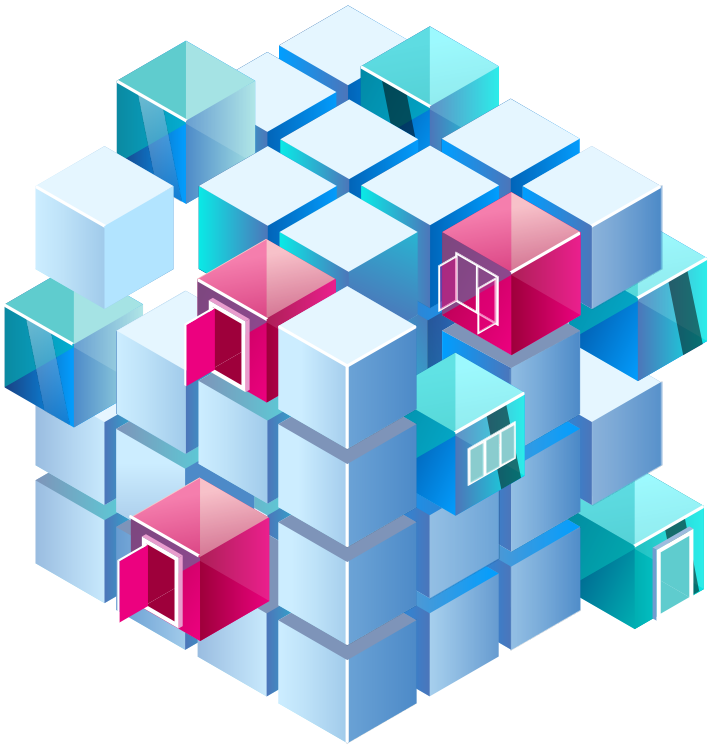
Hyökkäyspinta-alan kartoituspalvelu Hyöky

Palvelukuvaus



Yleinen kuvaus Hyöky -palvelusta

Hyöky on Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen (jäljempänä Kyberturvallisuuskeskus tai lyhenteenä KTK) tuottama kansallinen hyökkäyspintakartoitus kyberturvallisuuden parantamiseksi.

Hyöky-palvelun tarkoituksena on auttaa organisaatioita parantamaan kyberturvallisuuttaan tarjoamalla kohdennettua ja konkreettista havaintoihin perustuvaa tietoa heidän hyökkäyspinnastaan kyberuhkien tunnistamiseksi ja tukea asiakkaalle asetettujen, esimerkiksi lakisääteisten, tietoturvallisuusvelvoitteiden täyttämistä. Palvelun avulla organisaatiot pystyvät tunnistamaan ja suojaamaan kohteitaan etukäteen sekä edistämään omaa toimintakykyään. Lisäksi palvelu edistää kansalaisille tarjottavaa turvallisuutta ja toimintavarmuutta. Palvelua toteuttaa Kyberturvallisuuskeskuksen kumppanina 2NS Cybersecurity Oy.

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 raportin asiakkaan ilmoittamien IP-osoiteavaruuksien ja verkkotunnusten perusteella julkiseen internetiin näkyvien palveluiden muodostamasta organisaatiokohtaisesta hyökkäyspinnasta.

Palvelu on kohdennettu kaikille Suomeen rekisteröidyille organisaatioille ja sitä suositellaan erityisesti NIS2-toimialoihin kuuluville organisaatioille. Palvelun käyttö on maksutonta.

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. Asiakas syöttää palveluun hallinnassaan olevia IP-osoitteita ja verkkotunnuksia, joiden perusteella hyökkäyspinta-alan kartoitukset toteutetaan. 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 kuukausittain, 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.

Hyökkäyspintakartoitusten toteutustapa

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, minkä avulla niihin kohdistuvia kyberuhkia voidaan torjua ennakoivasti.

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.

Kartoitukset toteutetaan ennalta määritetyistä IP-osoitteesta
15.220.172.177 (scanner.prod.asm.2ns.fi).
Palvelulle on nimipalvelussa merkitty TXT-tietueet seuraavasti:

```
scanner.prod.asm.2ns.fi.   text = "note= Traficom NCSC-FI Hyoky scanner"
scanner.prod.asm.2ns.fi.   text = "coordinator=NCSC-FI"
scanner.prod.asm.2ns.fi.   text = "owner=2NS Cybersecurity Oy"
```

Tietoturvallisuus on keskeistä hyökkäyspintakartoitusten toteutuksessa. Kaikki kartoitusjärjestelmän sisältämät havainnot ja palvelun tiedot säilytetään Traficomin ja Traficomin valitseman kumppanin järjestelmässä. Tietojenkäsittely tapahtuu Kyberturvallisuuskeskuksen ja Kyberturvallisuuskeskuksen valitseman kumppanin operoimilla 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 joko turvallisuusselvitettyjen kumppanin asiantuntijoiden tai Kyberturvallisuuskeskuksen asiantuntijoiden toimesta. Hyöky-palvelun tietosuojaseloste on saatavilla palvelun asiakaskäyttöliittymästä.

