

2024

Jaarverslag



Zorgeloos online

2024

Inhoud

	<u>Voorwoord</u>	3
I	<u>Over SIDN</u>	6
2	<u>Onze strategie voor een veilig internet</u>	9
3	<u>Een mondiaal toonaangevend .nl-domein</u>	11
4	<u>Een veilig, stabiel en toekomstvast internet</u>	21
5	<u>Samenwerken voor de internetgebruiker</u>	32
6	<u>Ontwikkelingen binnen SIDN</u>	40
7	<u>Duurzaamheidsverslag</u>	46
8	<u>Verslag raad van toezicht</u>	49
9	<u>Financieel verslag</u>	53
10	<u>Personalia</u>	64
II	<u>Woordenlijst</u>	66
	<u>Colofon</u>	71



Loek Bakker, CTO SIDN

Roelof Meijer, CEO SIDN

Wereldwijde verbinding is de kracht van het internet

Voorwoord

Het internet is een grotendeels onzichtbaar netwerk dat bestaat uit meer dan 70.000 onderling verbonden netwerken. Het verbindt mensen over de hele wereld. Door het internet kunnen we grenzeloos samenwerken en hebben we toegang tot oneindig veel informatie en (vitale) digitale diensten. Van financiële en overheidsdiensten tot gezondheidszorg en onderwijs. We hopen dat de waarde die het internet brengt en de samenwerkingen in onze sector bestand blijven tegen de internationale conflicten en (geopolitieke) spanningen. En we hopen dat we ons hier in Nederland en internationaal voor blijven inzetten, als kracht tegen negatieve ontwikkelingen die mensen uit elkaar drijven. Zodat wereldwijde verbinding de kracht van het internet is en blijft.

Strategische besluiten voor een veilig en stabiel .nl

Een betrouwbaar Domain Name System (DNS) en domeinnaamregistratiesysteem (DRS) voor .nl is onze topprioriteit. Hier werken we aan vanuit onze missie: een kansrijk en zorgeloos digitaal bestaan voor iedereen. In 2024 lag onze focus voor een belangrijk deel op het nieuwe registratieplatform Hello Registry. Dit platform ontwikkelen we samen met onze strategische partner CIRA, op basis van haar huidige Fury Registry Platform. We hielden ons vooral bezig met het voorbereiden van de migratie van .nl, .amsterdam, .politie en .aw naar Hello Registry.

Ook stond 2024 in het teken van het proces dat volgde op de aankondiging van ons voorgenomen besluit: het migreren van een deel van de infrastructuur van ons registratiesysteem naar de publieke cloud van Amazon Web Services (AWS) in Europa. Deze keuze leidde tot zorgen over de Nederlandse digitale autonomie. Daar hebben we alle begrip voor, want de discussie over het gebrek daaraan wordt steeds urgenter en intensiever. De geopolitieke ontwikkelingen en de stand van zaken zoals beschreven in het [Draghi-rapport](#) en het [Clingendael-rapport](#), benadrukken het belang van de vergroting van onze strategische digitale autonomie. In Nederland en Europa.

Europese en Nederlandse cloudproviders kunnen de technische en functionele criteria en de juridische en organisatorische aspecten van SIDN op dit moment maar gedeeltelijk invullen. Dit komt naar voren uit het onderzoek dat Eraneos in 2023 voor ons uitvoerde. Ook blijkt het uit de quickscan van het Nederlandse en Europese cloudaanbod die in 2024 werd uitgevoerd in opdracht van het ministerie van Economische Zaken (EZ). In 2024 lieten we ook een Data Protection Impact Assessment (DPIA) uitvoeren en deed de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) een risicoanalyse.

De uitkomsten van de onderzoeken bevestigen dat we, voor zover we het redelijkerwijs konden overzien, een zorgvuldig beredeneerd besluit hebben genomen. Daarbij staan de betrouwbaarheid en beschikbaarheid van het .nl-domein voorop. Begin 2025 kregen we op basis van de quickscan, de DPIA en de risicoanalyse groen licht van het kabinet om het .nl-registratiesysteem onder bepaalde voorwaarden en in aangepaste vorm te migreren naar de publieke cloud van AWS.

Mede op basis van advies van de AIVD, implementeren we een aantal belangrijke maat-

regelen om de beschikbaarheid van .nl onafhankelijk van AWS te borgen. De kern van deze maatregelen betreft dat we de database voor de zonefile onderbrengen bij een Nederlandse provider. Deze database vormt de primaire, betrouwbare en vertrouwde bron op basis waarvan de generatie, signing en publicatie van de zonefile buiten AWS bij een Nederlandse provider plaatsvindt. Door deze maatregelen beperken we de afhankelijkheid van AWS en borgen we (digitale) autonomie.

Geleerde lessen nemen we mee in de vervolgstappen, waarbij we onze stakeholders nauw betrekken. Het beheer van .nl – en van het domeinnaamregistratiesysteem – blijft te allen tijde in onze handen en verbonden met Nederland. Zo zorgen we ervoor dat .nl altijd beschikbaar is en beschermen we onze gegevens.

> Lees meer over [onze keuze voor de publieke cloud, het uitsluitel van het kabinet en de DPIA](#)

Het beheer van .nl blijft in onze handen en verbonden met Nederland.

Samenwerken over grenzen heen

Het is cruciaal dat we vanuit vertrouwen, kennis en begrip blijven samenwerken aan gemeenschappelijke doelen. Van het bestrijden van internet-abuse tot het beschermen van de vitale digitale infrastructuur. Het huidige wereldbeeld en de politieke en publieke aandacht voor onze dienstverlening benadrukken het maatschappelijk belang van onze weerbaarheid en een sterk .nl-ecosysteem. Maar ook van een open, veilig en toegankelijk internet voor alle gebruikers wereldwijd.

Onze collega's van SIDN Labs doen daarom samen met universiteiten, onderzoekslabs en andere partners toegepast technisch onderzoek om de internetinfrastructuur te verbeteren. In Nederland én daarbuiten. Met SIDN fonds steunden we in 10 jaar tijd meer dan 400 innovatieve, maatschappelijke internetprojecten die bijdragen aan een sterk internet voor iedereen.

In 10 jaar tijd steunde SIDN fonds meer dan 400 projecten.

Daarnaast nemen we deel in internationale samenwerkingsverbanden, zoals CENTR, DNS-OARC, IETF en ICANN. Ook zijn we sponsor of kennispartner van partijen die zich inzetten voor een veiliger en sterker internet, zoals het Platform Internetveiligheid. In het kader van een open en veilige digitale toekomst voor iedereen, leverden we via het ministerie van EZ input voor de [UN Global Digital Compact](#). In september 2024 namen wereldleiders dit document formeel aan. Het dient als routekaart voor de wereldwijde samenwerking tussen partijen en lidstaten om de kansen van technologieën te benutten en digitale kloven te dichten.

Ontwikkelingen in de domeinnaammarkt

In 2024 hielden ook de ontwikkelingen in de Nederlandse en wereldwijde domeinnaammarkt ons bezig. Het .nl-domein is marktleider in Nederland, met een marktaandeel van 60,5 % eind 2024. Op de tweede plek staat .com met 26%. Na een lichte groei begin 2024 zagen we voor het eerst in de geschiedenis van .nl vanaf februari een lichte krimp gedurende 3 opeenvolgende kwartalen. In december stond de teller op bijna 6,2 miljoen domeinnamen. Een aanzienlijk deel daarvan wordt door de domeinnaamhouders nog niet of niet meer actief gebruikt. Samen met onze .nl-registrars zetten we in op campagnes, die zich richten op het verhogen van de merkvoorkeur en actief gebruik van .nl. Want .nl is hét domein van en voor Nederland en een van de allerveiligste ter wereld.

Niet alleen binnen .nl, maar in de hele domeinnaamsector zijn stagnatie en krimp zichtbaar. Internationaal zijn slechts enkele honderden van de vanaf 2013 geïntroduceerde gTLD's in beperkte mate succesvol. In Nederland gebruiken we ze sporadisch. We verwachten niet dat de nieuwe aanvraagronde door ICANN vanaf 2026 daarin veel verandering brengt, want de markt ziet er heel anders uit dan een paar jaar geleden. Artificiële intelligentie (AI)

in de vorm van ChatGPT, Microsoft Copilot en DeepSeek verminderen traditionele zoekopdrachten via zoekmachines. Een negatief effect op domeinnamen is nog niet duidelijk, hoewel ze in zoekresultaten minder zichtbaar worden. Tegelijkertijd nemen de investeringen in Web3.o-TLD's (blockchain) sinds 2024 af ten opzichte van enkele jaren eerder. Web3.o-TLD's zoeken steeds meer de integratie met traditionele DNS-TLD's. Daardoor lijkt deze ontwikkeling voor ons meer een kans dan een bedreiging.

Vooruitblik op 2025

Een stabiel, altijd beschikbaar en veilig .nl blijft onze topprioriteit. Daarom werken we ook in 2025 aan het robuuster maken van de infrastructuur daarachter. De migratie van een deel van onze technische infrastructuur naar de cloud bereiden we verder voor. We nemen de geleerde lessen mee en betrekken het ministerie van EZ, de Vereniging van Registrars (VvR) en andere stakeholders bij de vervolgstappen. Samen met CIRA werken we als één team verder aan het nieuwe registratieplatform Hello Registry en bereiden we de ingebruikname daarvan verder voor. We blijven inzetten op de verhoging van actief gebruik van .nl en het beperken van opheffingen. De bestrijding van abuse in de .nl-zone zetten we voort en we richten in 2025 een abusewerkgroep met registrars op. Security blijft top of mind en beperkt zich niet tot onze compliance met bijvoorbeeld ISO27001:2022 en NIS2.

