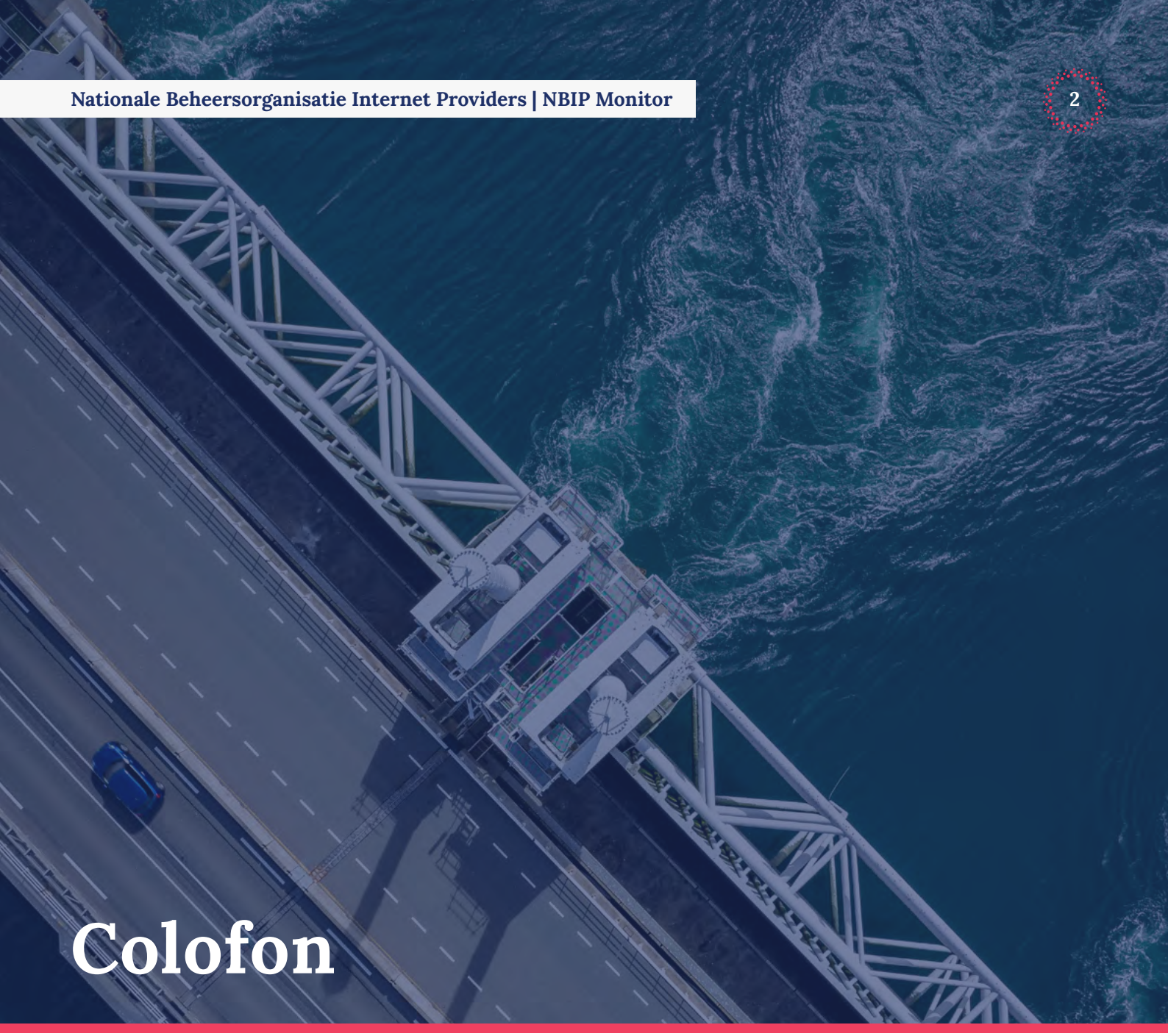
NBIP Monitor

Vernieuwing, inzicht, community & intensivering

NBIP
nationale
beheersorganisatie
internet providers



Colofon

Aan deze uitgave hebben meegewerkt:
Octavia de Weerdt, algemeen directeur, NBIP
Wouter Pegtel, communicatiemanager, NBIP

Met dank aan:
Ludo Baauw, Frans ter Borg,
Michiel Cazemier, Frank Dupker,
Simon Kuhn, Kai Peters

Voor meer informatie, zie www.nbip.nl.

Inhoudsopgave

Samenvatting

De afgelopen twee jaar stonden voor NBIP in het teken van een transitie die ertoe geleid heeft dat NBIP haar diensten nu volledig in eigen beheer uitvoert. NBIP blijft zich daarbij richten op Europese expansie en innovatie. Om diensten door te kunnen ontwikkelen, is ingezet op het verwerven van financiering vanuit Europese fondsen. Voor zowel Clean Networks als deelname aan een consortium in het kader van IPCEI-CIS (Important Project of Common European Interest – Cloud infrastructure and services) is financiering verworven. In het kader van IPCEI-CIS zal NBIP een open en gedistribueerd security platform ontwikkelen.

Ontwikkeling deelnemers

Ook in 2023 mocht NBIP voor zowel de Tapdienst als NaWas weer een gestage groei in het aantal deelnemers noteren.

In totaal hebben we 13 nieuwe deelnemers mogen optekenen. Een uitgebreid overzicht van het aantal deelnemers per dienst is verderop in dit rapport opgenomen.

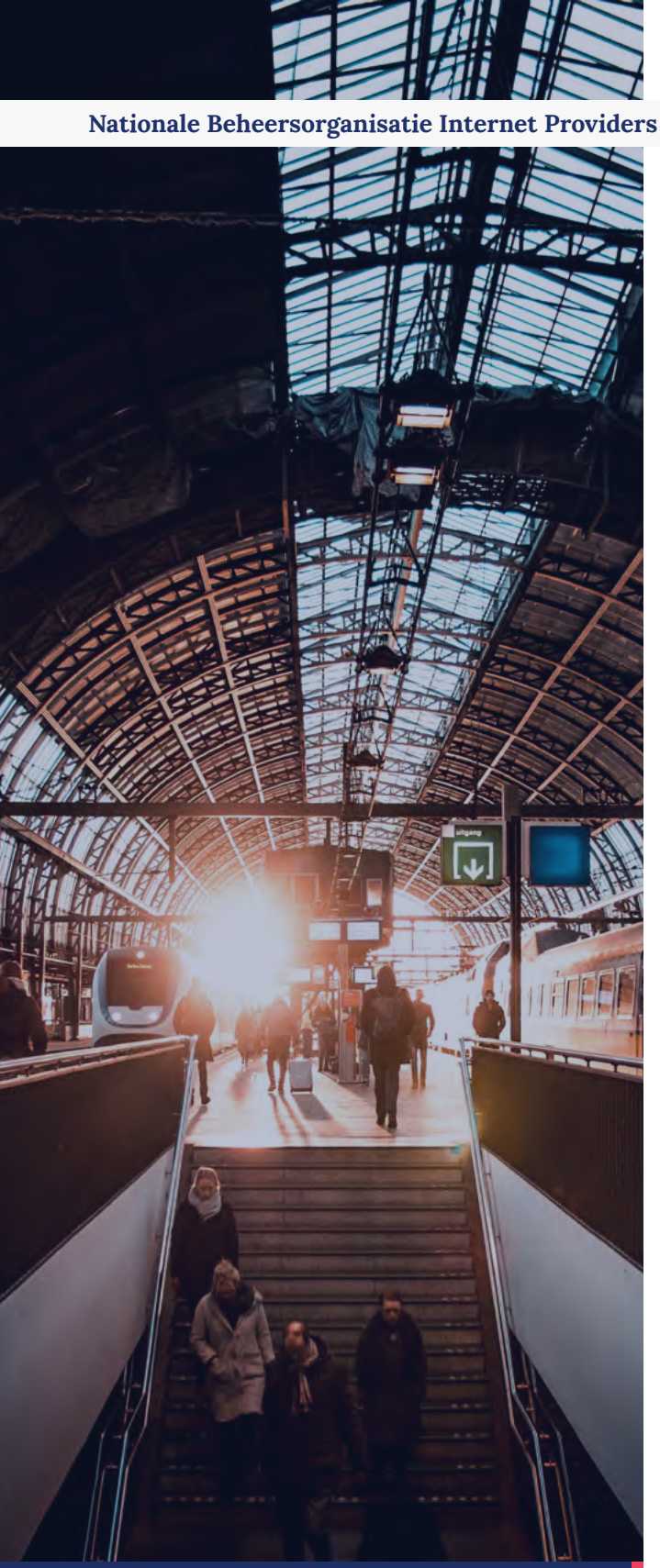
Een organisatie in ontwikkeling

Zowel de doelgroep als het dienstenpakket van NBIP verbreden zich. Kleine en middelgrote hosting-, cloud-, en VoIP-providers, andere aanbieders van digitale infrastructuur, organisaties uit de publieke sector en dienstverleners uit de private sector met een sterke digitale aanwezigheid weten hun weg naar NBIP te vinden. En dat niet alleen in Nederland, maar ook in Europa.

De reden daarvoor is duidelijk: ook organisaties die oorspronkelijk niet als kerntaak het verlenen en faciliteren van digitale diensten hebben, zijn inmiddels zo ver gedigitaliseerd dat zij hun dienstverlening vrijwel uitsluitend nog digitaal aanbieden. Vragen rondom beschikbaarheid en informatiebeveiliging zijn voor hen net zo belangrijk als voor aanbieders van digitale infrastructuur. Om die reden krijgen zij ook vanuit de wetgever te maken met nieuwe verplichtingen.

Dat steeds meer organisaties hun weg weten te vinden naar NBIP, getuigd dan ook van het succes van de coöperatieve insteek van NBIP en haar dienstverlening. Dit zien wij ook bij de Tapdienst terug. Waar NBIP deze dienst lange tijd vooral heeft uitgevoerd voor aanbieders met ixed netwerken, kan NBIP haar diensten ook aan Mobile Virtual Network Operators (MVNO's) aanbieden. We zien daarbij ook interesse vanuit Europa ontstaan. Met de implementatie van de e-evidence verordening in aantocht, ligt het voor de hand dat die interesse in de toekomst toeneemt.

Het fundament is gelegd om de dienstverlening van NBIP te verbreden en intensiveren. De stichting is nu goed voorgesorteerd op de waaier aan aankomende wetgeving waaruit operationele verplichtingen voor providers voortvloeit. Daar waar het logisch is om diensten gezamenlijk te organiseren, wordt onderzocht of dit haalbaar is en of er interesse is vanuit de community.



Toekomstvisie

NBIP richt zich kortom op de verdere ontwikkeling van haar diensten en infrastructuur. Hierbij ligt de focus op ontwikkeling en innovatie, het collectief organiseren van digitale weerbaarheid en op operationele wijze invulling geven aan de naleving van (Europese) wet- en regelgeving. Door het versterken van samenwerkingen en het delen van kennis, wil NBIP bijdragen aan een veiliger digitaal Nederland en Europa. De organisatie streeft ernaar om haar positie als constructieve en waar nodig kritische gesprekspartner voor de overheid en andere stakeholders op het gebied van internetveiligheid verder uit te breiden.

Daarom is NBIP begonnen voor te sorteren op een toekomst die onlosmakelijk gegrond in en verbonden is aan Nederland, maar die ook in toenemende mate Europees zal zijn.

NBIP blijft zich inzetten voor het ondersteunen van haar deelnemers en het bevorderen van een veilige en betrouwbare internetomgeving, waarbij samenwerking en gezamenlijke inspanningen centraal staan.

De organisatie streeft ernaar om haar positie als gewaardeerde gesprekspartner voor de overheid en andere stakeholders op het gebied van internetveiligheid verder uit te breiden.

Woord vooraf

Geachte lezer,

Het is een groot genoegen om u de NBIP Monitor te presenteren. Dit rapport is een beetje anders dan de vorige jaarverslagen die we hebben gepubliceerd, omdat we ervoor hebben gekozen om een algemeen overzicht te geven van de activiteiten van NBIP en de plannen voor de toekomst. Vanaf volgend jaar zullen we weer jaarverslagen publiceren. Zoals velen van u die dit verslag lezen zullen weten, markeren de afgelopen jaren een periode van strategische en operationele veranderingen voor het NBIP. Dankzij deze veranderingen kunnen we met een bloeiende, wendbare organisatie en dienstverlening de toekomst in. Dat is nodig, want er komt veel af op onze achterban, die zich overigens snel uitbreidt. Nieuwe wet- en regelgeving en een gepolariseerde wereld maken waakzaamheid en weerbaarheid steeds belangrijker.

