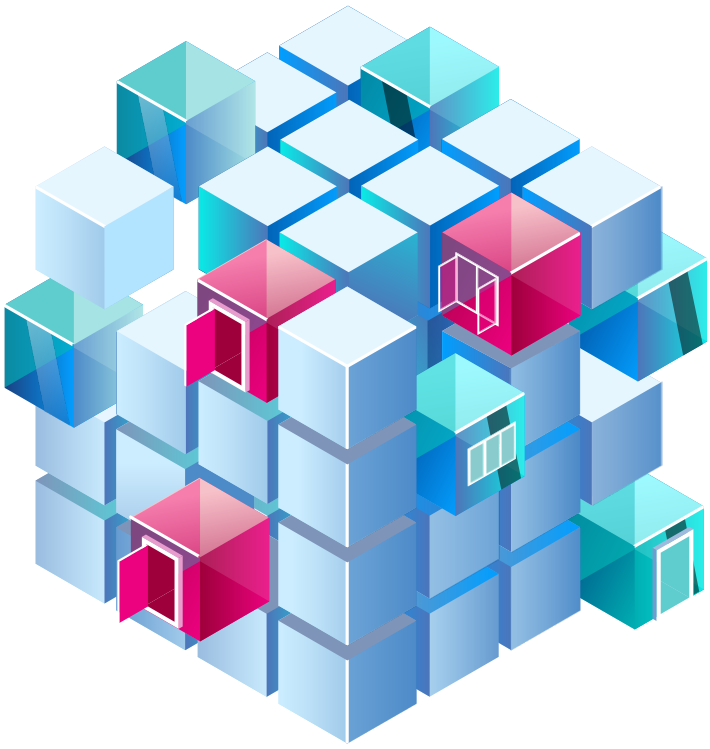
Tjänsten Hyöky för kartläggning av angrepps-ytor

Servicebeskrivning



Allmän beskrivning av Hyöky-tjänsten

Hyöky är en nationell kartläggning av angreppsytan för att förbättra cybersäkerheten, producerad av National Cyber Security Centre Finland (NCSC-FI) vid Finlands transport- och kommunikationsbyrå Traficom.

Syftet med Hyöky-tjänsten är att hjälpa organisationer att förbättra sin cybersäkerhet genom att tillhandahålla riktad och konkret observationsbaserad information om sin attackyta för att identifiera cyberhot och stödja uppfyllandet av informationssäkerhetsskyldigheter som åläggs kunden, såsom de som föreskrivs i lag. Med hjälp av tjänsten kan organisationer identifiera och skydda sina mål i förväg och främja sin egen operativa kapacitet. Dessutom främjar tjänsten säkerheten och tillförlitligheten som erbjuds medborgarna. Tjänsten implementeras av 2NS Cybersecurity Oy som partner till Cybersäkerhetscentret.

En angreppsyta avser svagheter och sårbarheter som kan utnyttjas av en obehörig part, till exempel för att genomföra ett dataintrång eller annan cyberattack. Attackyteintelligens hjälper organisationer att bedöma behovet av åtgärder och genomföra dem på ett riktat och proaktivt sätt. Hyöky-tjänsten producerar en rapport om den organisationsspecifika attackytan som bildas av tjänster som är synliga för det offentliga internet, baserat på de IP-adressutrymmen och domännamn som rapporterats av kunden.

Tjänsten riktar sig till alla organisationer registrerade i Finland och rekommenderas särskilt för organisationer inom NIS2-sektorerna. Tjänsten är kostnadsfri.

Som nationell informationssäkerhetsmyndighet har NCSC-FI en unik syn på informationssäkerhetsmiljön i det finska samhället. Genom internationellt samarbete mellan myndigheter får NCSC-FI även information om globala hot mot informationssäkerhet innan de offentliggörs. Organisationer som använder Hyöky-tjänsten kan använda den information och de tjänster som produceras av NCSC-FI i sitt eget informationssäkerhetsarbete.

I servicemodellen beställer kunden tjänsten från NCSC-FI och accepterar användarvillkoren. Kunden matar in IP-adresser och domännamn under sin kontroll i tjänsten, baserat på vilka kartläggningar av angreppsyta utförs. Efter utplacering kommer organisationen periodiskt att få en kartläggningsrapport om organisationens angreppsyta. Rapporten innehåller en översikt över brister i informationssäkerhet baserad på externa observationer gjorda via ett offentligt informationsnätverk samt en grundläggande rapport om de informationssäkerhetsproblem som upptäckts. Rapporten ger konkret information om möjliga tekniska brister i kundens tjänster, cyberhot mot dem och hur man kan förbereda sig för dem. Kartläggningar genomförs varje månad, vilket gör det möjligt för kunden att följa utvecklingen av organisationens angreppsyta och säkerställa att de korrigerande åtgärder som vidtas lyckas.

