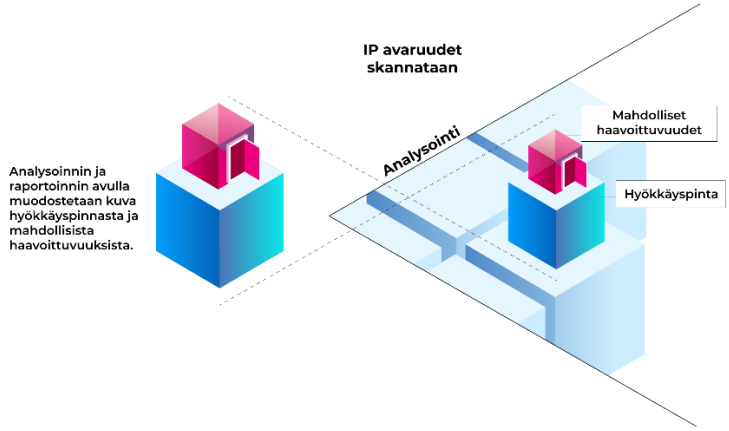
Kartoituksessa käytettyjä IP-osoitteita vastaavat nimet nimipalvelussa ovat muotoa: scannerN.ncsc.fi (N on numero väliltä 1-254 ja vastaa IP-osoitteen viimeistä oktettia. Esimerkiksi IP-osoitetta 93.190.98.23 vastaa nimi scanner23.ncsc.fi).

Tietoturvallisuus on keskeistä hyökkäyspintakartoitusten toteutuksessa. Kaikki kartoitusjärjestelmän sisältämät havainnot ja palvelun tiedot säilytetään Suomessa Traficomin konesaleissa. Tietojenkäsittely tapahtuu Suomessa Kyberturvallisuuskeskuksen hallinnoimilla laitteilla ja järjestelmillä pääsääntöisesti koneellisesti ja automatisoidusti. Yksittäiseen organisaatioon liittyvät tunnisteet järjestelmässä ovat pseudonymisoituja, mikä turvaa asiakkaan identiteettiä sekä yksittäisten havaintojen liitettävyyttä kyseiseen organisaatioon. Kehittämis-, ylläpito- ja hallintatoimenpiteet toteutetaan pääasiallisesti Kyberturvallisuuskeskuksen asiantuntijoiden toimesta.

Hyökkäyspintakartoitusten yksityiskohtaisempi toteutustapa sekä siihen liittyvien järjestelmien sisältämä tieto on luokiteltu salassapidettäväksi Julkisuuslain 24 §:n 1 momentin 7 ja 8 kohtien perusteella. Hyöky-palvelun tietosuojaseloste on saatavilla palvelun asiakaskäyttöliittymästä.

3 Hyöky-palvelu asiakkaalle

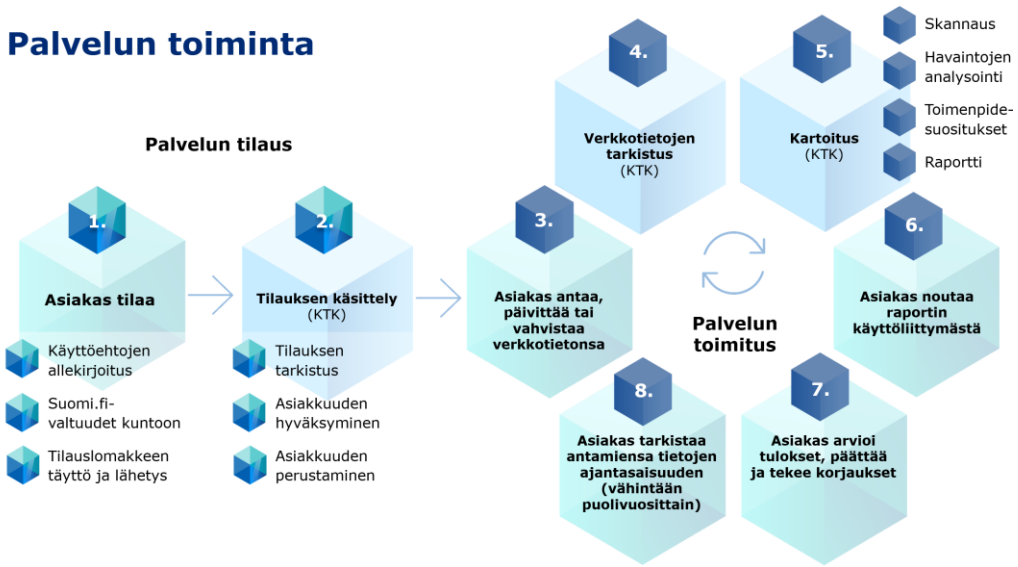
Kyberturvallisuuskeskuksen suorittamiin tietoverkkojen kartoituksiin perustuen organisaatio voi saada käyttöönsä näkymän omasta hyökkäyspinnastaan (kuva 2). Hyöky-palvelun käyttö ei edellytä asiakkaalta investointeja tai teknisiä toimenpiteitä asiakkaan järjestelmiin. Hyöky on matalan kynnyksen kyberturvapalvelu, jonka tarkoituksena on parantaa yhteiskunnan toimivuuden kannalta kriittisten palveluiden kyberturvallisuutta.