Oog op de toekomst

Alle reden dus om de handen verder en vaker ineen te slaan. De kracht van NBIP heeft altijd gelegen in het gezamenlijk organiseren van operationele naleving van uit de wet voortvloeiende verplichtingen en het versterken van de weerbaarheid tegen cyberdreigingen van deelnemers. Het uitgangspunt is daarbij meer dan ooit dat deelnemers samen sterk staan en vanuit samenwerking een veiliger internet voor iedereen mogelijk maken.

Deze formule blijft aan relevantie winnen. Niet alleen in Nederland, maar ook in Europa. Vanuit de EU komt veel wetgeving op ons af die zal leiden tot nieuwe operationele verplichtingen voor aanbieders van digitale infrastructuur. NIS2 is hiervan een van de bekendste, maar er staat nog meer op stapel. Data, online diensten en de beveiliging daarvan zijn een zaak van geopolitiek en dus Europees belang geworden. De implicaties daarvan zijn juist op operationeel niveau fors.

Op dit snijvlak -de vertaalslag van naleving van wetgeving naar operationele inspanningen- voorzien wij de komende jaren de grootste toegevoegde waarde van NBIP. Daar waar dit kan en duidelijk voordelen oplevert, moeten we digitale weerbaarheid en operationele naleving van wet- en regelgeving gezamenlijk regelen. Zo versterken we elkaar en leggen we rekenschap af van de maatschappelijke impact die onze sector heeft. Zowel de Tapdienst die NBIP biedt als het DDoS-mitigatie platform NaWas zijn vanuit deze filosofie succesvol geworden.

Grip op de eigen operatie

Een van de meest ingrijpende veranderingen de afgelopen jaren was de voltooiing van een transitie waarbij de dienstverlening van NBIP volledig in eigen beheer is genomen. Dit strategische besluit, dat enkele jaren geleden is genomen om meer sturing te krijgen op onze kernactiviteiten, heeft ons in staat gesteld om de operationele efficiëntie en flexibiliteit van onze diensten aanzienlijk te verbeteren.

Daarmee is ook de basis voor een toekomstbestendige organisatie gelegd. Door een eigen team met ervaren medewerkers op te bouwen en kennis intern te ontwikkelen en versterken, staat nu een organisatie die klaar is voor de toekomst. Die toekomst is meer dan de afgelopen 20 jaar onvoorspelbaar. Daarom is het goed om elkaar op te zoeken en gemeenschappelijke uitdagingen gezamenlijk aan te gaan. NBIP neemt dit niet alleen ter hand met haar dienstverlening, maar in toenemende mate ook met kennisdeling en andere vormen van ondersteuning.

Als algemeen directeur van NBIP ben ik trots op de prestaties van ons team en op de steun van onze deelnemers. Samen bouwen we aan een toekomst waarin internetveiligheid en samenwerking centraal staan. Ik nodig u graag uit om verder te lezen over de ontwikkelingen binnen NBIP en vooruit te blikken op de (nabije) toekomst.

Veel leesplezier!

Octavia de Weerdt
Algemeen Directeur
Stichting NBIP

Over NBIP

De Nationale Beheersorganisatie Internet Providers (NBIP) werd in 2001 opgericht door enkele internet providers (ISP's). De stichting werd in het leven geroepen om uitvoering te geven aan de wettelijke aftapverplichtingen die deze ISP's hadden onder de Telecommunicatiewet. Ruim 20 jaar laten bestaat deze zogenoemde Tapdienst nog steeds. Deze dienst voorziet in de behoefte van aanbieders om de naleving van de aftapverplichting uit te besteden aan een professionele organisatie waarbij onafhankelijkheid geborgd is. De stichting bouwt, onderhoudt en beheert de infrastructuur en kennis die nodig is om namens deelnemers uitvoering te geven aan tapvorderingen.

Het coöperatieve model van de Tapdienst heeft in 2014 navolging gekregen met de Nationale Wasstraat (NaWas). Deze collectieve oplossing voor de mitigatie van DDoS-aanvallen is naar hetzelfde model als de Tapdienst opgezet. Het collectieve probleem van DDoS wordt door deelnemers aan de NaWas gezamenlijk aangepakt, waarbij deelnemers naar rato bijdragen aan de instandhouding, onderhoud, vernieuwing en uitbreiding van de dienst. De dagelijkse operatie is in handen van in networking en DDoS gespecialiseerde engineers in dienst van de stichting.

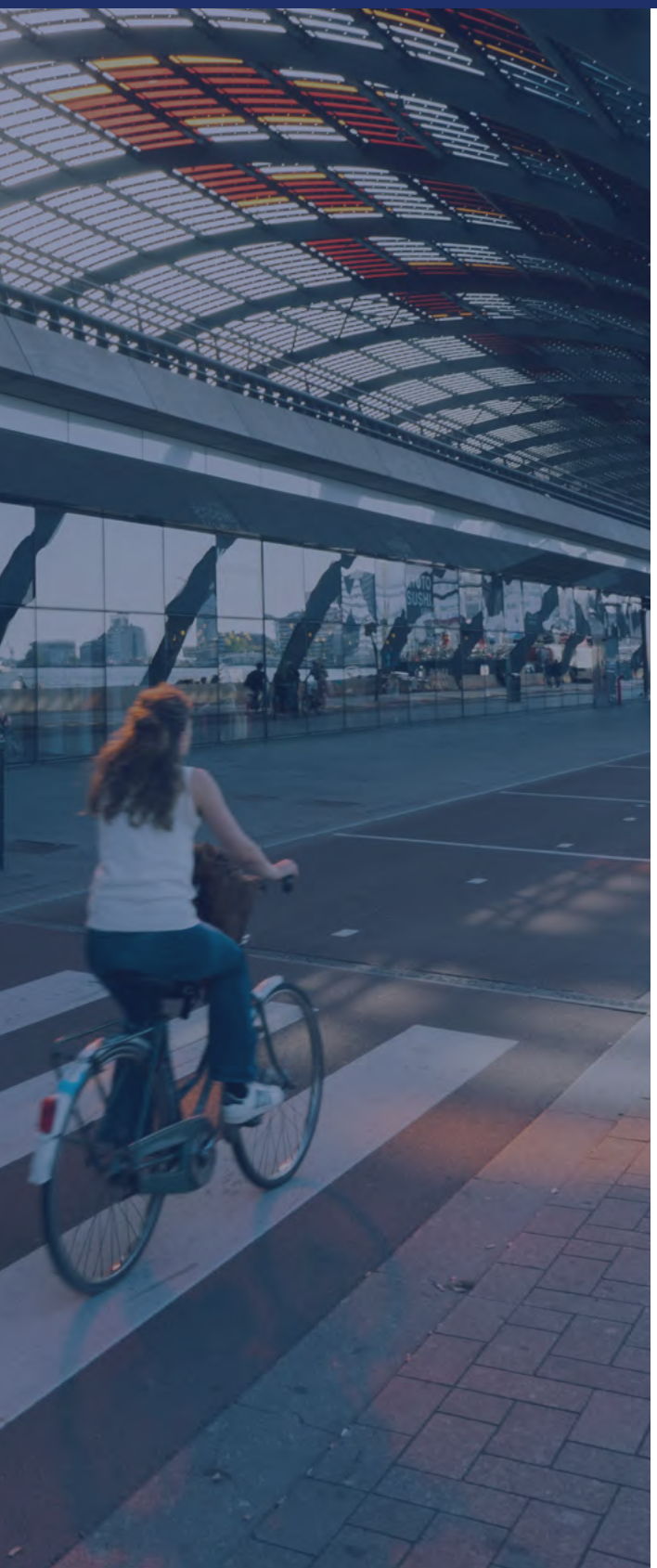
In 2022 is een volgende dienst gelanceerd: Clean Networks. Dit platform informeert deelnemers over beveiligingskwetsbaarheden en abuse zoals botnets of spamservers in hun netwerk. Deelnemers ondertekenen de sectorale Gedragscode Abusebestrijding, sectorbrede afspraken waarmee providers zich committeren aan het voorkomen, opsporen, mitigeren en verwijderen van abuse en kwetsbaarheden in hun netwerk. Clean Networks fungeert tevens als sectorale CSIRT.

Dankzij deze activiteiten heeft NBIP zich ontwikkeld tot expertisecentrum voor lawful interception en lawful disclosure, DDoS en mitigatie daarvan, internet abuse en detectie en mitigatie van beveiligingskwetsbaarheden in de dagelijkse operatie van providers. Er wordt nauw samengewerkt met verschillende partners, waaronder brancheorganisaties, de overheid, coalities en publiek-private samenwerkingen op zowel nationaal als Europees niveau.

De evolutie van NBIP heeft in de loop der jaren ook geleid tot een verbreding van de missie. Alles wat NBIP doet, is vanuit de overtuiging dat de internetsector samen sterker staat voor een schoon, veilig en betrouwbaar internet en dat iedereen daar baat bij heeft.

> *Alles wat NBIP doet, is vanuit de overtuiging dat de internetsector samen sterker staat voor een schoon, veilig en betrouwbaar internet.*

Missie en visie



NBIP biedt aanbieders van digitale infrastructuur en digitale diensten faciliteiten die onmisbaar zijn vanwege weerbaarheid, complaince en wettelijke plichten. Deze faciliteiten zijn niet altijd nodig en kostbaar in aanschaf, operatie en onderhoud. Het is daarom logisch om deze gezamenlijk te exploiteren.

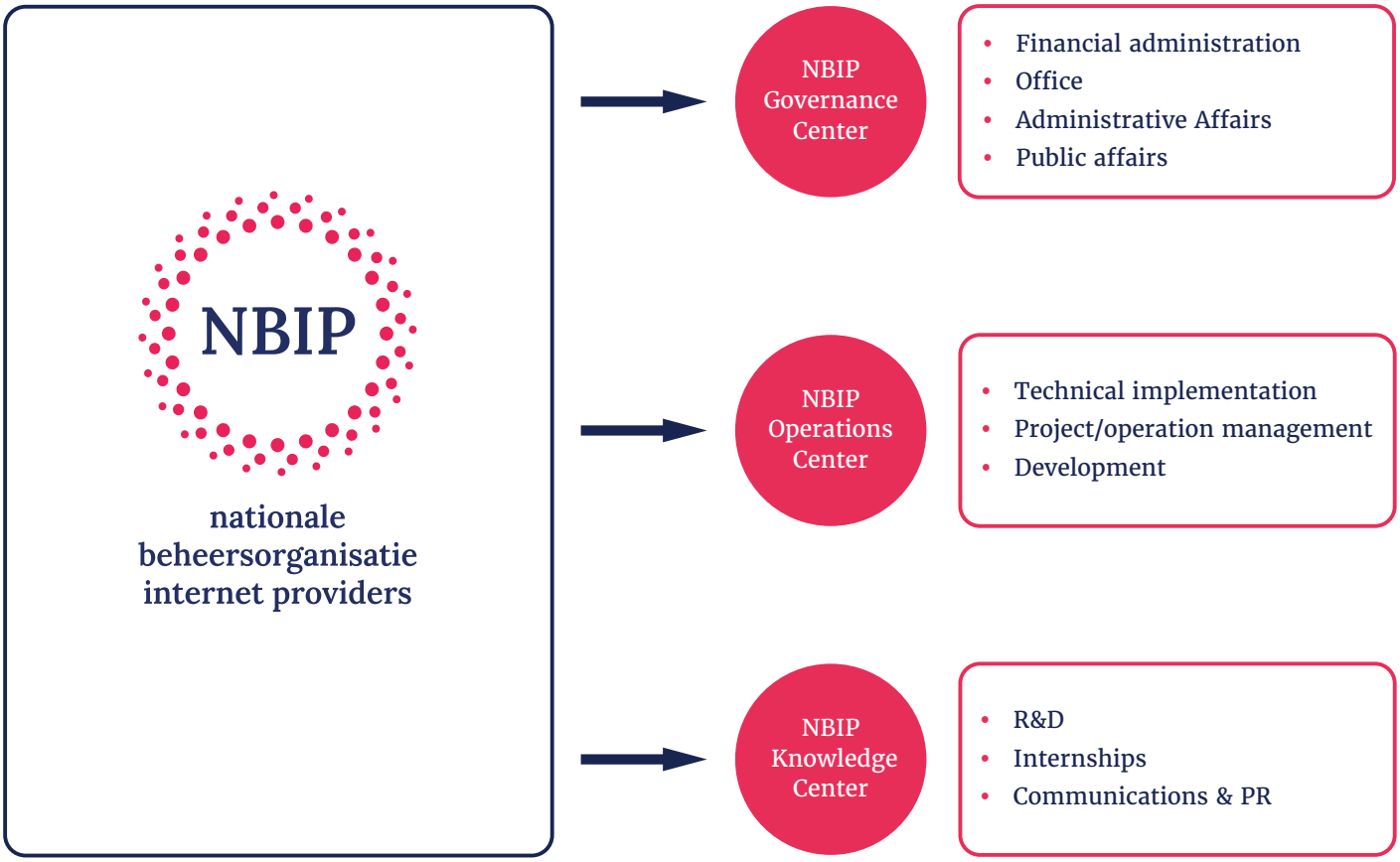
Door krachten, kennis en middelen te bundelen, organiseren deelnemers gemeenschappelijk hun digitale weerbaarheid en operationele naleving van wet- en regelgeving. De diensten die NBIP biedt, zijn voor deelnemers dan ook efficiënter collectief te exploiteren dan individueel. Dankzij deze gezamenlijke aanpak hebben zowel grote als kleine aanbieders op een laagdrempelige en kostenefficiënte manier hun zaken op orde.