Ook in 2025 putten we motivatie en kracht uit samenwerken aan gemeenschappelijke en maatschappelijke waarden. We zetten het belangrijke werk van SIDN Labs en SIDN fonds voort en investeren verder in een inspirerende en duurzame werkomgeving die samenwerking, persoonlijke ontwikkeling en kennisdeling stimuleert. Zo kunnen wij als bevlogen SIDN'ers topprestaties blijven leveren voor een veilig, stabiel en toonaangevend .nl en een open netwerk van netwerken dat internetgebruikers wereldwijd verbindt.

In dit jaarverslag lees je hoe we ons samen met partners inzetten voor een veilig, stabiel, robuust en autonoom .nl. We hopen dat je de hoogte- en leerpunten van ons werk in 2024 en onze plannen voor 2025 met plezier leest.

Roelof Meijer, CEO
Loek Bakker, CTO



Onze kerncijfers

6.169.270



Ruim 6,1 miljoen .nl-domeinnamen (per 31 dec. 2024)

We werken samen met ruim 1.100 registrars



Het .nl-domein bestaat 39 jaar



Het SIDN-team bestaat uit 99 collega's



SIDN is 29 jaar beheerder van .nl



Meer dan 60% van .nl is beveiligd met DNSSEC

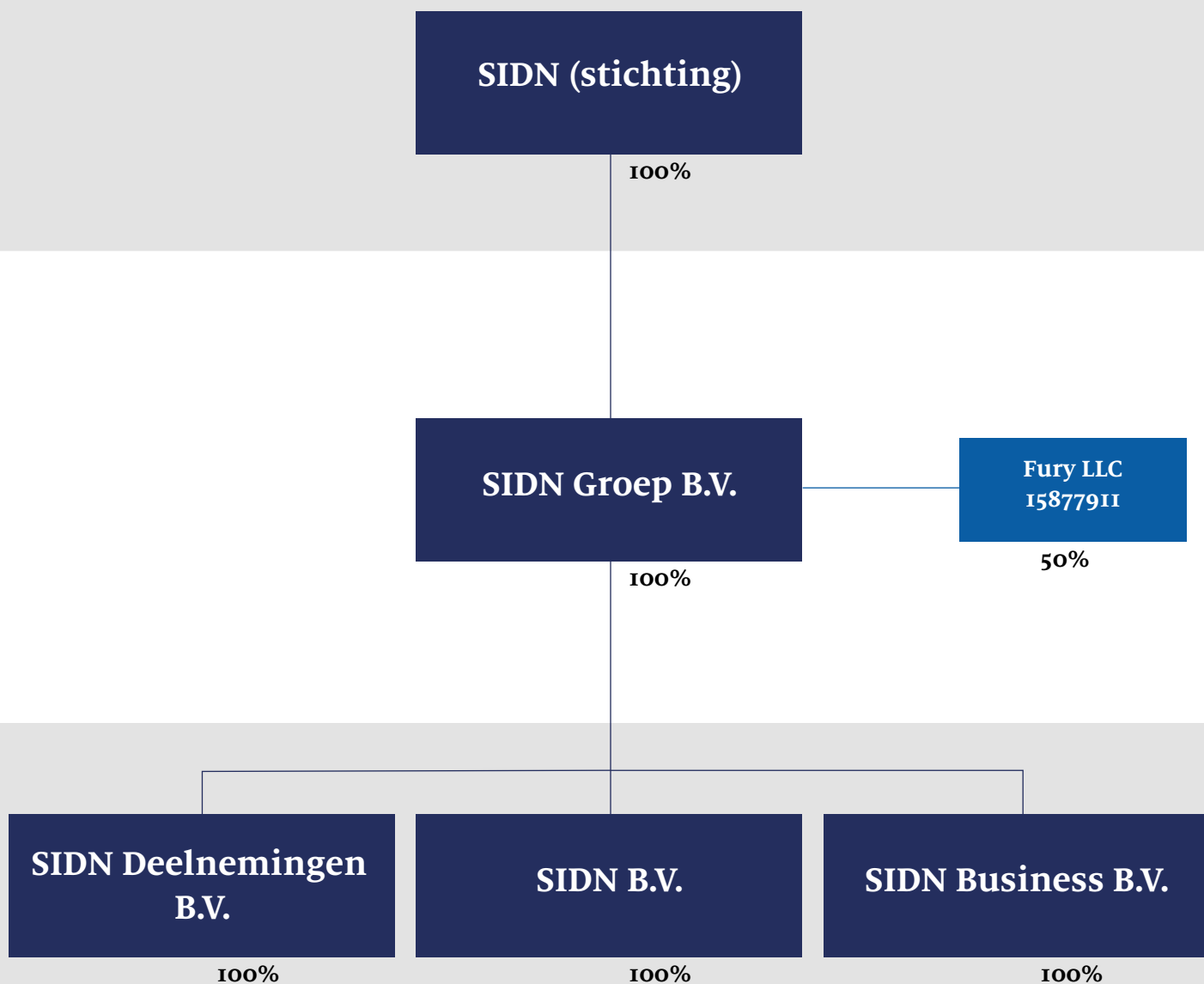
Een kansrijk en zorgeloos digitaal bestaan voor iedereen

I Over SIDN

Als beheerder van het .nl-toplevel domein werken we in het hart van het internet in Nederland én voor Nederland. Het .nl-domein is een van de veiligste en grootste landendomeinen ter wereld en daar zijn we bijzonder trots op. Maar we doen nog meer. We delen onze kennis, ontwikkelen diensten in het kader van cybersecurity en steunen initiatieven voor een beter en sterker internet. Onze missie is dan ook: een kansrijk en zorgeloos digitaal bestaan voor iedereen.



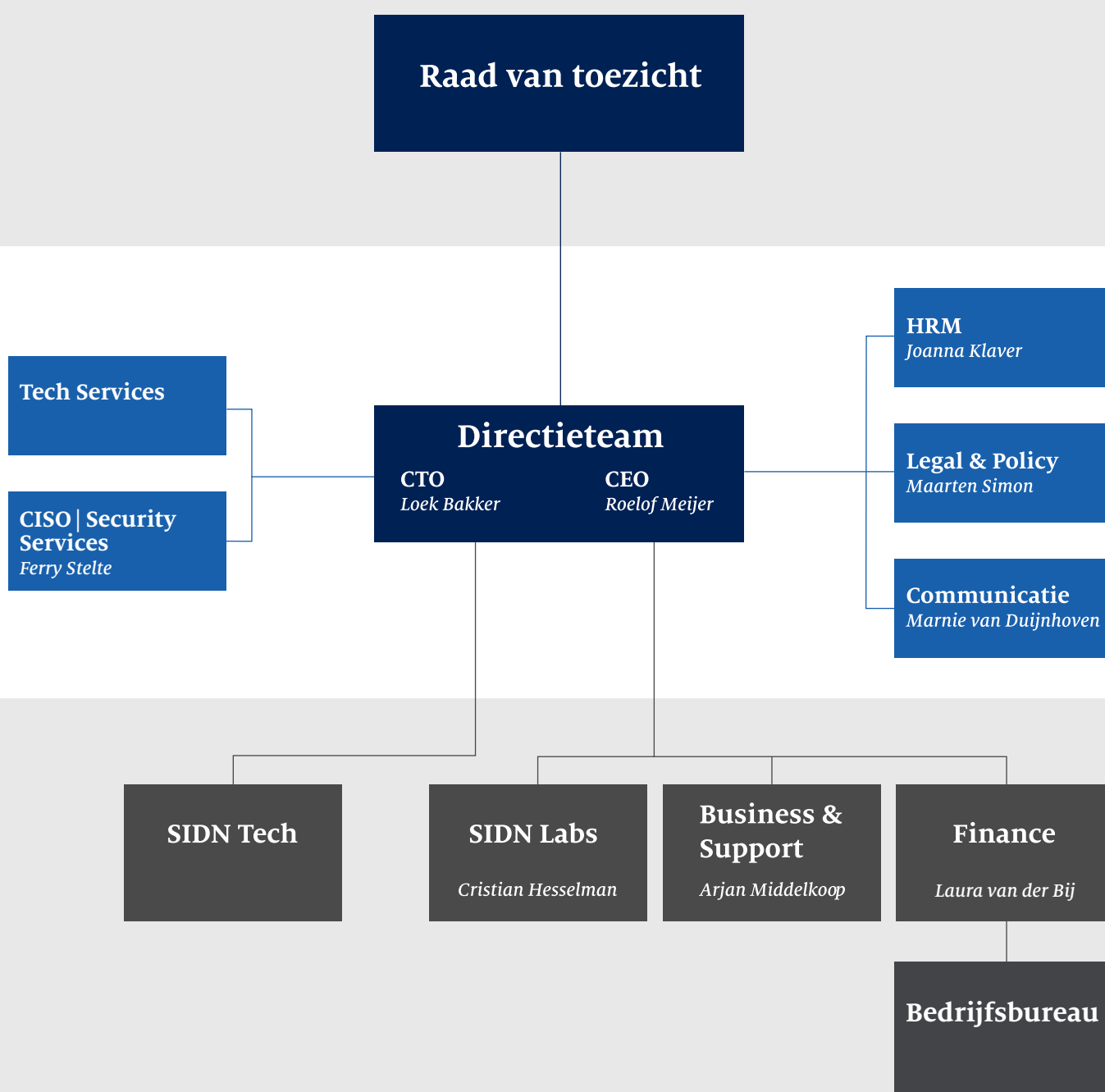
Juridische structuur



De delegatie van het .nl-domein (het recht om .nl te mogen beheren) en de operatie daarvan, de uitvoering van de taken die bij de delegatie komen kijken, zijn in verschillende juridische entiteiten ondergebracht. De delegatie is in bezit van de oorspronkelijke stichting (SIDN). De operatie is ondergebracht in een in 2023 opgerichte besloten vennootschap (SIDN B.V.), waarvan de oorspronkelijke stichting (indirect) alle aandelen houdt. Dit doen we om de ondernemersrisico's zoveel als mogelijk te spreiden. Zo willen we de continuïteit van het .nl-domein nog zekerder stellen.