Hyöky-palvelu asiakkaalle

Kyberturvallisuuskeskuksen suorittamiin tietoverkkojen kartoituksiin perustuen organisaatio voi saada käyttöönsä näkymän omasta hyökkäyspinnastaan. Hyöky-palvelun käyttö ei edellytä asiakkaalta investointeja tai teknisiä toimenpiteitä asiakkaan järjestelmiin. Palvelu sopii organisaatioille, joilla on käytössä julkiseen verkkoon näkyviä palveluita joko omassa ylläpidossa, palveluntarjoajakumppanin operoimana tai esimerkiksi julkisissa tai yksityisissä pilvipalveluissa.

Hyöky-palvelu muodostuu kertaluontoisesta tilausprosessista ja toistuvasta palvelun toimitusprosessista. Pääpiirteissään palvelun toiminta on kuvattu seuraavassa.

Palvelun tilaus ja käyttöönotto erityisesti asiakkaan toiminnan kannalta on kuvattu tarkemmin kohdassa **Palvelun tilaaminen, käyttöönotto ja käyttäminen**

Palvelun toimitus voi alkaa, kun asiakas on antanut tiedot julkisista IP-osoitealueistaan asiakaskäyttöliittymässä hyväksytyssä muodossa. 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 tai esimerkiksi pilvipalveluun. Kyberturvallisuuskeskus tarkistaa verkkotietojen rekisteröintitiedot ennen kartoituspalveluun liittämistä ja saattaa esittää lisätietopyyntöjä niihin liittyen.

Kartoitustoiminta asiakkaan osalta alkaa seuraavasta kartoitussyklistä sen jälkeen, kun verkkotiedot on tarkistettu ja liitetty kartoitusten piiriin. Ensimmäinen kartoitus toteutetaan noin viikon kuluessa verkkotietojen tarkistuksesta. Seuraavan kartoituksen ajankohta on asiakaskäyttöliittymässä nähtävissä ja verkkotietoihin voi tehdä muutoksia ennen seuraavaa kartoitusajankohtaa. Asiakkaan portaaliin rekisteröidyt käyttäjät saavat tiedon sähköpostiin, kun uusi kartoitusraportti on saatavissa. Raportteja tuotetaan asiakkaalle kuukausittain (12 kertaa vuodessa).

Havaintojen analysointi tapahtuu automaattisesti. Analysointi perustuu esimerkiksi asiakkaan palvelimen antamiin versiotietoihin, mistä johtuen jotkut havainnot voivat olla virheellisiä tai puutteellisia ja asiakkaan on 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. Palvelu tuottaa raportin, jossa on kaksi osaa eri tarpeisiin: Yhteenveto-osa tarjoaa helpommin hahmotettavan yleisnäkymän asiakkaan hyökkäyspintaan liittyviin havaintoihin sekä yleisiin suosituksiin havaintojen korjaamiseksi ja hyökkäyspinnan pienentämiseksi. Lisäksi yksityiskohtainen, tekninen osa sisältää yksilöidyt tiedot havainnoista. Lisäksi raportin sisältämä tieto on saatavilla asiakkaan käyttöön teknisen rajapinnan kautta, kuten kuvattu kohdassa **Palvelun tekninen rajapinta**.

Raporttien tarkastelu ja tarvittaessa lataaminen tapahtuu asiakkaalle dedikoidusta käyttöliittymästä palveluportaalissa. Kartoitusraportit on luokiteltu salassapidettäviksi. 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 muita 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 kartoitettavien osoitteiden joukosta asiakaskäyttöliittymässä. Asiakas voi käyttöliittymässä myös lisätä uusia IP-osoitealueita tai aliverkkotunnuksia, jolloin ne tulevat kartoitusten piiriin, kun ne on ensin palvelun toteuttajan toimesta tarkistettu ja liitetty kartoituksen kohteeksi. Asiakas vastaa antamiensa tietojen oikeellisuudesta ja niiden tarkistamisesta vähintään kerran vuodessa.

Palvelun toimittaminen voidaan keskeyttää, jos asiakas ei tarkista tietojensa ajantasaisuutta käyttöliittymässä annetussa määräajassa saamansa muistutuksen seurauksena. 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.