Het beginsel dat samenwerking helpt om sterker te staan, staat ook aan de basis van de non-profit opzet van NBIP. NBIP levert professionele diensten vanuit de gedachte dat een betrouwbaar internet een gezamenlijke verantwoordelijkheid is, en werkt daarom zonder winstoogmerk om dit doel te bereiken. Daarom werken we iedere dag aan een betrouwbaar internet voor alle gebruikers, ondersteund door een sterke gemeenschap van samenwerkende aanbieders van digitale infrastructuur.

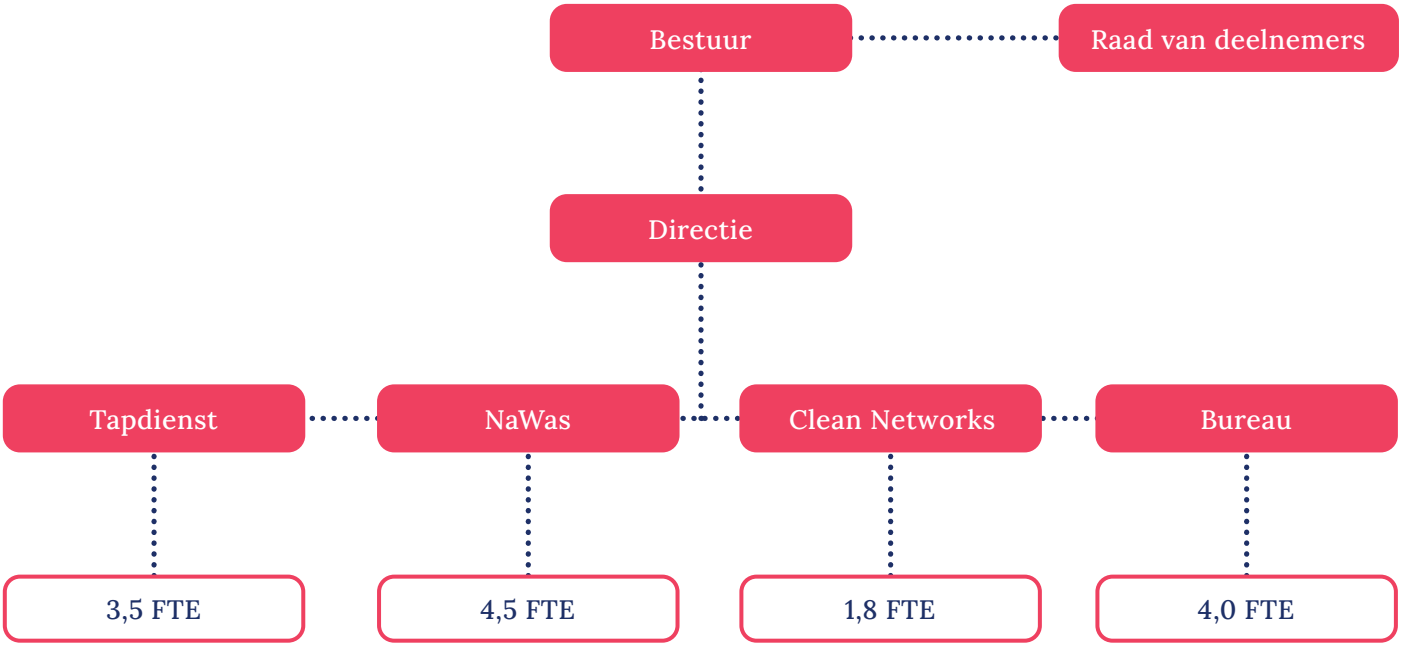
Organisatiestructuur

De diensten van NBIP worden geleverd vanuit een Operations Center, van waaruit dagelijks wordt gewerkt om de continuïteit van de diensten aan deelnemers te waarborgen. Het NBIP Governance Center levert ondersteunende diensten voor de NaWas, Tapdiensten en Clean Networks, waaronder financiële administratie, administratieve taken en bestuursondersteuning.

Het NBIP Knowledge Center is onder meer belast met ontwikkeling van zowel kennis, techniek als medewerkers. Extern is het kenniscentrum erop gericht zowel deelnemers als de bredere internetgemeenschap maar ook overheid, media en het bredere publiek te informeren over domeinen waarop NBIP actief is. Te denken valt aan technische informatie over DDoS mitigatie, maar ook laagdrempelige uitleg over hoe een DDoS-aanval werkt, of bijvoorbeeld de aanpak van bad hosters.



Organogram



Het bestuur van NBIP is samengesteld uit bestuursleden die ieder voortkomen uit een individuele deelnemer van NBIP. Het bestuur is verantwoordelijk voor de vorming van beleid, financiële controle en verantwoording, een behoedzame omgang met de stichting en de belangen van deelnemers die er in verenigd zijn.

Het bestuur wordt benoemd door de Raad van Deelnemers, waarin alle deelnemers van NBIP vertegenwoordiging hebben. Zij kunnen bij monde van de voorzitter van de Raad van Deelnemers het bestuur kritisch bevragen en gevraagd en ongevraagd van advies voorzien. De voorzitter van de Raad van Deelnemers heeft inzage in notulen van bestuursvergaderingen en heeft als een van de belangrijkste taken om namens deelnemers onderwerpen te agenderen bij het bestuur. De Raad van Deelnemers is statutair het hoogste orgaan binnen NBIP.

De directie van NBIP is verantwoordelijk voor de uitvoering van het beleid zoals vastgesteld door het bestuur en legt verantwoording af over behaalde resultaten. De algemeen directeur is verder autonoom binnen de uitgezette kaders om haar opdracht uit te voeren.

De algemeen directeur geeft leiding aan vier operationele afdelingen: Tapdienst, NaWas, Clean Networks en het Bureau, waar ondersteunende functies zoals financiële administratie, projectadministratie en -management, communicatie & PR en public affairs zijn ondergebracht. Elk van deze diensten heeft tenminste een medewerker die zelfstandig maar in nauw overleg met de directie de afdeling als meewerkend voorman of -vrouw aanvoert.

Bestuurssamenstelling

Ludo Baauw
Voorzitter

Ludo Baauw is voorzitter van stichting NBIP. Als voorzitter leidt hij het bestuur en ziet samen met hen toe op de koers van de stichting. Hij staat in nauw contact met onder meer de Raad van Deelnemers, andere stakeholders en partners in de branche. In het dagelijks leven is hij CEO van IMG (Intermax Group).

Rick Sulman
Vice-voorzitter & algemeen bestuurslid

Rick Sulman is algemeen bestuurslid en vice-voorzitter NBIP. Als bestuurslid speelt hij een rol in de governance van de organisatie en houdt hij zich bezig met toezicht op ethisch, transparant en effectief bestuur. Rick ziet toe op de belangen van VoIP providers binnen de stichting. In zijn dagelijkse werk is hij CEO van telecom operator Speakup B.V.

Tjebbe de Winter
Penningmeester

Tjebbe de Winter is penningmeester van NBIP. Hij ziet als penningmeester toe op de financiële gezondheid en stabiliteit van NBIP. Met meer dan 25 jaar ervaring in ISP-technologie en netwerken, kan hij goed de technische afwegingen en consequenties van de financiële plaat doorzien. Tjebbe is één van de oprichters en directeuren van Cyso Group.

Mike Janssen
Algemeen bestuurslid

Mike Janssen is algemeen bestuurslid bij NBIP. Hij zet zich in voor een veilige digitale infrastructuur. Mike richt zich op strategische besluitvorming en versterkt samenwerkingen om cybersecurity-uitdagingen zoals DDoS-aanvallen, gezamenlijk aan te pakken. Mike is CIO bij ITQ en houdt zich daar bezig met de algemene en digitale strategie.

Namens het bestuur Ludo Baauw

Voorzitter

Ludo Baauw is voorzitter van het bestuur van NBIP en CEO van Intermax Group, waaronder bij het ter perse gaan van dit jaarverslag acht IT-bedrijven vallen Hij waakt er samen met de andere bestuursleden voor dat NBIP op koers blijft bij haar schakelfunctie tussen ISP's, hosting providers, telecombedrijven en andere aanbieders van digitale infrastructuur en diensten.

Wat waren de afgelopen periode de belangrijkste thema's voor het bestuur van NBIP?

"Er stonden verschillende belangrijke thema's op de agenda. Een van de voornaamste ontwikkelingen was de intensivering van het contact met de deelnemers. Dit uitte zich onder andere in de zoektocht naar een nieuwe voorzitter voor de Raad van Deelnemers, wat dit jaar resulteerde in de benoeming van Frans ter Borg.

Daarnaast lag de focus op verdere professionalisering van de organisatie. Concrete voorbeelden hiervan waren de respectievelijk de voorbereiding op en de start van twee belangrijke projecten: MISD (Modular Intergrated Sustainable Datacenter) onder de vlag van IPCEI-CIS en Clean Networks. Het IPCEI CIS-project is gericht op het vergroten van de Europese autonomie en soevereiniteit op het gebied van data en cloudinfrastructuur en diensten. MISD draagt hier aan bij door een concept en field lab te ontwikkelen voor moderne, efficiënte modulaire datacenters voor een gedistribueerde cloudinfrastructuur. De NBIP bouwt hierbij voort op haar ervaring met de 'wasstraat' en onderzoekt mogelijkheden om secure by design open source-oplossingen te ontwikkelen als alternatief voor commerciële apparatuur.

Het Clean Networks-programma speelt in op de toenemende eisen van de overheid aan service providers, ISP's en telecombedrijven. Het doel is om kwetsbaarheden en onrechtmatigheid zo snel mogelijk van netwerken te verwijderen. Wij kunnen daar als NBIP een cruciale rol in vervullen. Deze projecten illustreren de kernfilosofie van de NBIP: 'Alleen ga je sneller, maar samen kom je verder.' Ze stellen de organisatie in staat om initiatieven te ontplooien die voor individuele deelnemers niet haalbaar zouden zijn.

En natuurlijk hebben we onze tapdiensten uitgevoerd en verder ontwikkeld. Onze meer dan 100 deelnemers hebben allemaal hun verplichtingen volgens de Telecommunicatiewet aan NBIP 'uitbesteed' en dagelijks is hier een hele club mensen bezig die waar nodig uitrukken met 'tapdozen' om op verzoek van politie, justitie of veiligheidsdiensten de verplichting namens de deelnemers secuur uit te voeren, met de hoogste vorm van vertrouwelijkheid."

De dienstverlening van NBIP werd volledig in eigen handen genomen Waarom is hiervoor gekozen en wat heeft dit opgeleverd?

"Na meer dan 20 jaar intensief te hebben samengewerkt met externe leveranciers, hebben we de strategische keuze gemaakt om de dienstverlening volledig zelfstandig uit te gaan voeren. Deze keuze werd vooral ingegeven door de aanzienlijke groei van de organisatie en het toenemende belang van onze werkzaamheden. We hebben zo meer controle over onze operaties en zijn minder afhankelijk van derden. Dat is cruciaal, gezien de politieke en maatschappelijke relevantie van ons werk. Bovendien heeft de organisatie nu een schaalgrootte bereikt waarbij het kostenefficiënter is om bepaalde activiteiten intern uit te voeren.

Deze verandering heeft verschillende voordelen opgeleverd voor de deelnemers. Ten eerste is er nu een intensiever en directer contact tussen de

deelnemers en het NBIP-bureau, waardoor het mogelijk is om sneller in te spelen op de behoeften van de deelnemers. Daarnaast kunnen we nu flexibeler en sneller nieuwe features ontwikkelen, omdat we beschikken over eigen mensen met de benodigde expertise. Uiteindelijk heeft het er mede toe geleid dat we, ondanks de toenemende kosten en inflatie in de buitenwereld, erin zijn geslaagd om de tarieven voor deelnemers vrijwel gelijk te houden."

Wat is de visie van het bestuur voor de komende jaren?

"We hebben als bestuur een ambitieuze visie voor de toekomst. Een belangrijk speerpunt is het benutten en delen van de opgedane kennis en expertise. We streven ernaar om de apparatuur die nu nog commercieel wordt ingekocht, te vervangen door open source-alternatieven. Dit past in het streven naar meer digitale soevereiniteit voor Nederland en Europa.