Organisatieschema



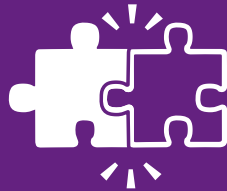
Onze strategische thema's



Toonaangevend .nl



Internetgebruiker centraal



Van knelpunten naar kansen



Toekomstvast internet



Samen

Onze waarde voor de internetgemeenschap

2 Onze strategie voor een veilig internet

We hebben een grote verantwoordelijkheid voor alle Nederlandse internetgebruikers door onze centrale rol in het Domain Name System (DNS). Veiligheid en betrouwbaarheid staan voorop vanaf de eerste dag dat we het .nl-domein beheren. Onze strategie is de brug tussen ons streven naar een kansrijk en zorgeloos digitaal bestaan en onze concrete acties om dat te bereiken. In deze strategie staan 5 thema's centraal. De speerpunten, activiteiten en strategische keuzes binnen deze thema's sluiten aan bij onze rol en verantwoordelijkheden voor Nederland en daarbuiten. In dit jaarverslag geven we daar invulling aan.

Een toonaangevend .nl

In Nederland is .nl veruit het populairste domein en ook wereldwijd is het .nl-domein toonaangevend. De kwaliteit, veiligheid en betrouwbaarheid van onze kernsystemen DNS en DRS en onze diensten voor .nl hebben de hoogste prioriteit. Vanuit daar bepalen we de agenda van SIDN. We houden .nl veilig door internetabuse actief te bestrijden, datagedreven te werken en continu te innoveren. Bovendien werken we met de beste mensen en zetten we de modernste bewezen (cloud)technologie in. Samen zorgen we ervoor dat .nl-domeinnamen voor iedereen makkelijk en breed toegankelijk zijn.

> Lees hierover meer in [hoofdstuk 3](#) en [hoofdstuk 6](#)

De internetgebruiker staat centraal

SIDN is een private organisatie met een publieke rol. We werken vóór de internetgebruiker samen met registrars, dienstverleners, overheden en partners uit de internetgemeenschap. Zo ontwikkelen en delen we onderzoeksresultaten, opensourcesoftware, data en open standaarden met de internetgemeenschap en we stimuleren de adoptie van deze open standaarden. Als het gaat om autonomie van de internetgebruiker maken we ons hard voor de waarden privacy en security by design, opensource en decentraal.

> Lees hierover meer in [hoofdstuk 3](#), [hoofdstuk 4](#) en [hoofdstuk 5](#)

Knelpunten omzetten naar kansen

We werken voortdurend aan het vergroten van de veiligheid van internetgebruikers en we stimuleren een optimaal en verantwoord gebruik van het internet. Zo pakken we knelpunten aan op het gebied van de internetinfrastructuur en cybersecurity. We sturen op verantwoord positief rendement om Nederland en de wereld te helpen innoveren, maar ook te investeren in een kansrijk en zorgeloos digitaal bestaan. Bovendien combineren we onderzoek en praktijk om zo te komen tot nieuwe oplossingen voor Nederlandse consumenten en organisaties, de internetgemeenschap en onszelf.

> Lees hierover meer in [hoofdstuk 3](#) en [hoofdstuk 4](#)

Bijdragen aan een toekomstvast internet

We werken continu aan het verder verhogen van de veiligheid en robuustheid van de huidige en toekomstige internetinfrastructuur. Dat doen we door onze onderzoeksresultaten te gebruiken, projecten te ondersteunen en diensten te ontwikkelen. Daarmee dragen we bij aan een inclusieve, rechtvaardige en duurzame digitale samenleving.

> Lees hierover meer in [hoofdstuk 4](#)

Samenwerking

Binnen SIDN werken we als één team. Samen bereiken we meer dan alleen, daarom richten we ons op samenwerkingen binnen Nederland, Europa en daarbuiten met partijen op het gebied van expertise en technologie. We werken met partners met vergelijkbare waarden, die zich net als wij inzetten voor een kansrijk en zorgeloos digitaal bestaan.

> Lees hierover meer in [hoofdstuk 5](#) en [hoofdstuk 6](#)

Strategieklankbordgroep

Met de strategieklankbordgroep blijven we doorlopend met een vertegenwoordiging van onze stakeholders in gesprek over onze strategie. De strategieklankbordgroep bestaat onder andere uit deelnemers van ministeries, universiteiten, partijen uit de internetsector zoals registrars en maatschappelijke- en belangenorganisaties. Tijdens de bijeenkomsten met deze groep verzamelen we input voor en feedback op onze strategie. De uitkomsten gebruiken we om onze strategie aan te scherpen. We vinden het vooral belangrijk dat we inzicht krijgen in de verschillende belangen. En dat deze zichtbaar en bespreekbaar worden voor alle stakeholders.

Net als voorgaande jaren hielden we 2 bijeenkomsten met de strategieklankbordgroep. Die in juni ging vooral over onze geleerde lessen uit de discussie over onze voorgenomen migratie naar de publieke cloud van AWS. En over onze plannen om het nieuwe registratieplatform, na succesvolle livegang van .nl, met onze Canadese partner CIRA ook aan te bieden aan andere ccTLD's. De bijeenkomst in november stond in het teken van de abusebestrijding in de .nl-zone. We bespraken onder andere de risico's en het bestrijden van phishing en nepwebwinkels. Uit de reflectie van de strategieklankbordgroep op de sessies en samenstelling van de groep, kwam de wens om dieper op thema's in te kunnen gaan. Daarom nemen we meer tijd voor de bijeenkomsten met ingang van 2025.



Foto: ANP / Sandra Uittenbogaart

Onze topprioriteit is een veilig en stabiel .nl

3 Een mondiaal toonaangevend .nl-domein

Bestrijding van internetabuse in de .nl-zone is een van de vele vlakken waarop we mondiaal toonaangevend zijn. We bundelen onze krachten met partners, zoals de politie, zodat we onze gezamenlijke impact vergroten. Met RegCheck identificeren we vroegtijdig verdachte domeinnaamregistraties en met SIDN Merkbewaking helpen we organisaties hun merk te beschermen. Verder versterken we .nl door het actief gebruik van .nl-domeinnamen te stimuleren. Bijvoorbeeld met ons incentiveprogramma voor registrars. In 2024 verlengden en verbreedden we onze samenwerking met de Vereniging van Registrars (VvR).

Bestrijding van internetabuse

Als beheerder van .nl nemen we voortdurend maatregelen om de veiligheid van de .nl-zone verder te verhogen. Het bestrijden van misbruik en criminele activiteiten binnen dit domein behoort tot onze kernactiviteiten. Dit werk is nog steeds hard nodig, want cybercriminelen vinden voortdurend nieuwe wegen. We doen daarom onderzoek naar misbruik met domeinnamen en werken samen met .nl-registrars, universiteiten en partijen als het NCSC.

Met RegCheck identificeren we automatisch verdachte domeinnaamregistraties in een vroeg stadium. Dit systeem kent risicoscores toe aan nieuwe domeinnaamregistraties en werd ontwikkeld door SIDN Labs. Vaak maken kwaadwillenden binnen 24 uur de meeste slachtoffers, waardoor het cruciaal is dat we malafide registraties zo snel mogelijk herkennen en snel ingrijpen. Bij een verdachte registratie heeft de houder na ons verzoek 3 dagen de tijd om zich te identificeren. Op deze manier proberen we misbruik te voorkomen.

Naast de detectie van verdachte registraties, strijden we tegen misbruik van .nl-domeinnamen voor online criminele activiteiten. Denk aan phishing, malware en nepwebwinkels. We sturen een gedetailleerde melding naar de betrokken houders, .nl-registrars en hostingpartijen bij phishing of malware waarbij de kwaadwillende een .nl-domeinnaam misbruikt. De betrokkenen kunnen vervolgens actie ondernemen om het probleem op te lossen en toekomstige aanvallen te voorkomen.

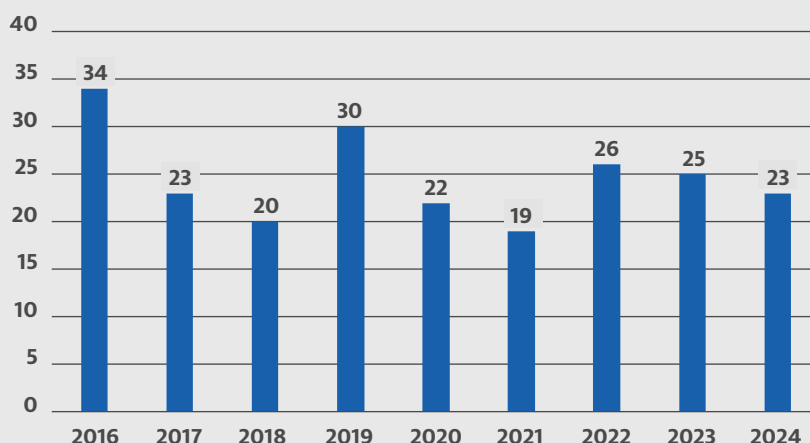
In 2024 haalden registrars op basis van onze meldingen ruim 60% van de sites met phishing en malware binnen 24 uur offline. In zo'n 400 gevallen grepen we zelf in en maakten we de domeinnaam en daarmee ook de website onbereikbaar. In november haalden we zo'n 125 domeinnamen van een malafide houder offline. Voordat we overgaan tot deze stap,

doen we in alle gevallen uitgebreid onderzoek. Bij het bestrijden van nepwebwinkels werken we nauw samen met partners, zoals de politie en de Autoriteit Consument & Markt (ACM). Eind november 2024 kondigden we een samenwerking aan met het Landelijk Meldpunt Internet-oplichting (LMIO) van de politie om internet-oplichting beter tegen te gaan. Zodra LMIO op basis van gedegen onderzoek vaststelt dat er sprake is van een nepwebwinkel, doet het meldpunt hier bij ons een melding van. Wij halen deze malafide website direct offline zonder verder uitgebreid onderzoek. Daarvan brengen we de domeinnaamhouder op de hoogte. Zo verminderen we de tijd die oplichters hebben om te opereren en kunnen we consumenten beter beschermen. Dat is cruciaal, want het aantal aangiftes over fraude via webwinkels steeg van 16.000 in 2023 naar 20.000 in 2024 (bron: Politie, 2024). Naast internetabuse kan ook een juridisch proces, bijvoorbeeld bij de inbreuk op merk- en handelsnamen, een reden voor ingrijpen zijn. In zo'n geval kan het nodig zijn dat we een .nl-domeinnaam doorhalen. We willen open en transparant blijven, want de impact van dit soort ingrepen kan groot zijn. Daarom publiceren we elk kwartaal een transparantierapport op onze website.