Tjänsten inkluderar till exempel inte intrångsförsök i informationssystem eller verifiering och reparation av upptäckta sårbarheter i kundens miljö.

Kunden ansvarar för mer detaljerad bedömning och kartläggning av brister som upptäckts i kartläggningen, samt för beslut och kostnader relaterade till korrigeringen, med hjälp av externa tjänsteleverantörer vid behov.

Hur angreppsytakartläggning implementeras

Implementeringsmetoden för attackytekartläggning baseras på icke-intrusiva metoder. Detta innebär att metoderna som används inte används för att försöka tränga in i kundens system, så kartläggningarna orsakar ingen skada för driften av de system eller tjänster som omfattas av dem. I praktiken innebär driftsmodellen tekniska förfrågningar eller maskinspråkskontakter till ett offentligt tillgängligt kommunikationsnätverk eller informationssystem, tjänst, dess server eller serverapplikation. Automatiserade tekniska kartläggningar som skickas i ett offentligt kommunikationsnätverk används för att samla in information om till exempel tekniska lösningar och de tjänster som tillhandahålls genom dem, såsom programvara som används i kommunikationsnätverk och informationssystem.

Genom att analysera svaren på de frågor som skickas av servrarna är det möjligt att identifiera otillräckligt skyddade eller sårbara lösningar, som kan användas för att proaktivt motverka cyberhot mot dem.

Kartläggningarna använder flera verktyg och datakällor för att göra observationer, berika dem, analysera dem och presentera resultaten. Sådana datakällor kan till exempel inkludera olika uppgifter relaterade till sårbarheter och deras allvar.

Mappningar utförs från fördefinierade IP-adresser
15.220.172.177 (scanner.prod.asm.2ns.fi).
TXT-poster har markerats för tjänsten i namnet service enligt följande:
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"

Informationssäkerhet är centralt för implementeringen av kartläggning av attackytor. Alla observationer och tjänsteinformation som ingår i kartsystemet lagras i Traficoms och en partner som valt ut av Traficom. Databehandling utförs med system som drivs av NCSC-FI och en partner utvald av NCSC-FI, främst med maskin och automation. Identifierarna relaterade till en enskild organisation i systemet är pseudonymiserade, vilket skyddar kundens identitet och kopplingen mellan enskilda observationer och den aktuella organisationen. Utveckling, underhåll och förvaltning utförs antingen av partnerexperter med säkerhetsprövning eller av experter från Cybersäkerhetscentret.
Hyöky-tjänstens integritetspolicy finns tillgänglig i kundens gränssnitt för tjänsten.

Hyöky-service för kunder

Baserat på informationsnätverkskartläggningar som genomförts av NCSC-FI kan en organisation få tillgång till en vy av sin egen attackyta. Användningen av Hyöky-tjänsten kräver inga investeringar eller tekniska åtgärder från kunden i kundens system. Tjänsten är lämplig för organisationer som använder tjänster som är synliga för det publika

nätverket, antingen under eget underhåll, drivna av en tjänsteleverantörspartner eller till exempel i offentliga eller privata molntjänster.

Hyöky-tjänsten består av en engångsbeställningsprocess och en återkommande tjänsteleveransprocess. Tjänstens huvudfunktioner beskrivs nedan.

Beställning och idriftsättning av tjänsten Ur kundens verksamhetsperspektiv beskrivs mer i detalj i avsnittet **Beställa, utplacera och använda tjänsten**

Serviceleverans kan påbörjas när kunden har lämnat information om sina publika IP-adressintervall i ett format som godkänts i kundgränssnittet. Kunden ansvarar för att säkerställa att de aktuella IP-nätverken är tillgängliga för dem och att de har tillstånd att inkludera dem i kartläggningens omfattning, om de är registrerade hos kundens tjänsteleverantör eller till exempel i en molntjänst. NCSC-FI kontrollerar registreringsdata för nätverksdata innan de kopplas till karttjänsten och kan skicka in förfrågningar om ytterligare information relaterad till dem.

Kartläggningsaktiviteter för kunden börjar med nästa kartläggningscykel efter att nätverksdata har kontrollerats och inkluderats i kartläggningens omfattning. Den första kartläggningar kommer att genomföras inom ungefär en vecka efter att nätverksdata har kontrollerats. Tiden för nästa kartläggning kan ses i kundgränssnittet, och ändringar kan göras i nätverksinformationen före nästa kartläggningsdatum. Användare som är registrerade i kundens portal kommer att meddelas via e-post när en ny rapport finns tillgänglig. Rapporter produceras till kunden varje månad (12 gånger per år).