Kuva 2. Hyöky tuottaa näkymän organisaatiokohtaisesta hyökkäyspinnasta.

Hyöky-palvelu muodostuu kertaluontoisesta tilausprosessista ja toistuvasta palvelun toimitusprosessista. Pääpiirteissään palvelun toiminta on esitetty kuvassa 3.

Palvelun tilaus ja käyttöönotto erityisesti asiakkaan toiminnan kannalta on kuvattu tarkemmin alaluvussa 4.



Kuva 3. Yleiskuva Hyöky-palvelun toiminnasta

Palvelun toimitus voi alkaa, kun asiakas on antanut tiedot julkisista IP-osoitealueistaan asiakaskäyttöliittymässä hyväksytyssä muodossa. IP-osoitealueiden antamisen yhteydessä on ilmoitettava taho, kenelle se on rekisteröity. Asiakas vastaa siitä, että kyseiset IP-verkot ovat heidän käytössään ja että heillä on lupa liittää ne kartoitusten piiriin, jos ne on rekisteröity esimerkiksi asiakkaan palveluntarjoajalle. Kyberturvallisuuskeskus tarkistaa verkkotietojen rekisteröintitiedot ennen kartoituspalveluun liittämistä ja saattaa esittää lisätietopyyntöjä niihin

liittyen. Asiakas näkee verkkotietoihin liittyvän käsittelytilanteen palvelun asiakaskäyttöliittymässä.

Kartoitustoiminta asiakkaan osalta alkaa seuraavasta kartoitussyklistä sen jälkeen, kun uudet verkkotiedot on tarkistettu ja liitetty kartoitusten piiriin. Verkkotietojen tarkistuksesta ja kartoitussyklistä riippuen muutaman kuukaudenkin viive on mahdollinen, ennen kuin valmis kartoitusraportti on nähtävissä annettujen uusien verkkotietojen osalta asiakaskäyttöliittymässä.

Tietoverkkojen skannaus suoritetaan julkisesti internetissä havaittavissa oleviin palveluihin ja järjestelmiin ei-intrusiivisin menetelmin, kuten luvussa 2 on kuvattu. Erityisesti palvelun alkuvaiheessa skannauksia voidaan toteuttaa myös kohdennetusti asiakkaiden kartoituksen piiriin ilmoittamiin IP-osoiteavaruuksiin.

Havaintojen analysointi tapahtuu pääsääntöisesti automaattisesti. Analysointi perustuu esimerkiksi asiakkaan palvelimen antamiin versiotietoihin, mistä johtuen jotkut havainnot voivat olla virheellisiä tai puutteellisia. Tästä johtuen asiakkaan olisi hyvä varmistaa havainnot omassa ympäristössään. Raporttien yhteydessä toimitetaan yksityiskohtaisemmat havaintotiedot, jotta asiakas voi todentaa havainnot, yksilöidä haavoittuvat palvelimet ja palvelut ja korjata mahdolliset tietoturvapuutteet.