We willen ons als NBIP bovendien verder ontwikkelen als een gewaardeerde gesprekspartner voor de overheid op het gebied van internetveiligheid, waarbij de nadruk ligt op een gezamenlijke, Europese aanpak in plaats van afhankelijkheid van niet-Europese partijen. Het unieke model van de NBIP als non-profit, community-based DDoS wasstraat krijgt bijvoorbeeld steeds meer interesse vanuit Europa. Die positie willen we verder uitbouwen en uitbreiden. De groei van het aantal internationale deelnemers onderstreept de relevantie van dit model. Op lange termijn zien we mogelijkheden voor de ontwikkeling van een kwaliteitsstempel of keurmerk. Dit zou de waarde van NBIP-deelnemerschap voor ISP's en telecombedrijven verder kunnen vergroten in hun interacties met de overheid en andere stakeholders."

Wat maakt de internetsector als community zo sterk en het werk voor de NBIP zo dankbaar?

"De kracht van de internetsector als community ligt in de gezamenlijke aanpak van uitdagingen die voor individuele partijen te complex of kostbaar zouden zijn om alleen aan te gaan. De NBIP fungeert als een verbindende factor die de kennis, middelen en belangen van haar deelnemers bundelt. Deze samenwerking stelt zelfs kleinere spelers in de markt in staat om te voldoen aan steeds strengere wet- en regelgeving en om gebruik te maken van geavanceerde diensten zoals de DDoS wasstraat.

Wij vervullen hierin een belangrijke rol als vertaler tussen de overheid en de sector, waarbij we praktische oplossingen bieden voor vaak complexe vereisten. Het werk voor de NBIP is bijzonder dankbaar omdat het een tastbaar verschil maakt. Door gezamenlijk op te treden, krijgt de sector een krachtige stem richting de overheid en andere stakeholders. Dit stelt ons in staat om de belangen van onze deelnemers effectief te behartigen en zo bij te dragen aan een veiliger en stabieler internet."

Waar ben je trots op?

"Er zijn verschillende aspecten van het werk van de NBIP waar ik met recht trots op ben. Allereerst is er de succesvolle transitie naar een organisatie die haar dienstverlening volledig zelf uitvoert en ontwikkelt. Ondanks de complexiteit van deze verandering is de dienstverlening aan onze deelnemers ononderbroken doorgegaan. Dit is een groot compliment aan het hele team, onder leiding van Octavia de Weerdt.

Daarnaast ben ik trots op onze positie als de eerste en grootste non-profit anti-DDoS wasstraat ter wereld. Dit unieke model trekt wereldwijd de aandacht en laat zien dat een coöperatieve aanpak in de internetsector zeer effectief kan zijn. Maar ook ons vermogen om toptalent aan te trekken, zelfs in een krappe arbeidsmarkt, zegt iets over onze organisatie. Het feit dat ervaren professionals kiezen voor de NBIP vanwege onze maatschappelijke impact, onderstreept de relevantie van ons werk.

Tot slot ben ik trots op de sterke community die we hebben opgebouwd. De NBIP belichaamt de Nederlandse traditie van samenwerking, vergelijkbaar met coöperaties in andere sectoren. Deze gemeenschapszin stelt ons in staat om grote uitdagingen aan te gaan en een betekenisvolle bijdrage te leveren aan een veiliger en betrouwbaarder internet voor iedereen."

Ontwikkeling diensten

Tapdienst

De tapdienst is de langstlopende dienst van NBIP en helpt aanbieders van openbare telecommunicatie-diensten en -netwerken om te voldoen aan verplichtingen uit de Telecommunicatiewet.

Overzicht van de Tapdiensten

NBIP fungeert als een centraal loket voor deelnemers bij het aannemen van vorderingen die bedoeld zijn voor aangesloten deelnemers. In de praktijk betekent dit dat justitie, politie en veiligheidsdiensten contact zoeken met NBIP als zij een vordering hebben voor een deelnemer aan de Tapdienst. NBIP draagt vervolgens zorg voor de technische, juridische en administratieve aspecten van deze verzoeken. Wanneer een opsporingsdienst een lastgeving uitvaardigt, beoordeelt NBIP de rechtmatigheid hiervan en verzorgt zij de implementatie van de tap. Dit proces omvat zowel de plaatsing van tapsystemen als het beheer van de interceptie gedurende de looptijd van de tap. Dit geldt ook voor verzoeken rondom het leveren van gegevens van verschillende aard. Dit alles gebeurt met strikte naleving van de wetgeving en onder strenge veiligheidsmaatregelen om de vertrouwelijkheid en integriteit van de gegevens te waarborgen.

> *NBIP biedt haar deelnemers uitgebreide ondersteuning op het gebied van internetveiligheid en wettelijke naleving.*

Enkele belangrijke ontwikkelingen

1.Toename in aansluitingen en dekking: NBIP heeft haar tapdiensten verder uitgebreid, met nu meer dan 100 deelnemers, waaronder nieuwe ISP's en VoIP-providers. Deze groei is deels gestimuleerd door aangescherpte wetgeving en strengere controles door de Rijksinspectie Digitale Infrastructuur (RDI), wat leidde tot een grotere vraag naar compliance oplossingen.

2.Technische infrastructuur en innovatie: een belangrijke mijlpaal was de voltooiing van het in eigen beheer nemen van alle kernactiviteiten. Dit omvatte de herinrichting van de technische infrastructuur en processen, waardoor NBIP nu beschikt over een dedicated tapkamer. Deze tapkamer is voorzien van moderne beveiligingssystemen en is 24/7 operationeel, wat de responstijd en betrouwbaarheid van de tapdiensten aanzienlijk heeft verbeterd.

3.Europese samenwerking en wetgeving: NBIP heeft haar expertise die is opgedaan met de tapdienst ook op Europees niveau mogen inbrengen. Met de verwachte implementatie van de nieuwe Europese e-evidence wetgeving, die het mogelijk maakt dat opsporingsdiensten uit andere EU-landen rechtstreeks gegevens kunnen opvragen bij Nederlandse providers en vice versa, speelt NBIP een actieve rolin de werkgroepen van de Europese Commissie om deze ontwikkelingen in goede banen te leiden.

4.Uitbreiding van diensten en educatie: naast de traditionele tapdiensten heeft NBIP gewerkt aan de uitbreiding van haar dienstenportfolio, waaronder het afhandelen van diverse justitiële vorderingen en de koppeling met het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT). Deze uitbreiding zorgt ervoor dat deelnemers volledig compliant zijn met alle wettelijke eisen en biedt hen een geïntegreerde oplossing voor hun verplichtingen richting opsporingsdiensten.

NaWas

De **Na**tionale **Was**straat tegen DDoS-aanvallen

Overzicht van de NaWas-dienst

De NaWas beschermt aanbieders van digitale infrastructuur met een eigen netwerk (AS) tegen DDoS-aanvallen. Vervuild verkeer wordt omgeleid naar een beveiligde omgeving, gefilterd en als schoon verkeer teruggestuurd naar de oorspronkelijke bestemming. Dit waarborgt de continuïteit van de dienstverlening voor zowel providers als hun klanten.

Enkele belangrijke ontwikkelingen

1. **Uitbreiding en redundantie:** een van de belangrijkste mijlpalen in 2023 was de fysieke uitbreiding van de NaWas infrastructuur naar Kopenhagen. Deze uitbreiding verhoogt de redundantie en zorgt voor een robuustere bescherming tegen DDoS-aanvallen door meerdere geografische locaties te benutten. De keuze voor Kopenhagen was strategisch vanwege de sterke connectiviteit en de aanwezigheid van een actieve internetgemeenschap die vraagt om lokale DDoS-bescherming.

2. **Technische ontwikkelingen:** NBIP heeft geïnvesteerd in de upgrade van haar technische infrastructuur, waaronder de vervanging van verouderde apparatuur door moderne systemen. Een voorbeeld is de vervanging van de DDoS-detectie oplossing die NaWas inzet, die in 2023 in gang is gezet. Ook is verkend hoe de connectiviteit van NaWas geoptimaliseerd kan worden. Dit soort upgrades verbeteren de mogelijkheden en efficiëntie van de NaWas, waardoor snellere en effectievere mitigatie van DDoS-aanvallen mogelijk is. Ook zijn er verbeteringen doorgevoerd in load balancing en data sharing tussen verschillende locaties, wat de veerkracht van het netwerk verder versterkt.

3. **Europese projecten en samenwerkingen:** NBIP heeft actief deelgenomen aan de aanvraag van financiering in het kader van Europese R&D-projecten die onder meer gericht zijn op de bouw van een veilige, gedistribueerde edge cloudinfrastructuur in Europa. NBIP legt zich daarbij onder meer toe op de ontwikkeling van edge cybersecurity oplossingen. Dit project, dat wordt ondersteund door Europese subsidies, zal de komende jaren een belangrijke focus blijven. Het doel is om een open platform te creëren voor bijvoorbeeld DDoS-detectie en mitigatie dat niet alleen door NBIP, maar door meerdere Europese entiteiten gebruikt kan worden. Dit bevordert de digitale autonomie en vermindert afhankelijkheid van commerciële, niet-Europese aanbieders.

4. **Groei in deelnemers:** het aantal deelnemers aan de NaWas-dienst is verder gegroeid, met nu zo'n 130 aangesloten partijen. Verwacht wordt dat deze groei de komende jaren doorzet, mede door de implementatie van NIS2 (Cyberbeveiligingswet) en andere wetgeving waarmee eisen worden gesteld aan de aantoonbaarheid van de maatregelen voor beschikbaarheid van digitale diensten en het beperken van de economische en maatschappelijke schade als dit soort diensten verstoord worden. De hierboven genoemde upgrades en uitbreidingen hebben ook tot doel om voldoende capaciteit voor deze groei paraat te hebben.

Clean Networks

Clean Networks is een initiatief dat internet, hosting- en cloudproviders helpt om hun netwerken schoon te houden van zogenoemd abuse. Hiermee bedoelen we zowel het misbruik van beveiligingskwetsbaarheden en systemen voor illegale activiteiten zoals spam of ransomware als onrechtmatige content.

Overzicht Clean Networks

Veel abuse vindt plaats in systemen van internet- en hostingproviders omdat zij grote netwerken hebben met soms wel duizenden servers, waarbij het lastig is om goed zicht te houden op de kwetsbaarheden die (bij klanten) voorkomen. Daarnaast is er een groep providers voor wie dit soort abuse een blinde vlek is. Zij zijn onbewust onbekwaam.

Clean Networks richt zich daarom op twee aspecten. Enerzijds bestaat het uit een door de sector breedgedragen Gedragscode die providers ondertekenen. Daarmee verbinden zij zich onder meer aan het treffen van maatregelen om abuse in hun netwerken op te sporen en beveiligingskwetsbaarheden te verhelpen. Zij verbinden zich ook aan een notice & takedown procedure, 'know your customer' beleid en een goede bereikbaarheid voor abusemeldingen. Ondertekenaars van de Gedragscode onderscheiden zich in positieve zin van vergelijkbare partijen die dat niet doen, doordat zij aantoonbaar maken dat zij abuse opsporen en uit hun netwerken verwijderen. Om dit onderscheid duidelijk te maken krijgen zij een certifi aat en op den duur een keurmerk.

Het tweede aspect van Clean Networks is technisch van aard. Het Clean Networks platform biedt deelnemers geautomatiseerde meldingen van kwetsbaarheden in hun netwerk. Het biedt daarbij in veel gevallen handelingsperspectief om deze kwetsbaarheden op te lossen. Het platform bundelt daarbij dreigingsinformatie uit verschillende bronnen zoals Shadowserver en CERT-Bund.

Doorontwikkeling

Clean Networks is in 2023 na een succesvolle lancering in 2022 verder ontwikkeld. Er is onder meer gewerkt aan een betere gebruikerservaring en het toevoegen en automatiseren van meldingen uit aanvullende bronnen. Eind 2023 verstrekte het platform uit 25 bronnen informatie aan deelnemers.

In de nabije toekomst zal Clean Networks het aantal ondertekenaars van de gedragscode aanzienlijk vergroten, omdat dit het doel van een schoner internet snel dichterbij brengt. Daartoe wordt een intensieve campagne gelanceerd om het bewustzijn en de bereidheid om aan te sluiten bij Clean Networks te vergroten.

Het nieuwe systeem werkt efficiënter en veiliger. Het zorgt ervoor dat gegevens sneller en betrouwbaarder worden verwerkt, wat de algehele dienstverlening ten goede komt.

Interview Kai Peters

Engineer NBIP

Kai Peters is Engineer bij NBIP, gespecialiseerd in technische aspecten van de tapomgeving Met een brede achtergrond in ICT, variërend van helpdesk tot systeembeheer, draagt zijn expertise bij de efficiënte en veilige uitvoering van complexe technische projecten van NBIP.

Waar houd jij je binnen NBIP mee bezig?