Observationer analyseras automatiskt. Analysen baseras till exempel på versionsinformationen som tillhandahålls av kundens server, vilket är anledningen till att vissa observationer kan vara felaktiga eller ofullständiga, och kunden bör verifiera observationerna i sin egen miljö. Rapporterna åtföljs av mer detaljerade observationsdata så att kunden kan verifiera resultaten, identifiera sårbara servrar och tjänster samt åtgärda eventuella säkerhetsbrister.

Rekommendationer för åtgärder för att rätta till brister relaterade till de vanligaste observationerna genereras automatiskt för rapporten i samband med observationerna. De är på en mycket allmän nivå och tar inte hänsyn till faktorer relaterade till implementeringen av kundens tekniska miljö eller dess lämplighet i mer detalj.

Rapporterna sammanställs från de observationer som gjorts, den relaterade analysen och rekommendationer för åtgärder. Tjänsten tar fram en rapport med två delar för olika behov:
Sammanfattningsavsnittet ger en mer begriplig översikt över kundens observationer av attackytor samt allmänna rekommendationer för att åtgärda resultaten och minska attackytan. Dessutom innehåller den detaljerade, tekniska delen individuell information om observationerna. Dessutom är informationen i rapporten tillgänglig för kunden via ett tekniskt gränssnitt, som beskrivs i avsnittet **Teknisk gränssnitt för tjänsten**.

Rapporterna kan ses och, vid behov, laddas ner från ett dedikerat användargränssnitt i tjänsteportalen. Kartläggningssrapporterna klassificeras som konfidentiella. Kunden kan dock dela information konfidentiellt, till exempel med sin egen tjänsteleverantör, så att utvecklingen av attackytan kan övervakas och förbättras på rätt sätt.

Utvärderingen av kartläggningens resultat bör genomföras i samarbete mellan kundorganisationen och den potentiella IKT-tjänsteleverantören. Resultaten av attackytekartläggningen baseras på tekniska observationer gjorda utanför organisationen, på det publika internetnätverket. Observationerna beskriver hur nätverkets attackyta ser ut ur den externa operatörens perspektiv vid en viss tidpunkt.

Att tolka indikativa observationer i termer av deras faktiska betydelse kräver kunskap om organisationens tjänsteinfrastruktur. Till exempel kan en brist eller ett hot som identifierats i kartläggningen vara lämpligt för implementering av IKT-system eller till exempel baseras på föråldrade mjukvaruidentifierare, även om mjukvaran redan har uppdaterats. Baserat på kartläggningen kan organisationens attackyta se svagare eller bättre ut än den faktiskt är, eller i vilken riktning den kan utvecklas när nya sårbarheter upptäcks. Å andra sidan kan även en kritisk sårbarhet i ett kritiskt system som upptäckts i kartläggningen vara mycket betydande för organisationens informationssäkerhet och tillgångsskydd.
Hyöky-tjänsten ersätter inte andra tjänster som kunden använder, utan dess syfte är att komplettera kundens kunskap och syn på deras ICT-enhet när det gäller den relaterade attackytan.

Mer djupgående testning av attackytan, granskning av resultaten, beslut om åtgärder och genomförande måste ordnas av kunden själv eller i samarbete med de tjänsteleverantörer de valt.

Informationen som tillhandahålls av kunden måste kontrolleras i kundgränssnittet med jämna mellanrum för att säkerställa att till exempel informationen om IP-adressområdena som ska mappas är uppdaterad och fortfarande tillhör kunden. Om kunden ger upp en av sina IP-adresser måste den omedelbart tas bort från listan över mappade adresser i kundgränssnittet. Kunden kan också lägga till nya IP-adressintervall eller subdomäner i användargränssnittet, i vilket fall de inkluderas i mappningarna när de har kontrollerats av tjänsteleverantören och lagts till i kartläggningen. Kunden ansvarar för att informationen är korrekt och för att kontrollera den minst en gång per år.

Leveransen av tjänsten kan avbrytas om kunden inte kontrollerar att deras data är aktuell till följd av en påminnelse som mottagits inom den tidsgräns som anges i användargränssnittet. I detta fall kan kartläggningsaktiviteterna återupptas när data har kontrollerats enligt användarvillkoren. Naturligtvis kan leveransen av tjänsten också avbrytas av andra skäl som nämns i användarvillkoren.

Uppsägning av tjänsten kan göras av någon av parterna på det sätt som överenskommits i användarvillkoren. Efter avslutandet kommer pseudonymiserade kundidentifierare inte längre att kopplas till nya observationer. Tidigare inspelade observationsdata raderas automatiskt från systemet efter fem år. Säkerhetskopior av data lagras enligt Traficoms praxis, som för närvarande är 10 år.

NCSC-FI garanterar inte en specifik servicenivå gällande tjänsten eller tillgången till information på Hyökys webbplats. NCSC-FI har rätt att helt eller delvis avbryta tillhandahållandet av tjänsten utan ansvar eller annat ansvar.