> Lees het [transparantierapport](#) op sidn.nl

In samenwerking met het Platform Internetstandaarden stimuleren we het gebruik van moderne open internetstandaarden. Dit zijn internationale afspraken over kwaliteits- en veiligheidseisen waaraan gegevensuitwisselingen tussen ICT-systemen moeten voldoen. De implementatie van deze standaarden draagt bij aan een veilig, stabiel en open internet. Naast dat we de adoptie van de standaarden stimuleren via de Registrar Scorecard (RSC), zijn we partner van Internet.nl. Dit is een samenwerkingsverband van de Nederlandse overheid en partijen uit de internet-sector. Samen met deze partijen vergroten we het gebruik van moderne veilige internetstandaarden.

Fig. 1 | Gemiddelde levensduur phishingsites en websites met malware in uren



Ook ondersteunen we internetgebruikers met publicaties over security, delen we onze kennis via SIDN Academy, SIDN TechTalk, webinars en praktische handleidingen en beantwoorden we op onze website veelgestelde vragen over de standaarden.

> Lees meer over de [moderne internetstandaarden](#) op [sidn.nl](#)

Met de Registrar Scorecard stimuleren we het gebruik van moderne open internetstandaarden.

Ontwikkelingen .nl-domein en de markt

In januari 2024 groeide .nl licht, waarna de Nederlandse domeinnaammarkt stabiliseerde. Van februari tot september zagen we een lichte krimp van 1,7% en ook in december kromp de zone. Eind 2024 stond de teller op bijna 6,2 miljoen domeinnamen, terwijl we 2024 startten met 6.297.384 domeinnamen. Het .nl-domein blijft daarmee staan in de top 5 van grootste landen-domeinen ter wereld op basis van het absolute aantal geregistreerde domeinnamen (bron: Verisign, 2024). Oorzaken van de krimp waren onder andere het

toegenomen aantal opheffingen na het eerste jaar, waarin domeinnaamhouders bij hun registrar vaak een lager tarief betalen voor hun .nl-domeinnaam dan de jaren daarna. En de daling van het aantal nieuwe registraties met 10%. Wat vooral lijkt te komen door de afname van het aantal startende ondernemers met 8% en het aantal bedrijfsbeëindigingen dat steeg met 15% (bron: KVK, 2024). Maar er zijn meer effecten dan alleen in Nederland die de omvang van .nl beïnvloeden.

Ook internationaal spelen ontwikkelingen die invloed hebben op de omvang van .nl en andere ccTLD's en gTLD's. CENTR noemde mogelijke verklaringen, zoals de opheffing van domeinnamen met kortetermijndoelen en stijgende verlengingsprijzen voor ccTLD's (bron: [CENTR, 2024](#)). Stagnatie en krimp zijn in de hele domeinnaammarkt zichtbaar. Zo krompen ook .eu en de meeste generieke topleveldomeinen (gTLD's), zoals .online en .top.

De vraag naar .com-domeinnamen in Nederland nam juist gedurende het hele jaar toe. Vooral in de maanden vóór de prijsverhoging van 7% voor .com-domeinnamen in september. Maar ook daarna bleef .com in Nederland licht groeien. In de eerste 3 kwartalen groeide .com in Nederland met 7,5%, terwijl de omvang hiervan wereldwijd afnam met 2,2% ten opzichte van een jaar eerder.

Naast bovengenoemde ontwikkelingen volgen we het effect van artificiële intelligentie (AI) op de domeinnaammarkt. Het marktonderzoeksbureau GfK deed onderzoek naar de invloed van AI op het gebruik van .nl-domeinnamen. Zo stellen steeds meer internetgebruikers vragen aan AI-systemen, zoals ChatGPT en AI-chatbots, waar zij voorheen antwoord zochten op websites. Deze ontwikkeling kan invloed hebben op de omvang van .nl.

De resultaten laten zien dat vooral oudere gebruikers van ChatGPT minder websites bezoeken.

Marktaandeel

De .nl-extensie heeft een prominente positie in de Nederlandse markt. Zeker bij ondernemers is .nl het meest populair. Toch daalde het marktaandeel van .nl licht van 62% in 2023 naar 61% in 2024. Het Nederlandse marktaandeel van .com nam toe van 23% tot 25% eind 2024.

Fig. 2 | Ontwikkeling .nl-domein

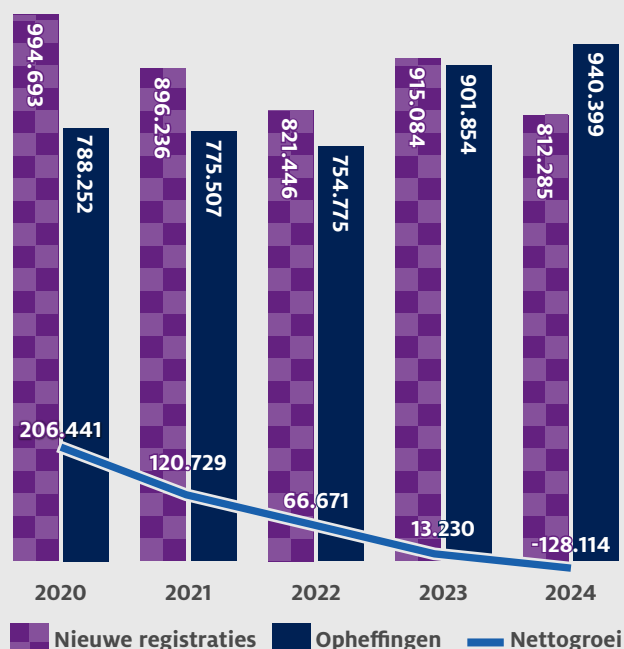
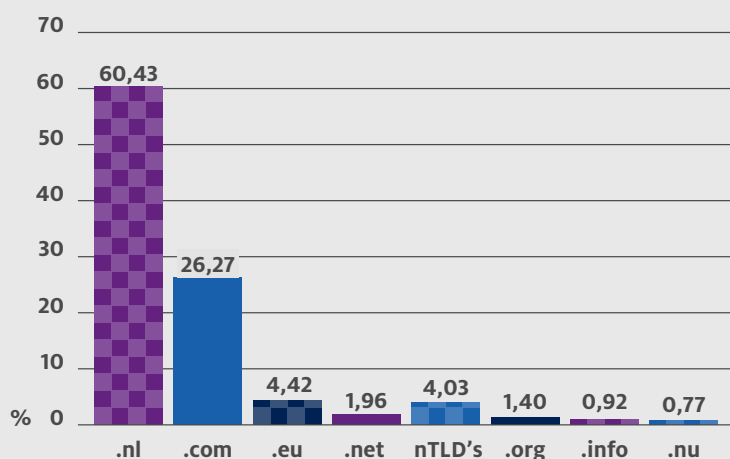


Fig. 3 | Marktaandeel in 2024



Convenant met ministerie van Economische Zaken

Sinds 2008 hebben we een convenant met het ministerie van EZ. In het convenant bevestigen we afspraken, waarmee we samen de continuïteit en stabiliteit van het .nl-domein borgen. Ook bevestigen we hierin de binding van .nl met en de vestiging van SIDN in Nederland. In het kader van het convenant vonden in 2024 regelmatig gesprekken met het ministerie van EZ plaats. Met name in relatie tot ons voorgenomen besluit over migratie van (een deel) van ons registratiesysteem naar de publieke cloud en de onderzoeken die in dat kader zijn uitgevoerd.