Toimenpidesuositukset yleisimpiin havaintoihin liittyvien puutteiden korjaamiseksi generoidaan automaattisesti raportille havaintojen yhteyteen. Ne ovat hyvin yleistasoisia eivätkä ota huomioon asiakkaan teknisen ympäristön toteutukseen liittyviä seikkoja tai tarkoituksenmukaisuutta tarkemmin.

Raportit koostetaan tehdyistä havainnoista, niihin liittyvästä analysoinnista ja toimenpidesuosituksista. Palvelussa on kahdenlaisia raportteja eri tarpeisiin.

- Erilaisia kuvaajia sisältävä yhteenvetoraportti tarjoaa helpommin hahmotettavan yleisnäkymän asiakkaan hyökkäyspintaan liittyviin havaintoihin, niiden ajalliseen kehittymiseen sekä yleisiin suosituksiin havaintojen korjaamiseksi ja hyökkäyspinnan pienentämiseksi.
- Yksityiskohtainen tekninen raportti sisältää yksilöidyt tiedot havainnoista, joiden avulla mahdollisia puutteita pystytään tarkemmin tunnistamaan, paikantamaan ja kohdentamaan tarvittavia korjaustoimenpiteitä.

Palvelun alkuvaiheessa raportteja tuotetaan asiakkaalle neljä kertaa vuodessa.

Raporttien tarkastelu ja tarvittaessa lataaminen tapahtuu asiakkaalle dedikoidusta käyttöliittymästä. Kartoitusraportit on luokiteltu salassapidettäviksi Julkisuuslain 24 §:n 1 momentin 7 ja 8 kohtien perusteella. Asiakas voi kuitenkin jakaa tietoa luottamuksellisesti esimerkiksi omalle palveluntarjoajalleen, jotta hyökkäyspinnan kehittymistä pystytään seuraamaan ja parantamaan tarkoituksenmukaisesti.

Kartoituksen tulosten arviointi on hyvä tehdä asiakasorganisaation ja mahdollisen ICT-palveluntarjoajan yhteistyönä. Hyökkäyspintakartoituksen tulokset perustuvat organisaation ulkopuolelta, julkisesta internetverkosta teknisesti tehtyihin havaintoihin. Havainnot kuvaavat, miltä verkon hyökkäyspinta näyttää ulospäin tiettynä ajanhetkenä ulkopuolisen toimijan näkökulmasta.

Suuntaa antavien havaintojen tulkitseminen niiden todellisen merkittävyyden kannalta edellyttää organisaation palveluinfrastruktuurin tuntemusta. Esimerkiksi kartoituksessa havaittu puute tai uhkatekijä voi olla ICT-järjestelmien toteutuksen kannalta tarkoituksenmukainen tai esimerkiksi perustua vanhentuneisiin ohjelmistotunnisteisiin, vaikka ohjelmistot olisikin jo päivitetty. Organisaation hyökkäyspinnan tilanne saattaakin näyttää kartoituksen perusteella heikommalta tai paremmalta, kuin mitä se todellisuudessa on tai mihin suuntaan se voi kehittyä, kun uusia haavoittuvuuksia löydetään. Toisaalta yksikin kartoituksessa havaittu

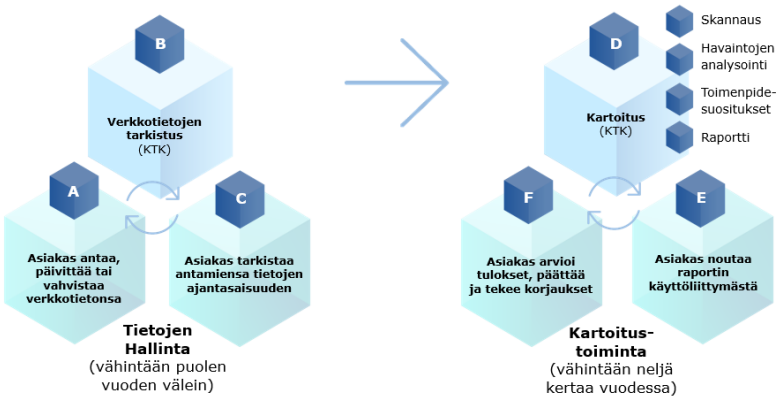
kriittinen haavoittuvuus kriittisessä järjestelmässä voi olla erittäin merkittävä organisaation tietoturvan ja omaisuuden suojaamisen kannalta.