Beställa, utplacera och använda tjänsten

Tjänsten beställs av kunden via registreringsgränssnittet i tjänstens användargränssnitt.

Hur registrerar en organisation sig för Hyöky-tjänsten?

För att använda tjänsten behöver du registrera dig hos din organisation. I samband med registreringen kontrolleras registrantens och organisationens information för att säkerställa säker och pålitlig användning av tjänsten.

Följande information krävs för att registrera sig:

En person som har rätt att företräda (rätt att skriva under) för organisationens räkning. Denna person måste identifiera sig i samband med registreringen med hjälp av suomi.fi identifieringstjänsten

En applikation för multifaktorautentisering , såsom Microsoft Authenticator (MFA)

Organisationens namn och företags-ID

Organisationens NIS2-industri. Bland alternativen väljs den sektor som bäst beskriver organisationens verksamhet.

Information om användarna i din organisation som kommer att använda tjänsten. Du behöver både för- och efternamn samt en e-postadress.

Organisationens IP- och nätverksadressinformation som används för att kartlägga attackytan. Adresser och domäner måste tillhöra organisationen.

Ordern behandlas vid NCSC-FI i den ordning då orderna anländer.

Kundrelationen godkänns och upprättas när beställningen behandlas.

För att kunna distribuera och använda tjänsten skapar servicekontaktpersonen användar-ID för sig själv och andra i sin organisation i kundens gränssnitt vid beställningstillfället eller vid ett senare skede. Genom en inloggning baserad på tvåfaktorsautentisering kan användaren få tillgång till en organisationsspecifik kundvy, där de kan ange IP-adressintervall eller deldomäner som tillhör organisationen och som ska mappas i det format som efterfrågas i klientgränssnittet. Följande kan ingå i kartläggningens omfattning:

- Nätverksnamn – till exempel traficom.fi
- IP-adresser – till exempel 192.168.1.1 eller IPv6-adresser
- Subnät – till exempel 192.168.1.0/24

När NCSC-FI eller dess tjänsteleverantörspartner har kontrollerat den tillhandahållna nätverksinformationen kommer den att inkluderas i kartläggningarnas omfattning.

Användningen av tjänsten sker med hjälp av ett kundgränssnitt, som kan nås från tjänstens webbplats. Där kan kunden rapportera nya IP-adressutrymmen och kontaktuppgifter, eller radera föråldrad information och hämta rapporter om kartläggning av attackytor för granskning.

Utvecklingen av Hyöky-tjänsten

Hyöky-tjänsten utvecklas av experter från Traficoms nationella cybersäkerhetscenter i Finland tillsammans med en tjänstepartner utvald av Traficom. Den feedback som ges av användarna av Hyöky-tjänsten tas i beaktande vid tjänstens utveckling.

Kunden har möjlighet att presentera feedback och utvecklingsönskemål angående utvecklingen av tjänsten enligt beskrivningen i kundgränssnittet. NCSC-FI beslutar vilka utvecklingsuppgifter som ska genomföras och i vilken ordning, till exempel baserat på deras användbarhet för olika aktörer, genomförbarhet, kostnader och tillgängliga resurser.

Målen för utvecklingsarbetet kan inkludera till exempel utveckling och underhåll av kartläggningsfunktionen, tjänstens innehåll och funktioner, kundgränssnittet, kartrapporter, användarinstruktioner och annat stödmaterial.

Utvecklingen inkluderar testning av olika funktioner, innehåll och tjänster. Med andra ord kan tjänsten ha funktioner som befinner sig i testfasen. Sådana sektioner som ska testas kan vara tillgängliga för kunder utan separat avgift, utan att vara en del av tjänsten enligt Hyökys användarvillkor. Tjänster eller funktioner i testfasen kan tas bort utan föregående meddelande.

Teknisk gränssnitt för tjänsten

Data och resultat från kartläggningar i Hyöky-tjänsten kan hämtas via ett tekniskt gränssnitt (API). Användarmanualen för det tekniska gränssnittet och identifieringsnyckeln kan begäras från Hyöky kundtjänst.

Mer information om Hyöky

Mer information finns på Hyökys servicewebbplats på: https://www.hyöky.fi.

Utöver ytterligare information innehåller webbplatsen till exempel de användningsvillkor som gäller vid varje given tidpunkt, samt vägledning om registrering för tjänsten och kundgränssnittet.

Feedback på tjänsten, såsom dess funktioner eller material relaterat till tjänsten, och utvecklingsönskemål kan skickas via e-post till Hyöky-tjänstens kundtjänst på asiakastuki@hyoky.2ns.fi.

Finska transport- och kommunikationsmyndigheten Traficom
PL 320, 00059 Traficom
Tel. 029 534 5000
traficom.fi