Toezicht op SIDN door Rijksinspectie Digitale Infrastructuur

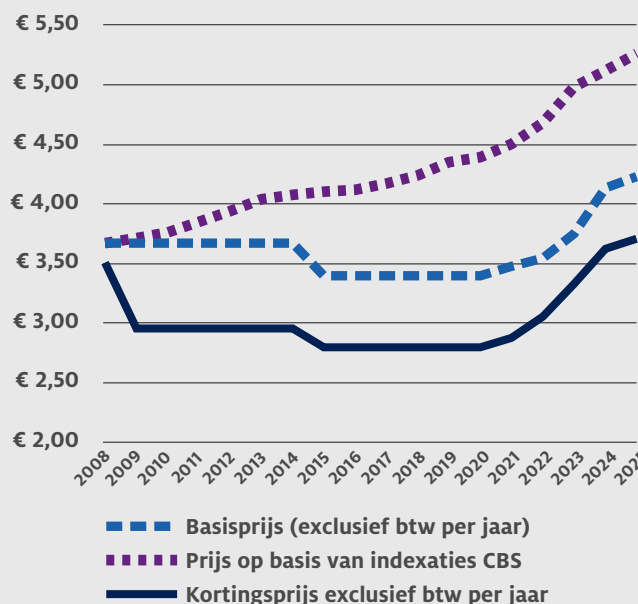
Sinds 2018 geldt de Wet beveiliging netwerk- en informatiesystemen (Wbni). Deze wet moet de

digitale weerbaarheid van Nederland vergroten, de gevolgen van cyberincidenten beperken en maatschappelijke ontwrichting voorkomen. Onder de Wbni is SIDN aangewezen als Aanbieder van Essentiële Diensten (AED). Onze diensten zijn van vitaal belang voor de Nederlandse samenleving. Daardoor staan we onder toezicht van de Rijksinspectie Digitale Infrastructuur (RDI). We hebben zorgplicht om risico's voor de beveiliging van onze netwerk- en informatiesystemen te beheersen en beveiligingsincidenten te voorkomen. Ook zijn we verplicht incidenten te melden die grote gevolgen hebben voor een stabiele dienstverlening. In 2024 was hiervan geen sprake. Wel informeerden we de RDI over het datalek als gevolg van onderhoudswerkzaamheden aan sidn.nl en over onze plannen om (een deel van) het registratiesysteem onder te brengen in de publieke cloud.

Samenwerking met de VvR

De Vereniging van Registrars (VvR) behartigt de belangen van .nl-registrars richting SIDN. Zo geeft de VvR ons gevraagd en ongevraagd advies op het gebied van bestuur, technologie, marketing en juridische thema's. We erkennen dat we de VvR in eerste instantie onvoldoende en te laat betrokken bij de voorgenomen migratie van ons registratiesysteem naar de publieke cloud. Daarom betrekken we de VvR sinds 2024 meer en in een eerder stadium bij belangrijke keuzes en activiteiten. Onder andere bij de verdere uitwerking van ons gebruik van de publieke cloud en de exitstrategieën. We werkten onder meer intensief samen met de Commissie Marketing & Communicatie en de Technische Commissie. Ook richtten we een werkgroep op met registrars die meedenken over de migratie naar het nieuwe registratiesysteem en de communicatie rondom het migratieproces. Verder bespraken we een nauwere samenwerking rondom abusebestrijding in de .nl-zone. Eind 2024 verlengden we de overeenkomst met de VvR voor 2025.

Fig. 4 | Prijsontwikkeling .nl in euro's

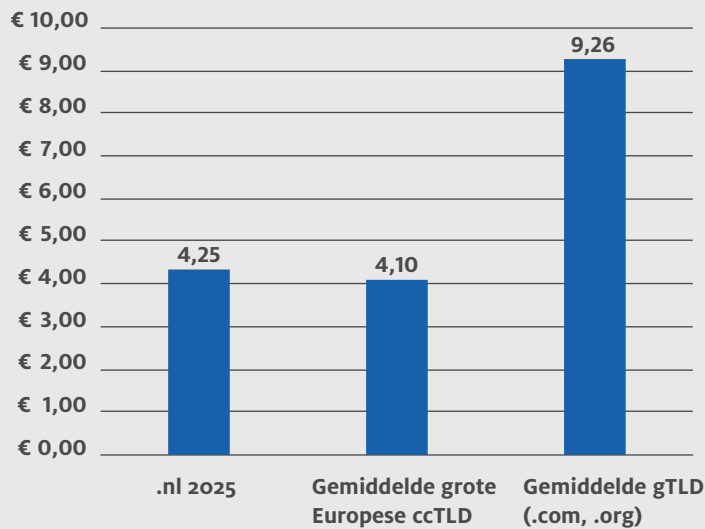


We intensiveren onze samenwerking met de VvR.

Prijsaanpassing

Met ingang van 2024 verhoogden we onze prijzen met 10%. Deze maatregel namen we om een gezonde en stabiele positie van .nl op de lange termijn te bewaken. Door de hoge inflatie, investeringen in ICT-systemen en de krappe arbeidsmarkt stijgen

Fig. 5 | Prijspeil .nl en peers
(inclusief kortingen en registrarfees)



onze kosten aanzienlijk. Terwijl onze inkomsten uit .nl-domeinnamen nauwelijks of niet autonoom stijgen. Ook willen we een investeringsreserve opbouwen, waarmee we noodzakelijke investeringen in onze ICT-omgeving en de vernieuwing van het domeinnaamregistratiesysteem kunnen financieren. Met deze reserve kunnen we ervoor zorgen dat prijsverhogingen beperkt blijven. In 2024 was de standaardprijs (exclusief kortingen en incentives) € 4,15 per jaar voor een .nl-domeinnaam. De registrarbijdrage was € 83,- per maand.

Ontwikkelingen registrarveld

In 2024 groeide het totaal aantal registrars in een jaar tijd van 1.079 naar 1.114 registrars. De nieuwe accounts zorgen nauwelijks voor een groei van de .nl-zone, doordat registrars deze accounts vooral gebruiken voor het kunnen opvragen van meer data voor handelsdoeleinden. Er waren geen verschuivingen in de top van het kanaal: eind 2024 hadden de 25 grootste registrars 83% van alle .nl-domeinnamen in beheer. Een heel kleine stijging ten opzichte van een jaar eerder (82%). Opvallend was dat meer registrars actief inzetten op duurzame registraties, bijvoorbeeld door het verlengen van domeinnamen na het eerste jaar te stimuleren en vereenvoudigen. Zowel in Nederland als internationaal.

We steunden 7 registratie-campagnes die de positie van .nl versterken.

Hoge registrartevredenheid

In 2024 beoordeelden registrars onze dienstverlening met een 7,8. Dit cijfer is lager dan de 8,1 in 2023. De belangrijkste en terugkerende oorzaak is de behoefte aan vernieuwing van onze systemen en de snelheid waarmee dat gebeurt, precies datgene waar we in 2024 en 2025 hard aan werken. 2024 stond vooral in het teken van de voorbereidingen voor de migratie naar het nieuwe registratiesysteem, maar dit merken registrars pas vanaf begin 2026. Daarnaast had de genoodzaakte prijsverhoging van 10% invloed op de beoordeling van registrars. Wel waardeerden zij onze dienstverlening en het persoonlijke contact. Onze supportafdeling scoorde ruim een 8.

Co-funded marketingacties

Samen met registrars versterken wij de positie en het gebruik van .nl in Nederland. Dat doen we onder meer door registrars te helpen bij het bekendmaken van .nl om het registreren en verlengen van .nl-domeinnamen te bevorderen. Zij kunnen het hele jaar door campagneondersteuning bij ons aanvragen. Ook namen we zelf proactief contact op met registrars om hen te ondersteunen, vooral met financiering, data en expertise.

In 2024 steunden we in totaal 7 registrarcampagnes die zorgden voor zo'n 20.000 nieuwe .nl-registraties. Bovendien stimuleerden we acties en campagnes van registrars en resellers die bijdragen aan een sterke .nl-zone, onder meer via ons dataplatform SIDN Insights. Verder kunnen registrars onze 5 campagnetoolkits met kant-en-klaar promotiemateriaal gebruiken.

Fig. 6 | Ontwikkeling klanttevredenheid

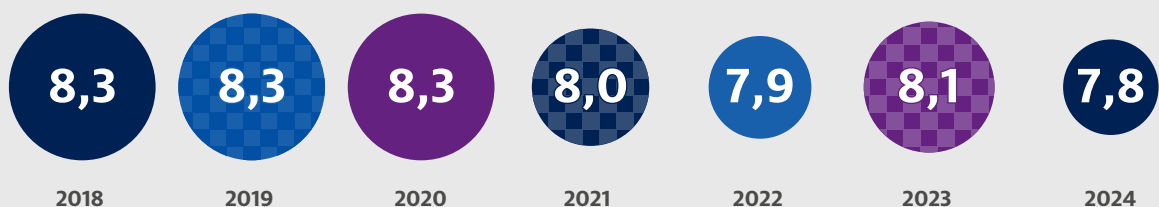


Fig. 7 | Ontwikkeling aantal met DNSSEC ondertekende domeinnamen (x 1.000)

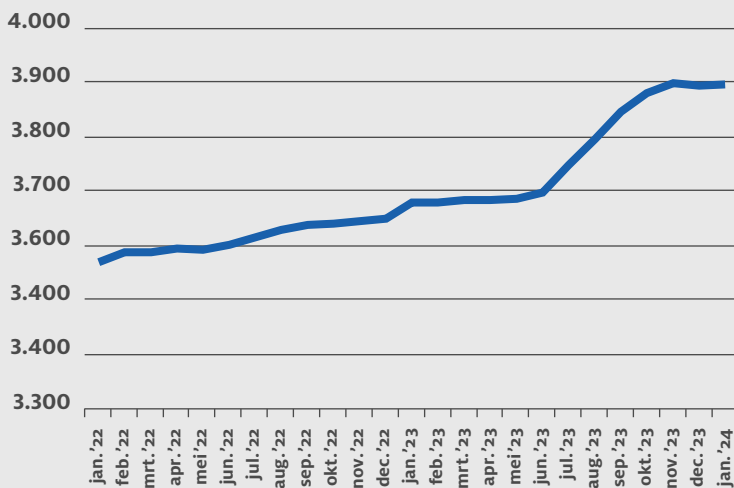


Fig. 8 | Ontwikkeling IPv6-adoptie (x 1 mln.)