"Ik werk aan het technische gedeelte van de tap-omgeving binnen NBIP. Een belangrijk project waar we mee bezig zijn, is de overstap naar een nieuw systeem voor live interception. We hebben een volledige nieuwe omgeving naast de oude gebouwd met de laatste versies van het LI-systeem, een ander OS en nieuwe beveiligingen. In het nieuwe systeem kunnen tapdiensten volledig nog verder geautomatiseerd worden via een message broker, waardoor veel handwerk verleden tijd is. Bovendien verhoogt dat de efficiëntie en verbetert het de veiligheid."

Wat merken deelnemers hiervan?

"De meeste deelnemers zullen weinig merken van de overgang naar het nieuwe systeem, omdat het zo is ontworpen dat ze naast elkaar kunnen draaien. Wij zullen tijdens de migratie dezelfde servers gaan uitrijden, maar met andere software waar de deelnemers verder niets van merken. Het nieuwe systeem werkt efficiënter en veiliger. Het zorgt ervoor dat gegevens sneller en betrouwbaarder worden verwerkt, wat de algehele dienstverlening ten goede komt."

Wat zijn de grootste uitdagingen op het gebied van de tapdienst?

"De grootste uitdagingen bij de tapdienst draaien om de ingewikkelde, verschillende netwerken en de beveiliging van gegevens. Elke deelnemer heeft een uniek netwerk met verschillende structuren, waardoor het lastig is om een goede locatie te vinden om taps in te richten en uit te voeren."

Hoe waarborg je de veiligheid van gegevens tijdens taps?

“De veiligheid van onze tapdienst wordt op meerdere manieren gegarandeerd. Alle gegevens die worden getapt, worden eerst versleuteld voordat ze worden verzonden, zodat alleen bevoegde personen er toegang toe hebben. Hierdoor blijven de gegevens beschermd tegen ongewenste toegang. Daarnaast zijn er strikte toegangscontroles, en slechts een klein aantal mensen heeft toegang tot het systeem. Deze mensen hebben een Verklaring Omtrent het Gedrag (VOG) en een geheimhoudingscontract getekend. Zelfs onderling wordt hier op de werkvloer niet inhoudelijk gepraat over de taps. Bovendien wordt er niets opgeslagen op de harde schijven van de systemen bij de deelnemers. Zodra een systeem wordt uitgeschakeld, verdwijnen alle gegevens die kunnen verwijzen naar een tap. Elke gegevensstroom en elk target wordt versleuteld met een unieke sleutel, waardoor de gegevensstromen strikt gescheiden blijven.”

Welke toekomstige ontwikkelingen kunnen we verwachten voor de tapdienst?

“Een van de belangrijkste veranderingen is de virtualisatie van de tap-servers. Dit houdt in dat de fysieke servers die nu bij de deelnemers staan, vervangen kunnen worden door virtuele machines. Hierdoor wordt niet alleen ruimte en geld bespaard, maar wordt het systeem ook flexibeler en makkelijker te onderhouden.

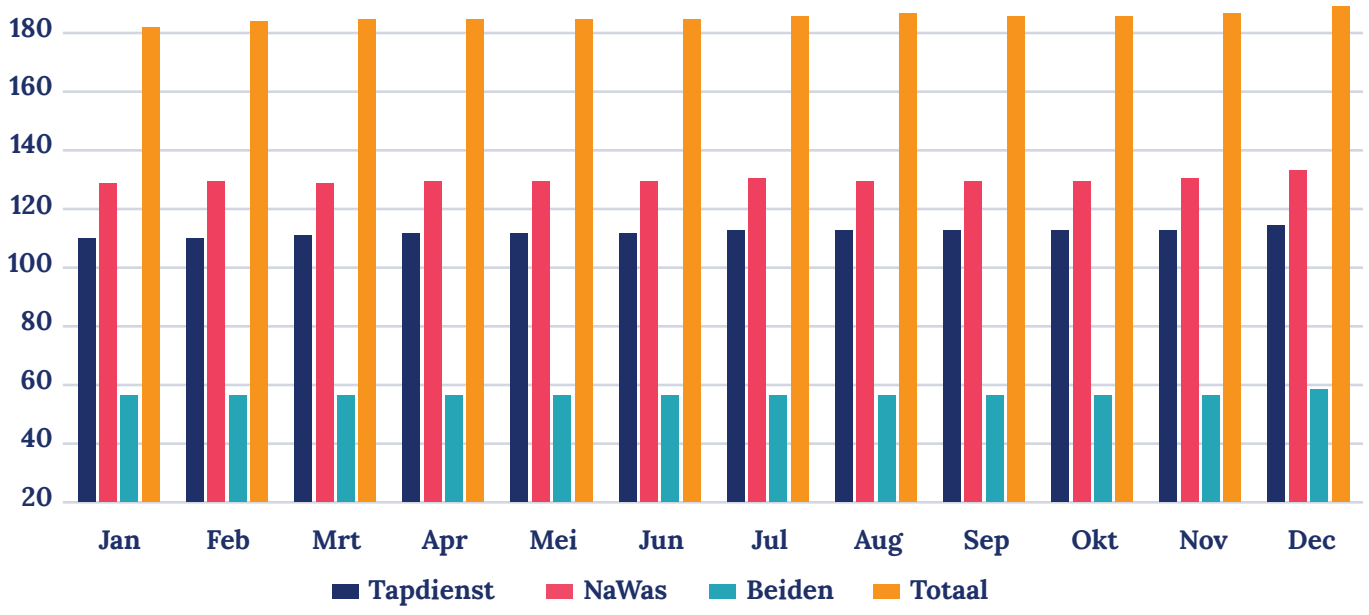
Waar ben je het meest trots op in je werk?

“Ik ben het meest trots op hoe snel ik me heb kunnen ontwikkelen sinds ik bij NBIP werk. In korte tijd heb ik mijn kennis over lawful interception en lawful disclosure en de architectuur van systemen daarvoor, flink kunnen verdiepen. Ook het feit dat we tijdens de migratie naar het nieuwe systeem verschillende technische uitdagingen hebben overwonnen zonder dat dit impact had, maakt me trots.”

Ontwikkeling deelnemers

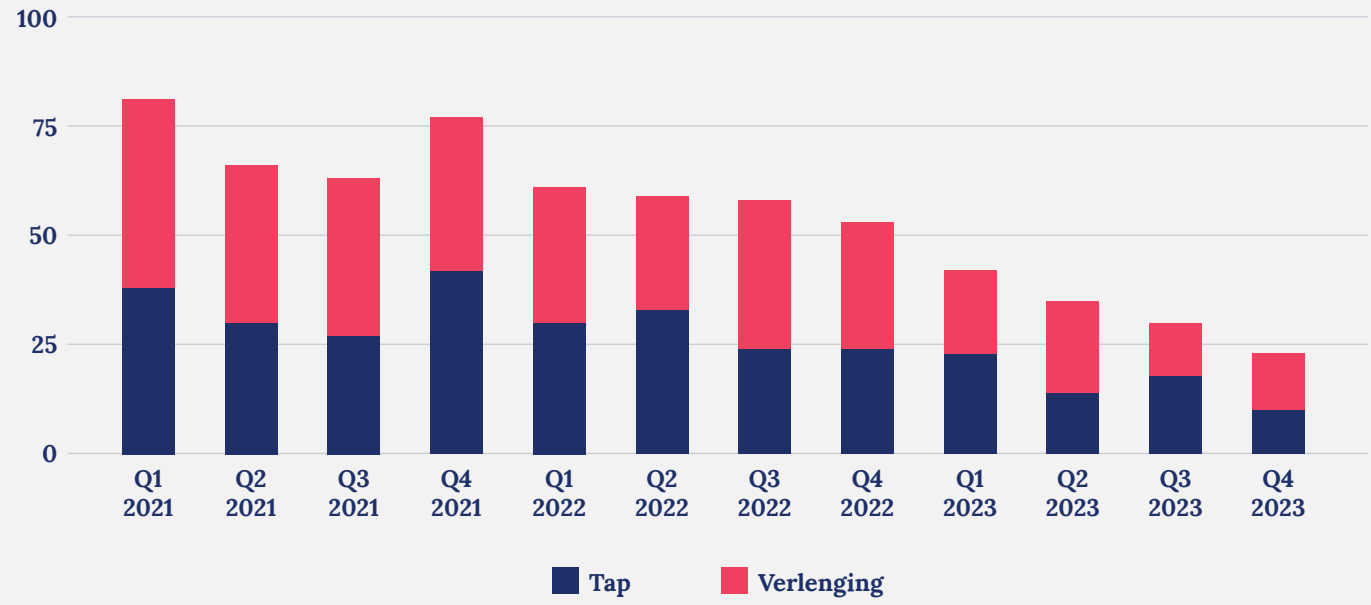
Het aantal deelnemers van NBIP is ook in 2023 weer gegroeid. Het aantal tapdienstdeelnemers groeide met vijf, terwijl het aantal NaWas-deelnemers met negen groeide. Eén deelnemer zegde deelname aan de Tapdienst op. In totaal groeide het aantal deelnemers aan de diensten met dertien. Organisaties die zowel van de Tapdienst als de NaWas gebruikmaken, worden in het totaal aantal deelnemers van NBIP als een enkele deelnemer geteld. Zo bezien had NBIP eind december 2023 190 deelnemers, waarvan 104 organisaties deelnemen aan de Tapdienst en 129 organisaties deelnemen aan de NaWas. Er zijn 43 organisaties die deelnemen aan beide diensten.

	Jan	Feb	Maa	Apr	Mei	Juni	Juli	Aug	Sept	Okt	Nov	Dec
Tapdienst	101	101	102	103 (+1)	103	103	104 (+1)	104	104	104	104	106 (+2)
NaWas	122	123 (+1)	123	123	123	123	124 (+1)	123 (-1)	123	123	124 (+1)	127 (+3)
Beiden	41	41	41	41	41	41	41	41	41	41	41	43 (+2)
Totaal	182	184	185 (+1)	185	185	185	186	187	186 (-1)	186	187	190 (+3)