Palvelun tilaaminen, käyttöönotto ja käyttäminen

Palvelun tilaaminen tapahtuu asiakkaan toimesta palvelun käyttöliittymässä olevan rekisteröitymiskäyttöliittymän kautta.

Miten organisaatio rekisteröityy Hyöky-palveluun?

Palvelun käyttö edellyttää organisaation rekisteröitymistä. Rekisteröitymisen yhteydessä tarkistetaan rekisteröijän ja organisaation tiedot palvelun turvallisen ja luotettavan käytön varmistamiseksi.

Rekisteröitymiseen tarvitaan seuraavat tiedot:

Henkilö, jolla on edustusoikeus (nimenkirjoitusoikeus) organisaation puolesta. Tämän henkilön tulee rekisteröinnin yhteydessä tunnistautua suomi.fi -tunnistuspalvelun avulla

Monivaiheisen tunnistautumisen sovelluksen esimerkiksi Microsoft Authenticator (MFA)

Organisaation nimi sekä Y-tunnus

Organisaation NIS2 -toimiala. Vaihtoehdoista valitaan parhaiten organisaation toimintaa kuvaava toimiala.

Organisaation käyttäjien tiedot, jotka tulevat palvelua käyttämään. Henkilöistä tarvitaan etu- ja sukunimen, sekä sähköpostiosoitteen.

Organisaation IP- ja verkko-osoitetiedot, joiden perusteella hyökkäyspinta-alaa kartoitetaan. Osoitteiden ja verkkotunnusten tulee olla organisaatiolle kuuluvia.

Tilaus käsitellään Kyberturvallisuuskeskuksessa tilausten saapumisjärjestyksessä.

Asiakkuus hyväksytään ja perustetaan tilauksen käsittelyn yhteydessä.

Palvelun käyttöönottoa ja käyttöä varten tilauksen yhteydessä tai myöhemmässä vaiheessa palvelun yhteyshenkilö luo itselleen ja organisaationsa muille käyttäjätunnukset palvelun asiakaskäyttöliittymään. Kaksivaiheiseen tunnistautumiseen perustuvan kirjautumisen kautta käyttäjä pääsee organisaatiokohtaiseen asiakasnäkymään, jossa hän ilmoittaa kartoituksen piiriin halutut organisaatiolle kuuluvat IP-osoitealueet tai aliverkkotunnukset asiakaskäyttöliittymässä pyydetyssä muodossa. Kartoituksen piiriin voi ilmoittaa:

- Verkkonimiä – esimerkiksi traficom.fi
- IP-osoitteita – esimerkiksi 192.168.1.1 tai IPv6 osoitteita
- Aliverkkoja – esimerkiksi 192.168.1.0/24

Kun Kyberturvallisuuskeskus tai sen palveluntarjoajakumppani on tarkistanut annetut verkkotiedot, ne liitetään mukaan kartoitusten piiriin.

Palvelun käyttäminen tapahtuu asiakaskäyttöliittymän avulla, jonne on ohjaus palvelun internetsivuilta. Siellä asiakas voi ilmoittaa uusia IP-osoiteavaruuksia ja yhteystietoja tai poistaa vanhentuneita tietoja sekä hakea hyökkäyspintakartoitusten raportit tutustuttavakseen.

Hyöky-palvelun kehittäminen

Hyöky-palvelua kehittävät Traficomin Kyberturvallisuuskeskuksen asiantuntijat yhdessä Traficomin valitseman palvelukumppanin kanssa. Palvelun kehittämisessä huomioidaan Hyöky-palvelun käyttäjien antama palaute.

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.

Palvelun tekninen rajapinta

Hyöky-palvelun kartoitusten tietoja ja tuloksia on mahdollista hakea teknisen rajapinnan (API) kautta. Teknisen rajapinnan käyttöohjeen ja tunnistautumisavaimen voi pyytää Hyöky-asiakaspalvelusta.

Lisätietoa Hyökystä

Hyöky-palvelun internetsivuilla on saatavissa lisätietoa osoitteessa: https://www.hyöky.fi.

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

Palautetta palvelusta, esimerkiksi sen toiminnallisuuksista tai palveluun liittyvistä materiaaleista, ja kehitystoiveita voi lähettää sähköpostitse Hyöky-palvelun asiakaspalveluun osoitteeseen asiakastuki@hyoky.2ns.fi.

Liikenne- ja viestintävirasto Traficom
PL 320, 00059 Traficom
puh. 029 534 5000
traficom.fi