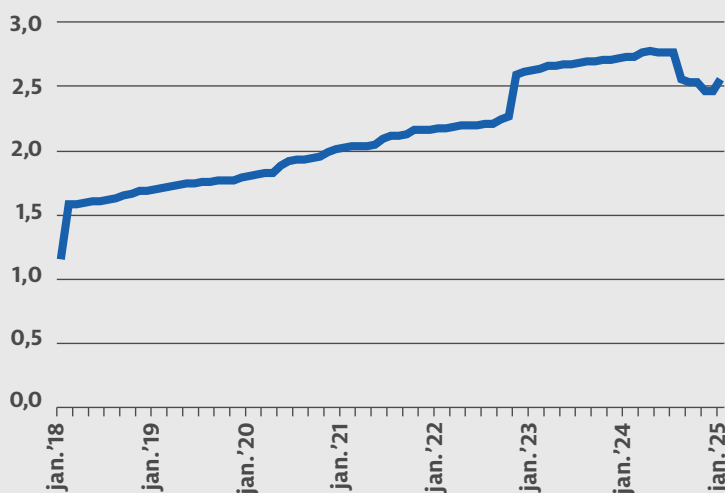
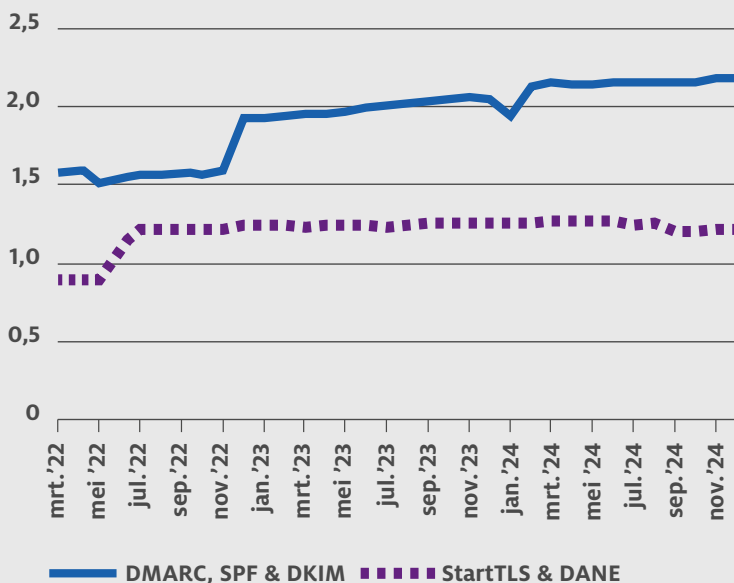


Fig. 9 | Veilige e-mailstandaarden (x 1 mln.)



SIDN Academy

Via het online platform SIDN Academy kunnen .nl-registrars kennis opdoen over een veilig en stabiel .nl-domein. We publiceerden een micro-learning over de veilige e-mailstandaarden StartTLS en DANE en over de Notice-and-Take-Down-procedure. Verder zijn alle e-learnings inmiddels ook in het Engels beschikbaar.

Faciliteren van verkoop van bestaande domeinnamen

Sinds 2023 draaiden we een pilot op sidn.nl, waarbij we de verkoop van domeinnamen faciliteerden. Als een bezoeker via onze .nl-suggestietool de status van een domeinnaam opvraagt en de domeinnaam is actief en 'te koop', dan verschijnt hierover een melding met uitleg. Uit de evaluatie van deze pilot begin 2024 bleek dat registrars hoofdzakelijk positief zijn, dus de functie blijft deel uitmaken van onze website. Zij kunnen de functie zelf implementeren in hun eigen domeinnaamsuggestietool.

Registrar Scorecard

De Registrar Scorecard (RSC) is ons incentive-programma voor .nl-registrars. Met financiële korting stimuleren we het actieve gebruik van domeinnamen en de adoptie van moderne, veilige en open internetstandaarden. Daarmee zorgen we voor een veiligere gegevensuitwisseling in de .nl-zone.

In 2024 introduceerden we geen nieuwe incentives binnen de RSC. Wel stimuleerden we net als voorgaande jaren de adoptie van IPv6 en DNSSEC en de e-mailstandaarden StartTLS, DANE, DMARC, DKIM en SPF. We verhoogden het percentage van de .nl-domeinnamen in het portfolio van registrars dat ondertekend moet zijn met DNSSEC als zij in aanmerking willen komen voor incentives van 10% naar 20%.

De incentive op IPv6 verlaagden we van 8 naar 6 cent per domeinnaam per halfjaar, omdat IPv6 steeds meer de standaard wordt. De totale waarde van financiële incentives was € 900.000,- in 2024 en de adoptie van alle standaarden bleef stabiel. Naast incentives krijgen registrars via de RSC ook inzicht in hun prestaties. Via hun eigen dashboard zien zij hun resultaten op het gebied van abuse-bestrijding en de kwaliteit van hun registratiedata. Ook in vergelijking met hun peers.

SIDN Panel

Ons SIDN Panel telde in 2024 ruim 550 leden, waaronder .nl-domeinnaamhouders, internet-gebruikers en ondernemers. Zij geven hun mening via enquêtes, zodat wij een beter beeld krijgen van ontwikkelingen in de markt en onze dienstverlening verder kunnen verbeteren. We vroegen de leden

onder andere naar cybercriminaliteit, de vindbaarheid van hun website in Google en hun voorkeur voor contentmanagementsystemen. De resultaten gebruikten we in onze artikelen en geven ons een beter beeld van trends die .nl raken. De gemiddelde respons per onderzoek was ongeveer 20%, ofwel zo'n 100 respondenten.

Resultaten uit het SIDN Panel geven ons een beter beeld van trends die .nl raken.

College voor Klachten en Beroep

In veruit de meeste gevallen verlopen de registratie en uitgifte van .nl-domeinnamen zonder problemen. Daar waar dat niet het geval is, kunnen .nl-domeinnaamhouders en registrars in beroep gaan bij het College voor Klachten en Beroep (CvKB) als zij het niet eens zijn met bepaalde beslissingen van SIDN. Ook behandelt dit college klachten over domeinnaamregistraties die in strijd zijn met de openbare orde of goede zeden. Dat wat we als samenleving moreel niet acceptabel vinden. Het CvKB deed in 2024 uitspraak over een beroep tegen een besluit van SIDN over een houderwijziging. Verder ontving het CvKB geen nieuwe beroepen of klachten.

> Lees [de uitspraken van het CvKB](#) op [cvkb.nl](#)

Geschillenregeling voor .nl-domeinnamen

Domeinnaamhouders kunnen te maken krijgen met onenigheden over een merk-, handels- of eigen naam of over namen van overheidsinstanties, verenigingen en stichtingen. In onze geschillenregeling voor .nl-domeinnamen staan alle afspraken over deze geschillen. Domeinnaamhouders en internetgebruikers kunnen de regeling voor een relatief laag bedrag gebruiken als alternatief voor een rechter. Sinds 1 september 2024 is een [nieuwe versie van de geschillenregeling](#) van kracht. In 2024 startten 51 zaken onder de geschillenregeling. Onze mediators behandelden 20 van deze zaken. In 9 gevallen zorgde onze bemiddeling voor een vroegtijdige oplossing voor het geschil.

Notice-and-Takedown-procedure

In de gedragscode Notice-and-Takedown (NTD) staat hoe de internetbranche meldingen over onrechtmatige en strafbare inhoud kan afhandelen. Denk

aan kinderporno, discriminatie, plagiaat of phishing-sites. De code is niet wettelijk verplicht, maar helpt partijen om zorgvuldig om te gaan met verzoeken om informatie van het internet te verwijderen. Samen met vele andere partijen uit de internetsector steunen wij de NTD-code. Bij meldingen over een .nl-website zijn wij een van de betrokken partijen. De persoon die het verzoek indient, doorloopt eerst enkele stappen, voordat wij de website onbereikbaar kunnen maken. We ontvingen 58 verzoeken die vielen onder de Notice-and-Takedown-procedure. We stelden 14 domeinnamen buiten gebruik en in de overige gevallen handelde een andere partij of was er geen sprake van (duidelijke) strafbare of onrechtmatige inhoud.

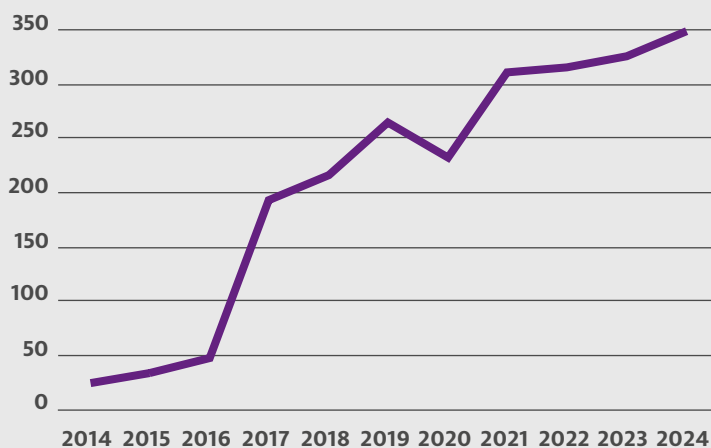
Europese NIS2-richtlijn

De Network and Information Security (NIS)2-richtlijn richt zich op digitale risico's voor netwerk- en informatiesystemen. De richtlijn moet de digitale en economische weerbaarheid van Europese lidstaten versterken. De NIS2 stelt onder andere eisen aan domeinnaamregistraties en de juistheid van bijbehorende data, zoals registratiegegevens. Registry's en registrars van domeinen in de Europese Unie moeten bijvoorbeeld verplicht het ingezette proces voor de verificatie van deze data in de Whois publiceren. Daarnaast beschouwt de NIS2 alle DNS-dienstverleners als aanbieder van essentiële diensten. Daardoor moeten zij, net als SIDN, voldoen aan strenge beveiligingseisen, meldplichten en nieuwe eisen rondom cybersecurity.