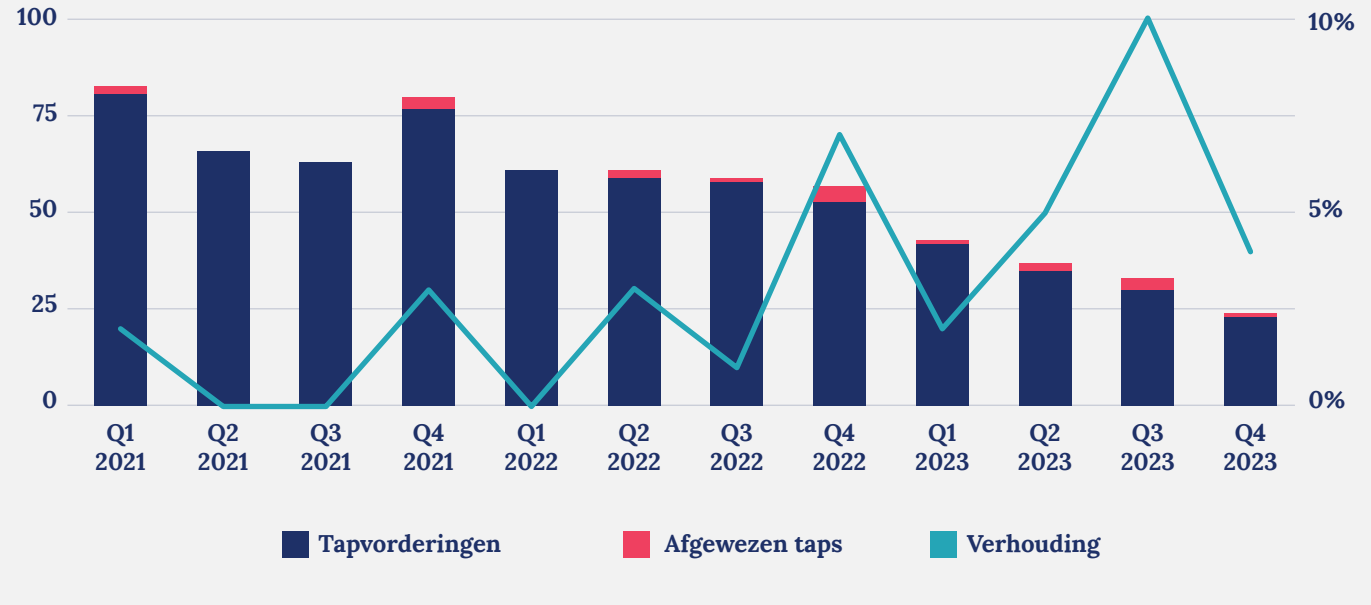


Tapdienst cijfers 2023

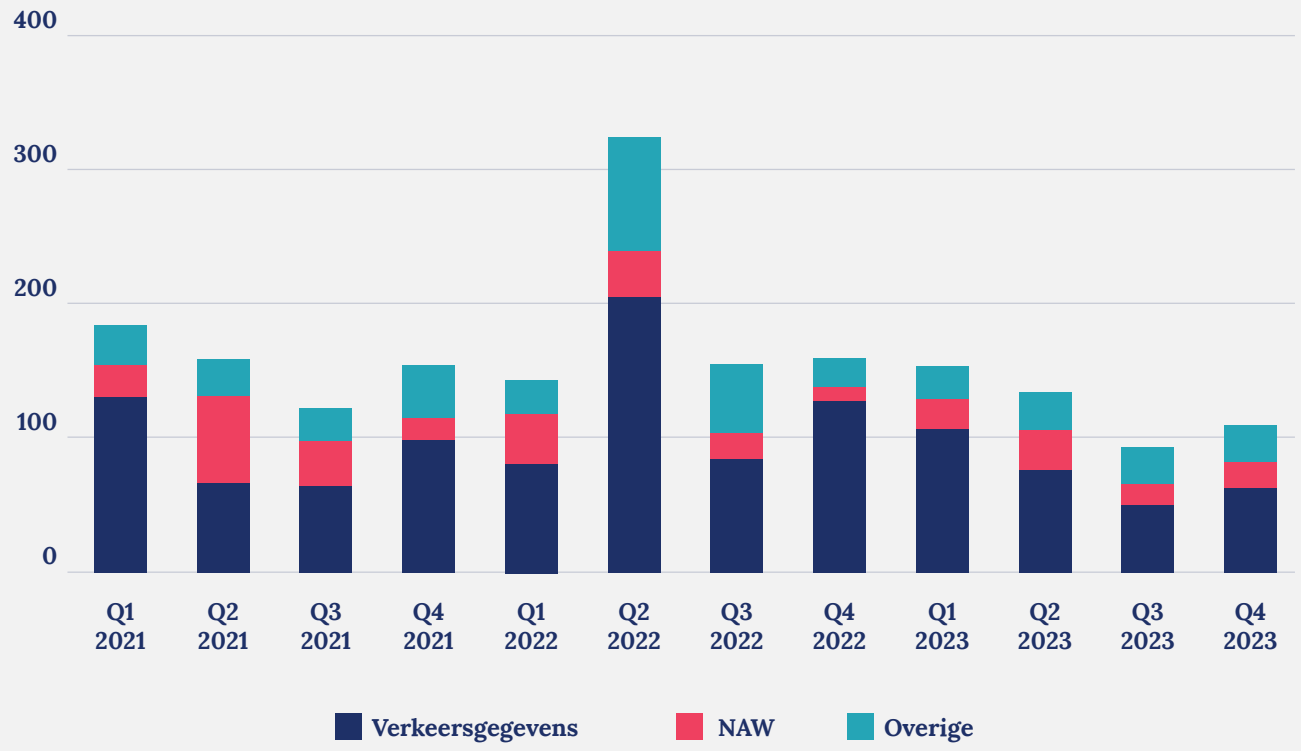
Taps en verlengingen per kwartaal



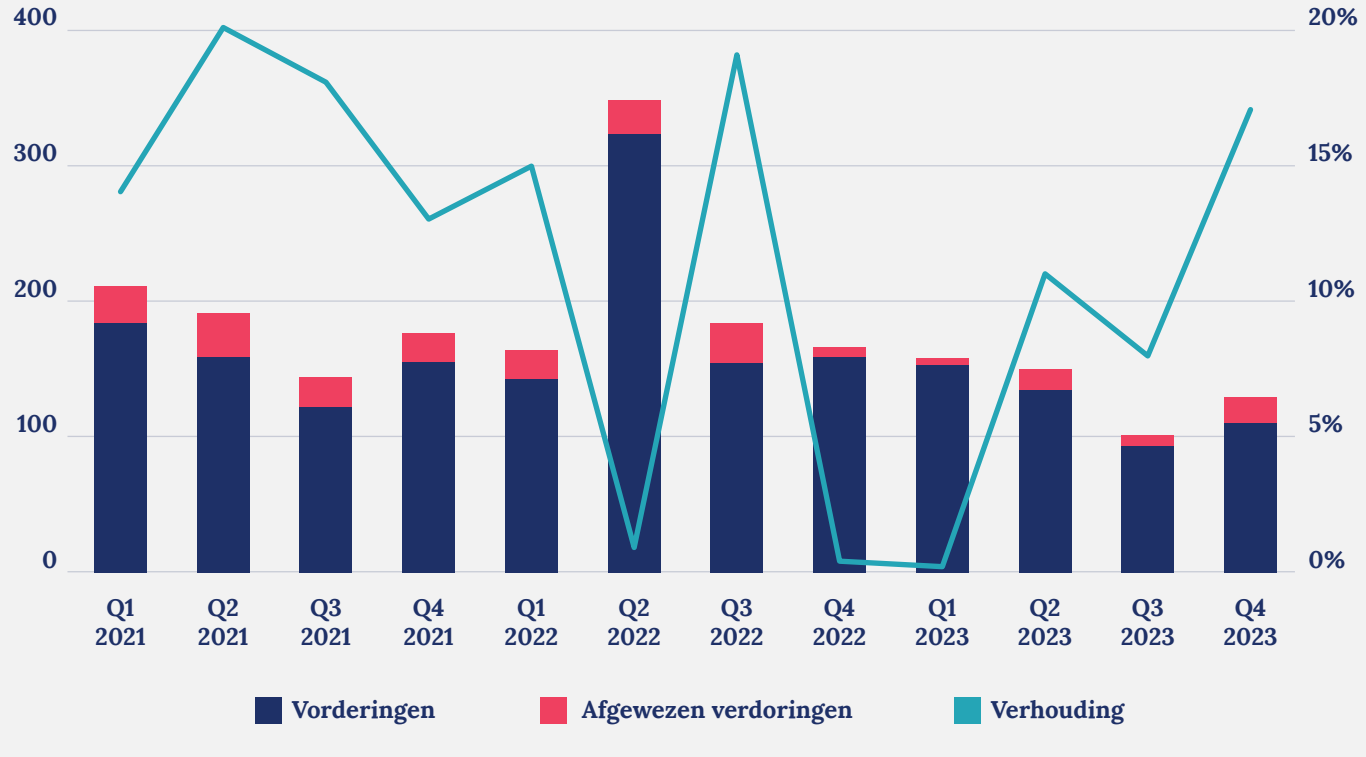
Tapvorderingen versus afgewezen



Overige vorderingen per kwartaal



Vorderingen versus afgewezen

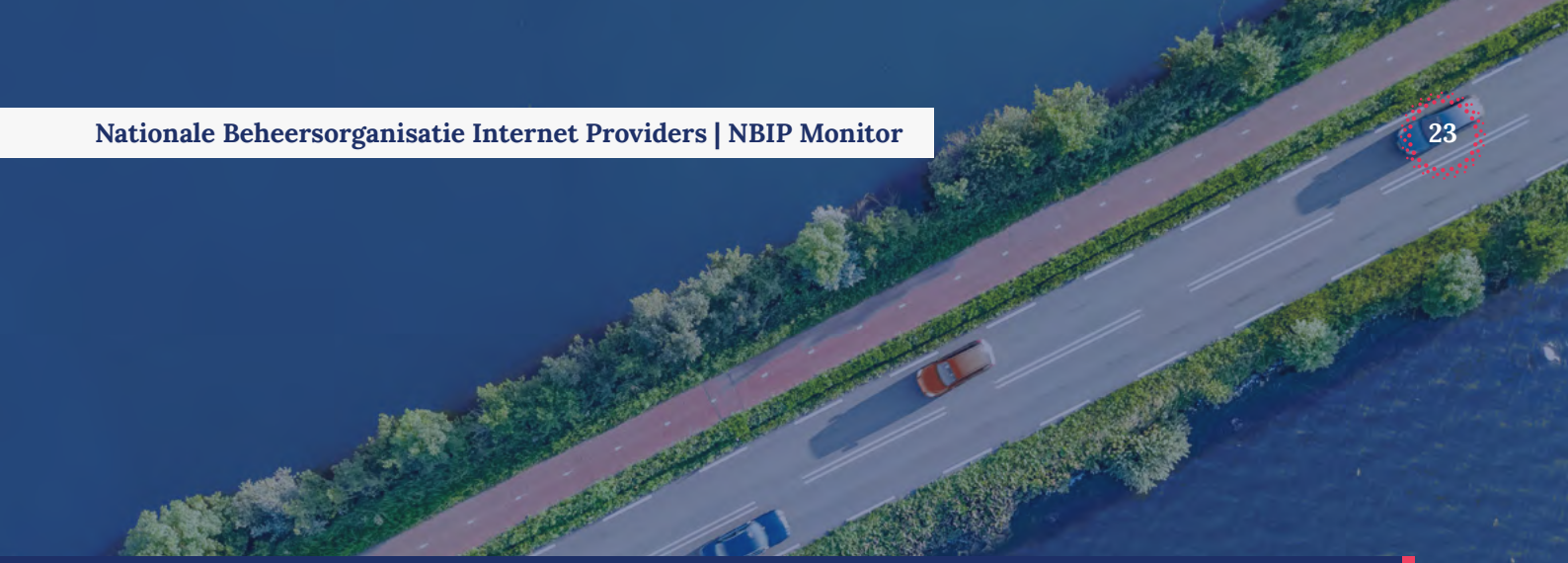


NaWas cijfers 2023

De NaWas statistieken over 2024 worden beschikbaar gemaakt in het jaarverslag 2024, dat in de eerste helft van 2025 zal verschijnen.

2023	Kwartaal 1	Kwartaal 2	Kwartaal 3	Kwartaal 4
< 1 Gbps	205	146	140	212
1 - 10 Gbps	410	213	300	376
10 - 20 Gbps	26	26	35	43
20 - 40 Gbps	20	13	15	28
> 40 Gbps	15	10	15	19

2023	Kwartaal 1	Kwartaal 2	Kwartaal 3	Kwartaal 4
< 15 min	337	200	293	361
15-60 min	242	121	124	204
1-4 uur	71	51	49	78
> 4 uur	26	36	39	35



Verwachte ontwikkelingen Tapdienst

In de komende jaren ligt de focus van NBIP op een transformatie en uitbreiding van de tapdienst, waarbij innovatie en Europese regelgeving centraal staan. De term 'Tapdienst 2 0' symboliseert deze evolutie, waarbij het niet enkel meer gaat om uitvoeren van (tap vorderingen, maar om een bredere service die inspeelt op de groeiende en veranderende eisen van toezichthouders en de wetgeving

Een van de kernonderdelen van deze transformatie is de ontwikkeling van een uitgebreider loket. Dit loket kan dienen als centraal punt waar bevragingen van toezichthouders binnenkomen en beoordeeld worden voordat ze uitgevoerd worden. Dit loket zal breder worden opgezet om meerdere bevragingen, afkomstig van verschillende organisaties met uiteenlopende mandatering, adequaat te kunnen behandelen. Deze uitbreiding sluit aan bij de eisen van onder andere de ATKM en e-evidence wetgeving. Hierdoor kan NBIP haar deelnemers beter ondersteunen in het voldoen aan nieuwe verplichtingen die voortvloeien uit wet- en regelgeving.

De e-evidence verordening en bijbehorende richtlijn zorgen voor een harmonisatie van het proces voor digitale opsporingsverzoeken. Dit betekent dat NBIP moet zorgen voor een infrastructuur die klaar is om een groot aantal bevragingen te verwerken, niet alleen van nationale, maar ook van internationale, Europese behoeftestellers. De uitdaging hierbij is om een laagdrempelig en efficiënt systeem te creëren dat direct aansluit bij de behoeften van zowel de behoeftestellers als internetproviders. De inzet op een gedecentraliseerd systeem moet ervoor zorgen dat deze bevragingen sneller en eenvoudiger verwerkt kunnen worden, wat leidt tot een hogere efficiëntie en betere naleving van de wetgeving.

Naast de praktische implementatie van nieuwe regelgeving, richt NBIP zich ook op het versterken van haar infrastructuur en dienstverlening. Dit omvat het ontwikkelen van nieuwe technologieën en het aanpassen aan ontwikkelingen zoals 5G en 6G, die nieuwe uitdagingen en kansen met zich meebrengen.

Verwachte ontwikkelingen NaWas

De NaWas zal verder ontwikkeld worden als Nederlandse dienst in Europa, waarbij de architectuur en infrastructuur doorlopend worden verbeterd. Met de uitbreiding naar Kopenhagen als voorbeeld, richt de NBIP zich op het versterken en verbreden van haar diensten op het gebied van DDoS-mitigatie en weerbaarheid van netwerken. Deze visie is gestoeld op drie belangrijke pijlers: digitale soevereiniteit en autonomie, 'Made in Europe', en een gedistribueerd, open platform.