Hyöky-palvelu ei korvaa asiakkaalla käytössä olevia palveluita, vaan sen tarkoitus on täydentää asiakkaan tietoa ja näkemystä ICT-kokonaisuudestaan siihen liittyvän hyökkäyspinnan osalta. Syvällisempi hyökkäyspinnan testaaminen, tulosten tarkastelu, korjaustoimista päättäminen ja niiden toteuttaminen asiakkaan on järjestettävä itse tai yhteistyössä valitsemiensa palveluntarjoajien kanssa.

Asiakkaan antamien tietojen tarkistaminen pitää tehdä asiakaskäyttöliittymässä määräajoittain, jotta voidaan varmistua siitä, että esimerkiksi tiedot kartoitettavista IP-osoitealueista pysyvät ajan tasalla ja että ne kuuluvat edelleen asiakkaalle. Jos asiakas luopuu jostakin IP-osoitteestaan, pitää se poistaa välittömästi organisaatiolle kartoitettavien osoitteiden joukosta asiakaskäyttöliittymässä. Asiakas voi käyttöliittymässä myös lisätä uusia IP-osoitealueita, jolloin ne tulevat kartoitusten piiriin, kun ne on ensin Kyberturvallisuuskeskuksessa tarkistettu ja liitetty kartoituksen kohteeksi. Asiakas vastaa antamiensa tietojen oikeellisuudesta ja niiden tarkistamisesta puolivuosittain.

Käytännössä palvelun toimitus koostuu kahdesta eripituisesta toistuvasta syklistä (kuva 4). Tietojen hallinta tarkoittaa asiakastietojen tarkistusta vähintään puolen vuoden välein. Ajan tasalla olevat verkkotiedot toimivat puolestaan syötteenä nopeampaan tahtiin (neljännesvuosittain) tehtävälle kartoitustoiminnalle. Kartoituksia tehdään vähintään neljä kertaa vuodessa.

Palvelun toistuvat osiot



Kuva 4. Palvelun toistuvat osiot ja niiden aikataulu.

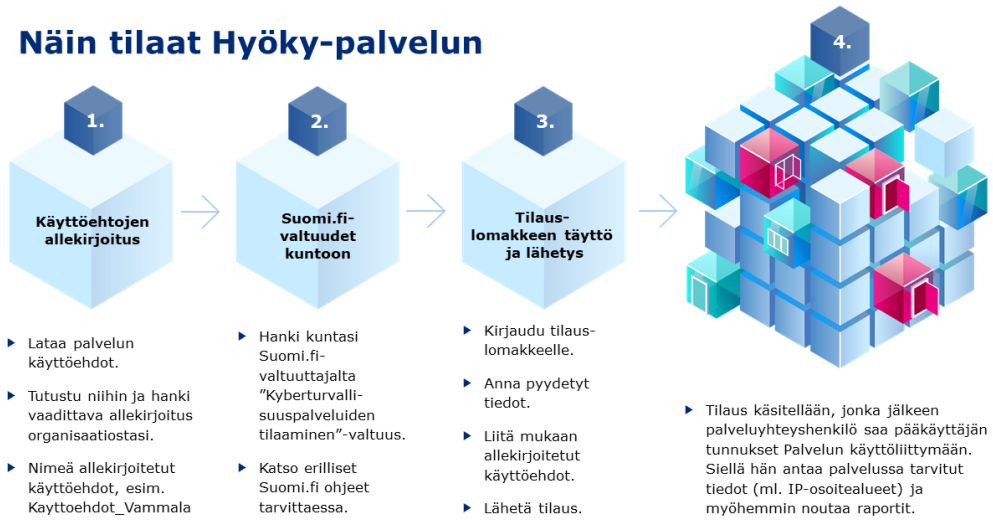
Palvelun toimittaminen voidaan keskeyttää, jos asiakas ei tarkista tietojensa ajantasaisuutta käyttöliittymässä annetussa määräajassa. Tällöin kartoitustoimintaa voidaan jatkaa jälleen, kun tiedot on tarkistettu käyttöehtojen mukaisesti. Luonnollisesti palvelun toimittaminen voidaan keskeyttää myös muista käyttöehdoissa mainituista syistä.