In dit kader bereidden we ons het verder voor op de richtlijn. We ontwikkelden samen met de VvR een aanpak voor de controle van registratiegegevens, die we voorlegden aan het ministerie van EZ. In 2025 willen we verdere stappen zetten in dit proces rondom registratiegegevens. Daarnaast richtten we een [online trust center](#) in. Hierop staan onder meer realtime informatie over onze security en de ISO27001:2022-certificering waaraan wij voldoen. Deze informatie hebben registrars nodig om te voldoen aan de richtlijn.

Op 17 oktober 2024 was de deadline voor de implementatie van de NIS2. Onze voorbereidingen op de NIS2 samen met registrars rondten we vóór deze deadline af. De belangrijkste reden voor de vertraging van de meeste lidstaten is dat de NIS2 veel ruimte laat in de vertaling naar de nationale wetgeving van de lidstaten. Dit zorgt voor discussie. Wel publiceerde de Rijksoverheid een conceptwetvoorstel voor online consultatie, dat goed laat zien hoe de overheid de wet interpreteert. In de voorlopige versie van deze Cyberbeveiligingswet staat dat het beleid en de procedures voor het verifiëren van domeinnamen zoveel mogelijk rekening moet

Fig. 10 | Aantal door SIDN Merkbewaking gemonitorde merknamen



houden met bestaande internationale normen en procedures. Denk aan het proces voor gegevens-validatie voor gTLD's.

De implementatie van de Cyberbeveiligingswet in Nederland duurt nog zeker tot het derde kwartaal van 2025. Toch is de NIS2 nu al merkbaar voor hosters en registrars, omdat zij vaak in meerdere lidstaten werken. Verschillende partijen nemen daarom stappen om controles zoals e-mailverificatie en het identificeren van houdergegevens uniform in Europa door te voeren, zodat de NIS2 voor hen werkbaar blijft.

Registrydiensten voor .amsterdam, .aw en .politie

Naast het beheren en managen van .nl zijn we registryserviceprovider voor de gTLD's .amsterdam en .politie en voor het landendomeinen .aw (Aruba). Ook leveren we DNS-diensten voor het .cw-domein (Curaçao) en het .dk-domein (Denemarken). In 2026 opent ICANN naar verwachting een nieuwe aanvraagronde voor gTLD's. Bedrijven en overheden kunnen dan een eigen extensie met hun naam aanvragen, zoals Amsterdam (.amsterdam) en Friesland (.frl) die al hebben.

In aanloop naar deze aanvraagronde onderzocht Markteffect in opdracht van ons hoe Nederlandse internetgebruikers denken over eigen domein-naamextensies. Uit het onderzoek blijkt dat er markt is voor domeinnaamextensies, vooral voor grotere Nederlandse steden en regio's. In dit kader werken we samen met Dotlocal, waarmee we Nederlandse partijen gaan ondersteunen bij het online brengen van nieuwe geografische topleveldomeinen (geoTLD's). Wij richten ons op de technische infrastructuur van de domeinen en Dotlocal op de marketing en het organisatiedeel.

SIDN Merkbewaking

Merkmisbruik kan de veiligheid van internet-gebruikers en de reputatie van de organisatie achter het merk schaden. Met onze monitoringsservice SIDN Merkbewaking kunnen organisaties, overheden en webwinkels hun merk beschermen. En zo de veiligheid voor hun online bezoekers en klanten en hun eigen organisatie vergroten. Via een persoonlijk dashboard krijgen gebruikers van SIDN Merkbewaking direct een melding bij de registratie van een domeinnaam die overeenkomt met of lijkt op hun merknaam, waarna zij meteen actie kunnen ondernemen. Waar dat kan, melden we ook gevonden domeinnamen onder andere toplevel-domeinen (TLD's). Met de module logodetectie geven we gebruikers inzicht in het gebruik van logo's op alle .nl-websites. Gebruikers kunnen als dat nodig is een beroep doen op juridische ondersteuning door de specialisten van ICTRecht en zelf actie ondernemen.

Inmiddels beschermt onze monitoringsservice ruim 350 merken, waaronder overheden, ziekenhuizen, banken, verzekeringsmaatschappijen en telecom-bedrijven. In 2024 voerden we kleine aanpassingen door in de gebruikersinterface. We vervingen onder meer IP-whitelisting door tweefactorauthenticatie, waarmee klanten vanaf elke locatie veilig kunnen inloggen. Ook investeerden we in het verbeteren van het algoritme in logodetectie. Daardoor kan de tool logo's sneller en nauwkeuriger herkennen.

SIDN Merkbewaking beschermt ruim 350 merken.

Datalek door onderhoudswerkzaamheden

Als gevolg van onderhoudswerkzaamheden aan sidn.nl waren in september registratiegegevens van 1.918 domeinnamen tijdelijk zichtbaar in de Whois. Het ging hier om de naam, adresgegevens, het e-mailadres en het telefoonnummer van de houder en de administratieve en technische contactpersoon. Deze gegevens mogen alleen zichtbaar zijn voor ons en de beherende registrar. We namen daarom contact op met alle contactpersonen van de 1.918 domeinnamen en meldden het incident direct bij de Autoriteit Persoonsgegevens en de RDI. Ook deden we onderzoek naar de impact, zodat we maatregelen kunnen treffen om dit in de toekomst te voorkomen. Het incident had voor zover bekend geen vervelende gevolgen voor de contactpersonen van de domeinnamen.

.nl Control 2.0

Met onze service .nl-control hebben .nl-domeinnaamhouders meer controle over hun domeinnaam. Zo moet de domeinnaamhouder altijd expliciet toestemming geven aan de .nl-registrar voor bijvoorbeeld het opheffen van een domeinnaam. De geplande lancering van .nl Control 2.0 in 2024 verviel, omdat we .nl-registrars de vernieuwde functies vanaf 2026 via Hello Registry kunnen aanbieden.

Vooruitblik

Samenwerken tegen online fraude

In 2025 werken we aan het sneller bestrijden van phishingmails. We stellen vaste criteria op, waaraan deze mails moeten voldoen om ze uit de lucht te halen. In het kader van online fraudebestrijding richten we ons ook op nieuwe samenwerkingen met bijvoorbeeld de Kansspelautoriteit en met toezichthouders in de medische sector en oliehandel. Cybercriminelen in de oliehandel gebruiken eenzelfde methode als bij nepwebwinkels, waarbij ze bedrijven via een .nl-website een aantrekkelijk aanbod doen en factureren voor niet-bestaande opslagcapaciteit.

Nieuwe tarieven

Door de relatief grote aanpassing van onze prijzen in 2024, is in 2025 alleen een inflatiecorrectie nodig. Met ingang van dat jaar verhogen we onze prijzen met 2,5%. De standaardprijs die een registrar betaalt voor een .nl-domeinnaam is dan € 4,25 per jaar en de registrarbijdrage is € 85,- per maand.

Vrij van privacy- en proxydiensten

Sinds 1 oktober 2023 geldt een verbod op het registreren van een .nl-domeinnaam op naam van een privacy- of proxydienstverlener of andere derde partij. Daarom monitoren we nieuwe registraties en werken we samen met privacy- en proxydienstverleners binnen .nl om bestaande registraties aan te passen. Ons doel is een .nl-zone die uiterlijk 1 oktober 2025 volledig vrij is van privacy- en proxydiensten.

Incentive voor security.txt

Vanaf 2025 nemen we een financiële incentive op in de RSC voor de toepassing van security.txt. Registrars krijgen dan een financiële beloning op .nl-domeinnamen waarvan de website een valide security.txt-bestand bevat. Aan het einde van 2024 was dit nog maar voor 2,8% van de .nl-websites het geval.

Implementeren NIS2-richtlijn

We blijven in gesprek met de VvR over hoe we registrars kunnen ondersteunen bij het implementeren van de NIS2-richtlijn en de daarop gebaseerde Cyberbeveiligingswet, vooral rondom het identificeren van houdergegevens. Ontwikkelingen rondom de richtlijn volgen we op de voet.

Registrydiensten via Hello Registry

Met Hello Registry richten we ons op het creëren van een netwerk van gelijkgestemde toplevelregistry's die zich inzetten voor innovatie, gedeelde waarden en het bouwen van een gemeenschap die nauw samenwerkt. Tijdens ICANN81 in Istanbul, waar we samen met CIRA de naam van het nieuwe registratieplatform onthulden, en de daaropvolgende weken kon Hello Registry op veel belangstelling rekenen van collega-registry's. Het doel is dan ook om na de migratie van .nl in 2026 ook andere ccTLD's op dit platform te onboarden. Zodat we collega-ccTLD's helpen aan een goede en stabiele oplossing en het internet veiliger maken. Samen met CIRA benaderen we geïnteresseerde partijen en zijn we aanwezig op evenementen om met ccTLD-registry's in gesprek te komen.

“De investeringen die ze daarvoor moeten doen, verdienen ze vervolgens dubbel en dwars terug.”