Digitale soevereiniteit en autonomie benadrukken het belang van Europese onafhankelijkheid op het gebied van technologie en cyberveiligheid. Het uitbesteden van kennis, technologie en toepassingen aan partijen buiten de EU, vormt in toenemende mate een veiligheids- en continuiteitsrisico. Dit valt natuurlijk niet los te zien van het geopolitieke landschap, dat de laatste jaren snel is veranderd. Europabreed is een beweging naar digitale soevereiniteit en autonomie gaande parallel aan soortgelijke bewegingen op andere vlakken zoals energie. Er dient zich een multipolaire wereld aan waarin zowel economische als technologische keuzes en ontwikkelingen direct gerelateerd zijn aan de geopolitieke krachtsverhoudingen.

In de praktijk betekent dit voor NBIP dat de inzet op een veilig en schoon internet de implicatie heeft dat doorontwikkeling van de NaWas in een Europese context plaatsvindt. De eerste stappen op dat vlak zijn enkele jaren geleden al gezet. In dit kader streeft de NBIP ernaar de NaWas te positioneren als een robuust onderdeel van de Europese cyberweerbaarheid. Door te participeren in Europese projecten en samenwerkingsverbanden, wil de NBIP bijdragen aan een veiliger en zelfvoorzienend digitaal Europa.

Het concept van Made in Europe speelt hierbij een leidende rol. De NBIP streeft ernaar om technologieën en oplossingen te ontwikkelen die in Europa zijn vervaardigd en voldoen aan de Europese normen en waarden. Dit betekent dat de NaWas niet alleen technologisch geavanceerd moet zijn, maar ook aansluit bij de juridische en ethische standaarden die in Europa gelden. Door gebruik te maken van open source technologieën en samen te werken met Europese partners, wil de NBIP ervoor zorgen dat de NaWas niet alleen effectief, maar ook transparant en betrouwbaar is.

Een gedistribueerd, open platform is de derde pijler van de toekomstvisie voor de NaWas. Dit houdt in dat de NaWas infrastructuur verspreid wordt over meerdere locaties in Europa, wat de robuustheid en veerkracht vergroot. Door gebruik te maken van een gedistribueerd netwerk, kan de NaWas beter reageren op aanvallen en verstoringen, en biedt het een hogere mate van bescherming aan de deelnemers. Daarnaast zorgt een open platform ervoor dat er meer samenwerking en kennisdeling plaatsvindt, wat leidt tot continue verbetering en innovatie binnen de dienst.

Een ander belangrijk aspect van de toekomstvisie is het versterken van de samenwerking met kleine internetproviders en hostingbedrijven in Europa. Door hen te ondersteunen in het voldoen aan de steeds strengere Europese regelgeving, wil de NBIP ervoor zorgen dat ook zij toegang hebben tot de middelen en kennis die nodig zijn om cyberveiligheid te waarborgen. Dit betekent dat de NaWas niet alleen een dienst is voor grote spelers, maar ook een betrouwbare en betaalbare optie voor kleinere bedrijven die vaak beperkte middelen hebben om zichzelf te beschermen.

Interview Simon Kuhn

Head of Engineering

Simon Kuhn is Head of Engineering bij NBIP . Hi startte in 2023 bij NBIP en heeft een breed gedefiniee de rol die zowel operationele taken als strategische planning en de architectuur van systemen omvat .Zijn team bestaat uit vijf engineers, waaronder hijzelf, die werken aan het moderniseren en verbeteren van de infrastructuur en diensten van NBIP . Simon werkte voordathij bij NBIP aan de slag ging onder meer bij Amazon Web Services en Vodacom in verschillende rollen

Kun je iets meer vertellen over de modernisering van de NaWas-architectuur?

"Toen ik eind vorig jaar in dienst kwam, beschikten we over een zeer functionele dienst, maar we wilden daar een aantal vernieuwingen in aanbrengen. We hebben ons vervolgens gericht op ingrijpende vernieuwing, inclusief de apparatuur zelf, om meer flexibiliteit, zichtbaarheid en veerkracht te bieden. We hebben een belangrijke verandering in de architectuur aangebracht die, hoewel niet direct merkbaar voor onze deelnemers, ons in staat stelt om nieuwe mogelijkheden te introduceren in de toekomst. Zo zijn we bijvoorbeeld aan het kijken of we /32-hostbescherming (uitgesproken als slash 32-hostbescherming) kunnen bieden, wat momenteel buiten onze architectonische mogelijkheden valt. Deze modernisering helpt om de NaWas aan te laten sluiten bij de behoeften van onze deelnemers. Daarnaast blijven we zo bij met de recente ontwikkelingen op het gebied van mitigatie."

Wat behelst die /32-hostbescherming precies?

"/32-hostbescherming stelt deelnemers in staat om specifieke hosts uit te kiezen voor mitigatie, terwijl de rest van het netwerkverkeer binnen dat subnet onaangetast en ongeïnspecteerd door kan gaan. Dit is een oplossing voor wat wij het 'luidruchtige buur'-scenario noemen. Op dit moment, wanneer

We hebben een fundamentele verandering in de architectuur aangebracht die ons in stelt stellen om nieuwe mogelijkheden te introduceren.

deelnemers hun netwerkverkeer naar ons sturen, gaat het hele netwerk door onze mitigatie, wat invloed kan hebben op services die eigenlijk niet het doel van de aanval waren. Met /32-hostbescherming kunnen we zeer agressieve mitigaties toepassen op de specifieke IP's die worden aangevallen zonder ons zorgen te maken dat deze beleidsregels ander legitiem verkeer beïnvloeden. Dit verbetert niet alleen de ervaring van deelnemers, maar zorgt ook voor een efficiënter gebruik van bandbreedte in onze mitigatie-omgevingen en vermindert de belasting van onze ondersteuningsinfrastructuur. We zullen dit niet op korte termijn beschikbaar hebben, maar het is één van de mogelijkheden die de upgrade van de architectuur binnen bereik brengt."

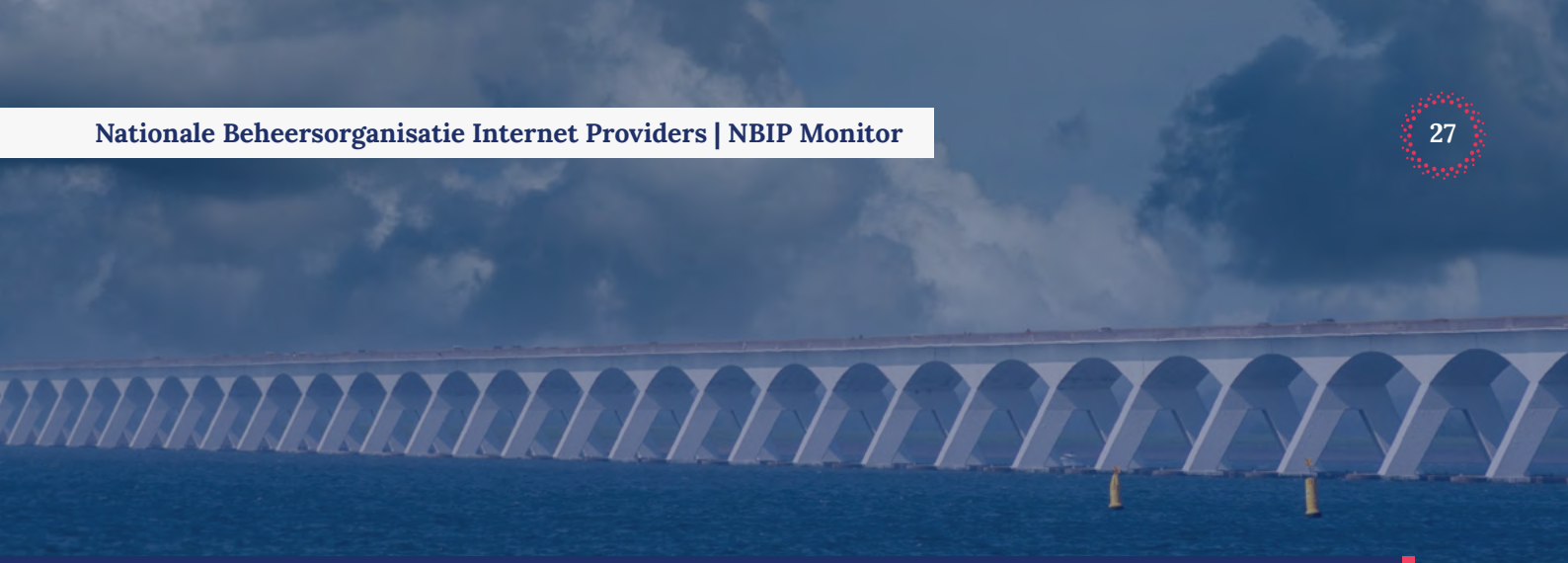
Wat zijn de ambities op het vlak van Europese expansie van de NaWas?

"We zijn van oudsher een enkele point-of-presence (PoP)-service met onze Amsterdamse PoP, die nu weliswaar twee locaties heeft voor datacenter-redundantie. We hebben dit uitgebreid met een PoP in Denemarken, die we aan Amsterdam hebben gekoppeld. Deze multi-PoP-infrastructuur biedt interessante mogelijkheden voor ons. Zodra we daar klaar voor zijn, kijken we zeker of we de Deense PoP op verschillende locaties in Europa kunnen repliceren. Het voordeel van deze edge-locaties is een lagere latency voor schoon verkeer, vooral wanneer de bron en bestemming zich in dezelfde regio bevinden.

Dankzij deze uitbreiding kunnen we een betere service bieden door de daadwerkelijke mitigatie dichter bij onze deelnemers te brengen, wat ten goede komt aan latencygevoelige toepassingen zoals spraak of gaming."

Wat behelst het IPCEI-CIS programma en welke rol speelt de NBIP hierin?

"Het IPCEI-CIS (Important Project of Common European Interest on Cloud Infrastructure and Services) is het eerste IPCEI op het gebied van cloud en edge computing. Het is een Europees initiatief dat is gericht op het bevorderen van innovatie en samenwerking om strategische ketens te versterken en de technologische soevereiniteit van Europa te vergroten. Dit specifieke project gaat om de ontwikkeling van het eerste interoperabele en openlijk toegankelijke Europese ecosysteem voor gegevensverwerking, het multi-provider continuüm van cloud tot edge. Je kunt je voorstellen dat cybersecurity daarin van groot belang is. NBIP leidt dit cyberbeveiligingsaspect op basis van security by design. Het is onze rol om ervoor te zorgen dat beveiliging vanaf het begin wordt ingebouwd in alle R&D-projecten en niet wordt gezien als een toevoeging. Als non-profit organisatie met een missie om het internet veiliger te maken, is NBIP goed gepositioneerd om bij te dragen aan dit project dat gericht is op het ontwikkelen van technologie die de markt alleen niet zou nastreven vanwege de kosten."



Security by design: deelname aan IPCEI-CIS

NBIP is deelnemer aan het Modular integrated sustainable data center (MISD) consortium dat werkt aan een field lab voor een modulair edge datacenter voor een Europese cloudinfrastructuur.

NBIP neemt deel aan het IPCEI-CIS (Important Project of Common European Interest on Cloud Infrastructure and Services) via het MISD-consortium. In dit consortium nemen zeven organisaties deel, ieder met een eigen specialisatie, waarbij NBIP cybersecurity voor haar rekening neemt.

Het doel van MISD is om een nieuw modulair, duurzaam en secure by design ontwerp te ontwikkelen dat ingezet wordt op plekken dichtbij eindgebruikers (edge computing). De innovaties en ontwikkelingen die worden gerealiseerd binnen het project, komen samen in een gevalideerde, gedistribueerde opstelling in een field lab. De looptijd van het project is 5 jaar, van 2024 tot 2029.

Rol NBIP

NBIP richt zich op de ontwikkeling van een open security platform dat geïntegreerd is in het modulaire edge datacenter dat binnen het project wordt ontwikkeld. De bedoeling is de volgende generatie Europese datacenters secure by design te ontwerpen, zodat weerbaarheid georganiseerd wordt daar waar het hoort, namelijk waar de applicaties, computing power en data zich bevinden.

Een belangrijke doelstelling voor NBIP's betrokkenheid bij het IPCEI-CIS is het creëren van een testbed. Dit testbed dient als een gecontroleerde omgeving waar nieuwe ideeën en technologieën op het gebied van cyberbeveiliging getest en geoptimaliseerd kunnen worden voordat ze worden uitgerold. Het biedt deelnemers de mogelijkheid om hun innovatieve concepten in de praktijk te brengen en te evalueren hoe effectief ze zijn in het tegengaan van cyberdreigingen. Dit proces van testen en valideren is essentieel om ervoor te zorgen dat de uiteindelijke producten en diensten voldoen aan de hoge standaarden die in Europa gelden.

Een leidend beginsel in dit proces is 'security-by-design', wat betekent dat beveiliging vanaf het begin in het ontwerp en de ontwikkeling van systemen en technologieën wordt geïntegreerd. Door security-by-design te implementeren, wordt de veiligheid niet als een bijkomstigheid behandeld, maar als een fundamenteel onderdeel van het product, wat resulteert in robuustere en beter beschermde oplossingen.