Palvelun irtisanominen voi tapahtua kumman tahansa osapuolen toimesta käyttöehdoissa sovitulla tavalla. Irtisanomisen jälkeen pseudonymisoituja asiakastunnisteita ei enää liitetä uusiin havaintoihin. Aiemmin tallennetut havaintotiedot poistuvat järjestelmästä automaattisesti viiden vuoden kuluttua. Varmuuskopioita tiedoista säilytetään Traficomin käytäntöjen mukaisesti, mikä on tällä hetkellä 10 vuotta.

Kyberturvallisuuskeskus ei takaa tiettyä palvelutasoa Palvelua koskien tai tiedon saatavuutta Hyöky-verkkosivulla. Kyberturvallisuuskeskuksella on oikeus ilman korvausvelvollisuutta tai muuta vastuuta keskeyttää Palvelun tarjoaminen kokonaan tai osittain.

4 Palvelun tilaaminen, käyttöönotto ja käyttäminen

Palvelun tilaaminen tapahtuu asiakkaan toimesta sähköisellä tilauslomakkeella. Lomakkeella annetaan palvelun tuottamisessa tarvittavat yhteystiedot sekä toimitetaan organisaatiossa hyväksytyt ja allekirjoitetut palvelun käyttöehdot. Tilauksen vaiheet pääpiirteissään on kuvattu alla (kuva 5).



Kuva 5. Hyöky-palvelun tilaamisen vaiheet.

Ennen tilaamista tilauslomakkeen täyttäjä tarvitsee Suomi.fi-valtuuden palvelua tilaavalta organisaatiolta. Valtuuden saatuaan hän voi luotetusti tunnistettuna kirjautua lomakkeelle ja edetä tilaamaan palvelun kyseisen organisaation puolesta. Tilauksessa tarvittavan Suomi.fi-valtuuden tunnistetiedot ovat:

- Valtuuden nimi: Kyberturvallisuuspalveluiden tilaaminen
- Kuvaus: Tällä valtuudella valtuutettu voi valtuuttajan puolesta tilata kyberturvallisuuspalveluita ja ilmoittaa
  niissä tarvittavia tietoja, kuten palvelun tuottamisessa tarvittavia yhteystietoja ja verkko-osoitteita.

Palvelun käyttöehdot on hyvä myös ladata ja valmistella ennen tilauslomakkeen täyttämistä, sillä organisaation puolesta allekirjoitetut käyttöehdot liitetään palvelun tilauslomakkeelle.

Käyttöehdot, yksityiskohtaiset tilausohjeet ja linkki tilauslomakkeelle löytyvät palvelun internetsivuilta (ks. kohta 6 Lisätietoa Hyökystä).

Tilaus käsitellään Kyberturvallisuuskeskuksessa tilausten saapumisjärjestyksessä. Palvelutiimi käsittelee tilauksia virka-aikana. Käsittelyn kestoaika riippuu muun muassa tilausjonon pituudesta ja voi kestää arviomme mukaan vuorokaudesta kolmeen viikkoon.

Asiakkuus hyväksytään ja perustetaan tilauksen käsittelyn yhteydessä. Käyttöehtojen mukaisesti Traficomin Kyberturvallisuuskeskuksella on oikeus päättää, mitä kohderyhmiä ja asiakkuuksia se kulloinkin hyväksyy mukaan palveluun. Alkuvaiheessa palvelu on kohdistettu erityisesti kunnille. Myöhemmin palvelua on tarkoitus laajentaa uusille kohderyhmille, kuten muille julkishallinnon organisaatioille ja yhteiskunnan toiminnan kannalta kriittisille organisaatioille.

Palvelun käyttöönottoa ja käyttöä varten tilauksen yhteydessä ilmoitetulle palvelun yhteyshenkilölle luodaan käyttäjätunnukset palvelun asiakaskäyttöliittymään. Kaksivaiheiseen tunnistautumiseen perustuvan kirjautumisen kautta käyttäjä pääsee organisaatiokohtaiseen asiakasnäkymään, jossa hän ilmoittaa kartoituksen piiriin halutut organisaatiolle kuuluvat IP-

osoitealueet asiakaskäyttöliittymässä pyydetyssä muodossa (CIDR, IP-alue (alku- ja loppuosoite) tai yksittäinen IP-osoite). Kun Kyberturvallisuuskeskus on tarkistanut annetut verkkotiedot, ne liitetään mukaan kartoitusten piiriin.

Palvelun käyttäminen tapahtuu asiakaskäyttöliittymän avulla, jonne on ohjaus palvelun internetsivuilta (ks. kohta 6). Siellä asiakas voi ilmoittaa uusia IP-osoiteavaruuksia ja yhteystietoja tai poistaa vanhentuneita tietoja sekä hakea hyökkäyspintakartoitusten raportit tutustuttavakseen. Palvelussa annettujen tietojen oikeellisuus tarkistetaan määräajoin käyttöliittymässä opastetulla tavalla. Alkuvaiheen pelkistettyä käyttöliittymää on tarkoitus kehittää monipuolisempaan suuntaan toiminnoiltaan ja sisällöiltään asiakkailta saamamme palautteen perusteella. Palautetta kerätään palvelun käyttäjiltä eri tavoin, myös asiakaskäyttöliittymän kautta.

5 Hyöky-palvelun kehittäminen

Hyöky-palvelua kehittävät Traficomin Kyberturvallisuuskeskuksen asiantuntijat yhdessä kuntien ja heidän antamansa palautteen avulla. Palvelua on kehitetty ja koekäytetty eri vaiheissa jo noin 60 kunnallisen organisaation kanssa Valtionvarainministeriön hankerahoituksen turvin.

Asiakkaalla on mahdollisuus esittää palautetta ja kehitystoiveita Palvelun kehittämistä kohtaan asiakaskäyttöliittymässä kerrotulla tavalla. Kyberturvallisuuskeskus päättää, mitä kehitystehtäviä toteutetaan ja missä järjestyksessä esimerkiksi perustuen niiden hyödyllisyyteen eri toimijoille, toteutettavuuteen, kustannuksiin ja käytettävissä oleviin resursseihin.

Kehitystyön kohteina voivat olla esimerkiksi kartoitustoiminnon, palvelun sisällön ja toiminnallisuuksien, asiakaskäyttöliittymän, kartoitusraporttien, käyttöohjeistuksen ja muun tukimateriaalin kehitys- ja ylläpitotoimet.

Kehittämiseen kuuluvat erilaisten ominaisuuksien, sisältöjen ja palvelujen testaukset. Palvelussa voi siis olla toiminnallisuuksia, jotka ovat kokeiluvaiheessa. Tällaiset testattavat osiot voivat olla asiakkaiden käytettävissä ilman erillistä maksua, olematta kuitenkaan osa Hyöky-käyttöehtojen mukaista palvelua. Kokeiluvaiheen palvelut tai ominaisuudet voidaan poistaa ilman ennakkovaroitusta.

6 Lisätietoa Hyökystä

Hyöky-palvelun internetsivuilla on saatavissa lisätietoa osoitteessa: https://www.hyöky.fi (osoitteesta ohjaus sivulle: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/hyoky)

Lisätietojen lisäksi sivuilta on löydettävissä esimerkiksi kulloinkin voimassa olevat käyttöehdot sekä ohjaus tilauslomakkeelle ja asiakaskäyttöliittymään.

Palautetta palvelusta, esimerkiksi sen toiminnallisuuksista tai palveluun liittyvistä materiaaleista, ja kehitystoiveita voi lähettää sähköpostitse osoitteeseen hyoky@traficom.fi.