Binnen het IPCEI-CIS werkt NBIP ook aan de ontwikkeling van gedecentraliseerde mitigatietechnieken. Dit houdt in dat in plaats van te vertrouwen op een gecentraliseerde infrastructuur, er een netwerk van gedistribueerde systemen wordt opgezet die gezamenlijk kunnen

reageren op cyberaanvallen. Deze aanpak verhoogt de veerkracht en flexibiliteit van de verdedigingsmechanismen, waardoor de kans op succes van een aanval aanzienlijk wordt verminderd. Het gedecentraliseerde systeem maakt het mogelijk om sneller en effectiever te reageren op dreigingen, wat van groot belang is in een tijd waarin cyberaanvallen steeds geavanceerder en frequenter worden.

Breder belang, goed voor deelnemers

In de bredere context van het IPCEI-CIS streeft NBIP ernaar om een bijdrage te leveren aan de algehele cyberveiligheid in Europa. Dit omvat samenwerking met andere Europese partijen om best practices te delen, gezamenlijke onderzoeksprojecten op te zetten en gezamenlijk te werken aan oplossingen die de digitale autonomie en soevereiniteit van Europa versterken.

Voor deelnemers heeft deelname aan dit project het voordeel dat het NBIP in staat stelt om efficiënter en gestructureerder te werken aan doorontwikkeling van haar infrastructuur. De dienstverlening zal daardoor niet alleen verbeteren, maar ook zeer nauw de markt volgen en mogelijk zelfs voor sommige aspecten voorop kunnen gaan lopen. Het helpt daarnaast om NBIP in Europa verder te profileren. Dit kan allerlei voordelen hebben, waaronder verdere schaalvoordelen en ingangen bij de juiste gremia om de belangen van deelnemers in Europa verder te kunnen bestendigen.

Kenniscentrum

Het kenniscentrum van NBIP is bedoeld om zowel vakinhoudelijke als algemene kennis te delen .

Enerzijds wordt zeer specifieke expertise gedeeld, bijvoorbeeld als het gaat om DDoS, abuse bestrijding of lawful interception. Anderszijds heeft het kenniscentrum een publieke functie. Zowel deelnemers, stakeholders en samenwerkingspartners als media, bestuurders, politici en andere geïnteresseerden kunnen bij NBIP terecht voor informatie. De bedoeling is om de activiteiten van het kenniscentrum de komende jaren verder uit te bouwen.

Het kenniscentrum is primair een platform voor informatie-uitwisseling en samenwerking. Door het regelmatig publiceren van artikelen, rapporten, whitepapers en casestudies, biedt NBIP waardevolle inzichten die deelnemers kunnen gebruiken om hun eigen beveiligingsstrategieën te verbeteren. Ook organiseert het kenniscentrum evenementen, workshops en webinars.

Een ander belangrijk aspect van het kenniscentrum is de ondersteuning bij naleving van regelgeving en wetgeving. NBIP helpt deelnemers te begrijpen welke nieuwe wetten en richtlijnen op hen van toepassing zijn, en hoe zij hieraan kunnen voldoen. Te denken valt aan het bieden van tools en resources om naleving van wet- en regelgeving te vergemakkelijken. Door deze ondersteuning kunnen deelnemers zich beter voorbereiden op audits en inspecties, en kunnen zij hun risico's op non-compliance minimaliseren.

Daarnaast zet NBIP zich in om de toegang tot Europese subsidies en financiering te vergemakkelijken voor haar deelnemers. Veel aanbieders van digitale infrastructuur en andere organisaties in de branche zien op tegen de bureaucratie en complexiteit van Europese subsidieaanvragen. NBIP wil hierin met het kenniscentrum een faciliterende rol spelen door kennis en ervaring te delen, en door deelnemers te ondersteunen bij aanvragen. Zo wordt het voor hen eenvoudiger om gebruik te maken van de beschikbare middelen en hun eigen cyberbeveiligingsprojecten te realiseren.

Het kenniscentrum is tot slot ook actief betrokken bij onderzoeksprojecten en innovaties op het gebied van cybersecurity. Daartoe wordt samengewerkt met academische instellingen, onderzoeksorganisaties en private partners in de sector. Deelnemers van NBIP liften mee op deze inspanningen doordat zij in de opgedane kennis delen, hetzij door middel van de diensten van NBIP hetzij door kennisdeling.

Public affairs

De public affairs activiteiten van NBIP zullen zich de komende jaren waarschijnlijk intensiveren. Daar zijn meerdere redenen voor. Primair moet de sector van aanbieders van digitale infrastructuur zich conformeren aan nieuwe wet- en regelgeving en tegelijkertijd haar weerbaarheid tegen cyberdreigingen versterken. Dit gaat vaak hand in hand, omdat de wetgever het maatschappelijk en economisch belang van digitale diensten erkent en inziet dat verstoringen grote gevolgen kunnen hebben. De uitwerking van wet- en regelgeving in beleid en de samenwerkingsverbanden die hieruit ontstaan, zijn daarom ook een punt van aandacht voor NBIP.

NBIP staat in nauw contact met onder meer het ministerie van Justitie en Veiligheid, het ministerie van Binnenlandse Zaken, het Nationaal Cyber Security Centrum (NCSC), Digital Trust Center (DTC), de Rijksinspectie Digitale Infrastructuur (RDI), het Openbaar Ministerie (OM), Nationale Politie en verscheidene Europese overheidsorganisaties.

Daarnaast neemt NBIP deel aan sectorale initiatieven, coalities en overleggen, waaronder de anti-DDoS-coalitie, het Anti Abuse Netwerk (AAN) en stichting Digitale Infrastructuur Nederland (DINL). Ook staat NBIP in nauw contact met de verschillende brancheorganisaties in de sector. Op Europees niveau haakt NBIP steeds meer aan bij samenwerkings-verbanden en coalities.

Vanuit DINL, waarin de kern van de Nederlandse digitale infrastructuur vertegenwoordigd is, wordt ook namens NBIP aan belangenbehartiging gedaan voor haar achterban.

NBIP zit dicht op het vuur en haar input wordt door stakeholders gewaardeerd. Dit heeft tot gevolg dat NBIP in staat is om zorgen en praktische uitdagingen die spelen bij deelnemers over te brengen aan de juiste overlegtafels.

Namens de Deelnemers Frans ter Borg

Voorzitter Raad van Deelnemers

Frans ter Borg is sinds april 2024 de voorzitter van de Raad van Deelnemers van de NBIP, waar hij zich inzet om de belangen van de deelnemers te behartigen Met een lange carrière in de internetsector en als oprichter van Quanza in 2001, heeft Frans ruime ervaring in netwerk- en infrastructuuroplossingen Hij heeft eerder bestuursfuncties vervuld bij de Dutch Cloud Community (DCC) en stichting Digitale Infrastructuur Nederland (DINL), waar hij zich onder andere bezighield met beleidsvraagstukken rondom security en internetinfrastructuur

Sinds april 2024 ben je de nieuwe voorzitter van de Raad van Deelnemers van de NBIP . at heeft je doen besluiten deze rol op je te nemen?

“Er was al enige tijd een vacature, en ik vind het van belang dat de stem van de deelnemers goed terechtkomt in wat er gebeurt binnen de NBIP. Ik voelde me geroepen om dit te doen.”

Kun je iets meer vertellen over jezelf en wat jou geschikt maakt voor deze functie?

“Mijn carrière in de Nederlandse internetsector gaat terug tot 1996, waardoor ik diepgaande kennis heb opgedaan van hosting, telecom en clouddiensten. Via mijn bedrij Quanza heb ik specifie e expertise ontwikkeld in core internetinfrastructuur, wat direct aansluit bij de activiteiten van de NBIP. Mijn bestuurservaring, opgedaan tijdens mijn zevenjarige termijn bij de Dutch Cloud Community en voorganger ISPConnect, DINL en mijn voorzitterschap van CITA (Cloud IT Academy), heeft me vertrouwd gemaakt met belangrijke vraagstukken rondom security en beleid en educatie in de sector. Deze nieuwe rol bij de NBIP is een mooie mogelijkheid om ook aan de operationele kant te gaan werken en te voelen wat dat beleid nou met zich meebrengt.”

Je hebt het stokje overgenomen van Bernard Edelenbos, die deze rol bijna 10 jaar heeft vervuld Zijn zijn schoenen lastig te vullen?

“Hoewel Bernards schoenen natuurlijk moeilijk te vullen zijn vanwege zijn jarenlange ervaring, breng ik een iets andere aanpak mee. Ik ben van origine wellicht iets meer een techneut, wat mij in staat stelt om vanuit een ander perspectief naar oplossingen te kijken voor zowel de business als de organisatie.”

Wat is je ambitie in deze rol en welke thema’s zijn belangrijk voor je?

“Ik wil het contact met de deelnemers versterken, meer interactie hebben en de wensen en uitdagingen

van de deelnemers goed bij het bestuur kunnen brengen. Zodat daar op een goede manier actie op kan worden ondernomen en oplossingen voor kunnen worden gebouwd. Aan de DDoS-kant van de NBIP zou het mooi zijn als er een constructie gebouwd kan worden waarbij er inderdaad meer internationale locaties zijn waarop fi tering kan plaatsvinden om de load te verdelen. Dat zou ook interessant kunnen zijn voor buitenlandse deelnemers. Daarnaast wil ik me richten op het zelf ontwikkelen van technologie. Door eigen technologie uit te bouwen en open source te maken, maak je het internet als geheel veiliger. Op de lange termijn kan dit tegen lagere kosten, wat de deelnemers weer ten goede komt."

Wat maakt de Nederlandse internetsector zo'n mooie community?

"In de Nederlandse internetsector is het wij-gevoel heel erg ontwikkeld. Dat maakt de sector mooi. Organisaties zoals de Dutch Cloud Community, DINL en de NBIP versterken dat in specifie e deelgebieden. Er is de bereidheid om met elkaar te sparren over problemen en een kijkje bij elkaar in de keuken te geven. We hebben toch allemaal dezelfde problemen, dus laten we van elkaar leren. Er zit een stukje vriendschappelijkheid in die ik in andere sectoren veel minder herken."

Wat maakt de NBIP als organisatie bijzonder?

"De NBIP is een van de unieke organisaties van 'Internet Nederland' die echt vanuit gezamenlijkheid is ontstaan. We hebben met z'n allen hetzelfde probleem, zoals DDoS-aanvallen, en proberen dat samen op te lossen. Soms gaat de kost voor de baat uit, maar uiteindelijk creëren we met z'n allen iets moois en efficiënts. Dit collectieve karakter is best uniek, zeker internationaal gezien. In andere landen zijn dit soort initiatieven vaak meer commercieel van aard.

Bij de NBIP gaat het niet alleen om het individu, maar om het collectief. We investeren in de gezamenlijkheid, wetende dat het later weer terugkomt en we er allemaal iets aan hebben. Dat maakt de NBIP echt bijzonder.

En wat ik ook genoemd wil hebben, is dat de organisatie de afgelopen anderhalf jaar een zware wedstrijd gehad heeft met het in eigen beheer nemen van de dienstverlening. Dat heeft een hele hoop werkdruk opgeleverd. De NBIP, en dan bedoel ik de directie, medewerkers en het bestuur, hebben daar echt een huzarenstukje geleverd en ik denk dat we dat als deelnemers echt moeten waarderen, hoeveel werk daar verzet is met zo'n klein team."

Over NBIP

De stichting Nationale Beheersorganisatie Internet Providers (NBIP) is in 2001 opgericht als uitvoeringsinstituut voor tapbevelen in de Telecommunicatiewet. Tegenwoordig is de NBIP uitgegroeid tot het expertisecentrum voor DDoS-mitigatie, Lawful Interception en Threat Intelligence-analyse voor internet-, hosting- en cloudproviders in Nederland en Europa.

NBIP heeft de missie om aanbieders van digitale infrastructuur te helpen aan hun operationele compliance te voldoen met diensten die efficiënt te exploiteren zijn. Deelnemers kunnen dure of complexe faciliteiten die ze niet de hele tijd nodig hebben gezamenlijk via NBIP gebruiken. Het bekendste voorbeeld hiervan is de Nationale Wasstraat (NaWas), het grootste non-profit DDoS scrubbing center ter wereld waarvan meer dan 130 organisaties in 10 Europese landen gebruikmaken.

NBIP is door de jaren heen uitgegroeid tot een vaste waarde in het Nederlandse internetlandschap. Met meer dan 200 deelnemers, een internationale aanwezigheid en betrokkenheid bij strategische Europese ontwikkelingstrajecten, is bewezen dat de filosofie van NBIP ook in de praktijk werkt. Zowel aanbieders van digitale infrastructuur als publieke en private partners weten hun weg naar NBIP te vinden.

NBIP nationale beheersorganisatie internet providers