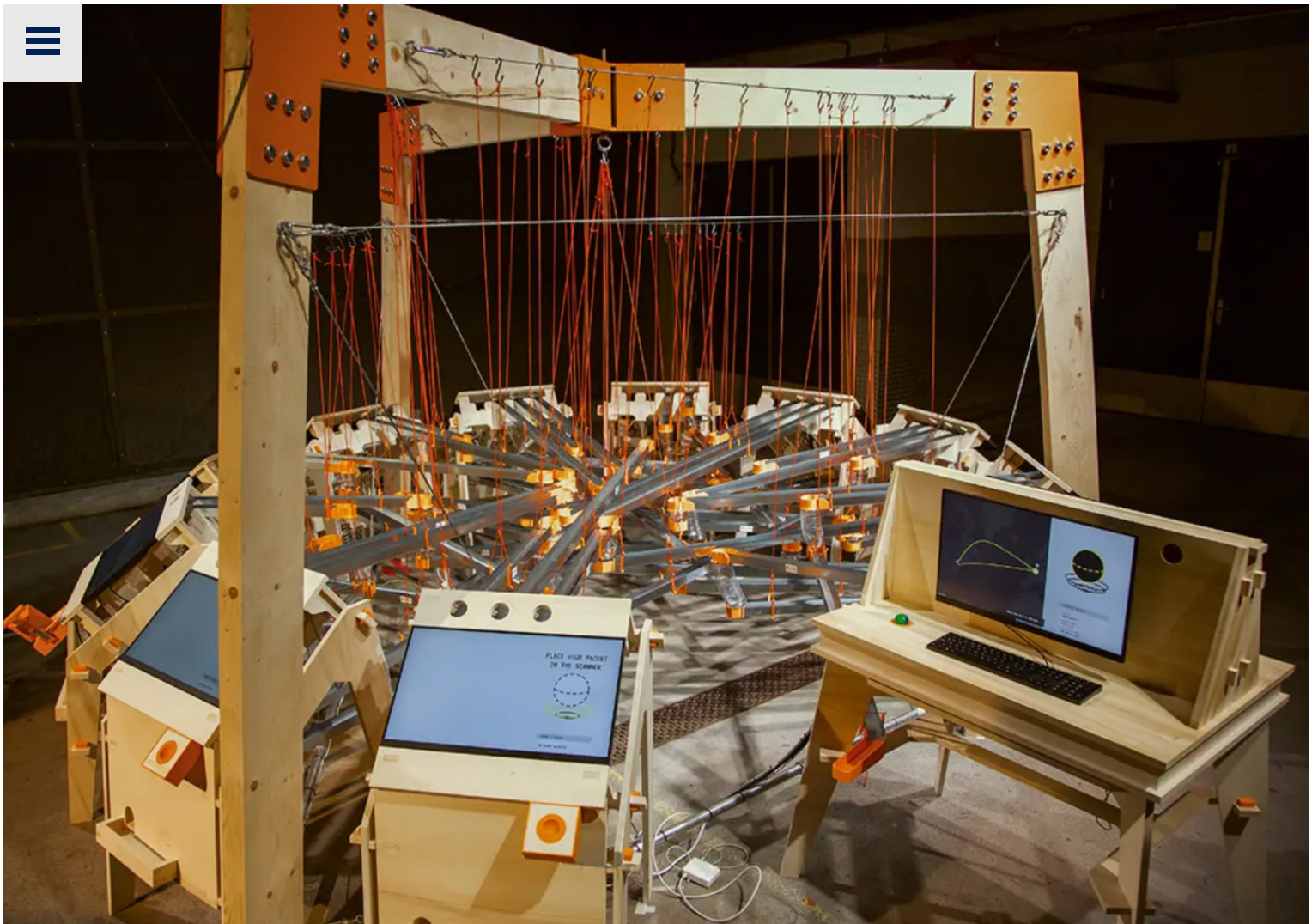
Gijs van der Linden

Teamleider Landelijk Meldpunt Internetoplichting van de politie

Elk uur nieuwe slachtoffers

“Het aantal aangiftes van aan- en verkoopfraude bij webshops omhoog blijft gaan. Van 2023 naar 2024 stegen die van 16.000 naar zo’n 20.000. En dan moet je er ook nog eens rekening mee houden dat naar schatting maar 1 op de 5 slachtoffers aangifte doet. Sommige scams zijn echt heel professioneel opgezet. Dan bouwen criminelen bijvoorbeeld tot in detail een bekende webwinkel na. De investeringen die ze daarvoor moeten doen, verdienen ze vervolgens dubbel en dwars terug. Elk uur dat een malafide webwinkel langer in de lucht is, vallen er nieuwe slachtoffers. Daarom sluiten SIDN en het Landelijk Meldpunt Internetoplichting (LMIO) van de politie een overeenkomst. Op basis hiervan kan SIDN zonder verder onderzoek webshops offline halen, als LMIO heeft vastgesteld dat er sprake is van oplichting.”

> Lees meer over [de samenwerking tussen LMIO en SIDN](#)



Onze publieke rol voor de Nederlandse en wereldwijde internetgemeenschap

4 Een veilig, stabiel en toekomstvast internet

Een veilig internet is een sleutelvoorwaarde voor zorgeloos gebruik daarvan. Zeker nu we hier steeds meer afhankelijk van zijn. Daarom werken we aan een veilig, stabiel en toekomstvast internet voor Nederland, Europa en de wereld. Onze focus ligt in het bijzonder op het .nl-domein voor de Nederlandse samenleving. SIDN Labs voert daarvoor toegepast technisch onderzoek uit om de veiligheid van de internetinfrastructuur verder te verhogen. Vanuit SIDN fonds investeren we in projecten gericht op een inclusief, veilig en verbindend internet. Bovendien bundelen SIDN Labs en SIDN fonds hun krachten met partners en onderling, zoals met het programma Internet Infrastructuur in Beeld.

SIDN Labs

De rol die het internet vandaag de dag speelt is cruciaal. Moderne digitale samenlevingen zijn sterk afhankelijk van een veilige internetinfrastructuur. Deze onmisbare laag transporteert data van A naar B over het internet, meestal via meerdere netwerken. Onze onderzoeksafdeling SIDN Labs werkt aan het verder verbeteren van de veiligheid van deze infrastructuur voor Nederland, Europa en daarbuiten door toegepast technische onderzoek. De onderzoeksagenda van SIDN Labs is gericht op 3 hoofdthema's: domeinnaamsecurity, infrastructuursecurity en emerging internettechnologieën. Het team werkt samen met universiteiten, infrastructuuroperators en andere onderzoekscentra aan zowel korte- als langetermijnprojecten. Binnen de onderzoeken is bijzondere aandacht voor de operationele uitdagingen van SIDN en .nl. Onderzoeksresultaten zijn publiek beschikbaar en breed toepasbaar, zodat belanghebbenden hiermee hun eigen bijdrage kunnen leveren aan een sterk internet.

SIDN Labs brengt onderzoek en praktijk samen en slaat een brug tussen de onderzoeks- en operationele wereld. In 2024 gaven we de vakken Advanced Networking en Security Services for the Internet of Things aan de Universiteit Twente (UT) en gaven we gastcolleges aan de Universiteit Leiden en de UT. Ook werkten we nauw samen met de UT binnen het samenwerkingsverband Twente University Centre for Cybersecurity Research (TUCCR). We leveren kennis op het gebied van cybersecurity, die TUCCR gebruikt voor onderzoeksprojecten en de ontwikkeling van nieuwe oplossingen. Ook begeleidde we 5 MSc-studenten en 3 PhD-studenten. Net als voorgaande jaren leenden we 4 teamleden 1 dag per week uit aan universiteiten voor gezamenlijk onderzoek en onderwijs: de Technische Universiteit Delft (1 collega), de Universiteit van Amsterdam (1 collega) en de UT (2 collega's). Daarnaast zijn we actief betrokken bij Internet.nl en onderzoekers van SIDN Labs maken deel uit van de raad van advies van SIDN fonds, van 2 werkgroepen binnen de IETF en van de Root Server System Advisory Committee (RSSAC) van ICANN. De SIDN Labs-directeur is lid van de Cyber Security Raad (CSR) van het kabinet. Als lid geeft hij namens de wetenschappelijke community mede richting aan het veiliger maken van de Nederlandse en Europese digitale infrastructuur.

Enkele projecten van SIDN Labs in 2024

Post-kwantumcryptografie in het DNS

In het project PATAD (Post-quantum Algorithm Testing and Analysis for the DNS) brengen we empirisch de impact van post-quantum cryptography (PQC) op DNSSEC in kaart. In 2024 maakten we de software van het PATAD-testbed opensource beschikbaar voor andere DNS-onderzoekers en operators. Met onze software kunnen zij met de PQC-algoritmes MAYO, Falcon en SQCSign in het DNS experimenteren. Zij kunnen op programmatische wijze realistische DNS-topologieën nabootsen en evalueren hoe DNSSEC met PQC werkt. De 3 algoritmen maken deel uit van het evaluatie- en standaardisatieprogramma voor PQC-algoritmen van het National Institute of Standards and Technology (NIST). Ook voerden we zelf metingen uit op ons testbed, zoals het vergelijken van het ondertekenen van verschillende DNS-zonebestanden met MAYO en Falcon en met de 2 traditionele algoritmes RSA en ECDSA.

DDoS-clearinghouse

Het systeem DDoS-clearinghouse maakt DDoS-fingerprints waarmee overheden, banken, internetproviders en andere vitale aanbieders automatisch onderling informatie over DDoS-aanvallen kunnen delen. Zo zijn zij voorbereid op deze aanvallen.

Sinds april 2024 draait het DDoS-clearinghouse bij de Nationale Beheersorganisatie Internet Providers (NBIP) onder de vlag van de Nederlandse Anti-DDoS Coalitie (NL-ADC). Vanuit SIDN Labs leidden we de afgelopen jaren het onderzoek voor en de ontwikkeling van het clearinghouse samen met vooral SURF en de Universiteit Twente. Het technische peer-reviewed blad IEEE Communications Magazine publiceerde ons artikel over het DDoS-clearinghouse, dat we samen met SURF en de UT schreven.

Het peer-reviewed blad IEEE Communications Magazine publiceerde ons artikel over het DDoS-clearinghouse.

Autocast

Autocast staat voor de automatisering van anycast. Het is een observatieplatform voor DNS-operationsteams, zoals die van SIDN. Het platform levert geautomatiseerde aanbevelingen voor bijvoorbeeld het af- en bijschakelen van .nl-anycastnodes of -sites. Dit doet het platform op basis van veel gedetailleerdere internetmetingen, zoals land, regio en round-triptijd, dan de traditionele monitoringsystemen. Autocast gebruikt daarvoor passieve en actieve internetmetingen uit ons opensourcedataplatform ENTRADA en de software Verfploeter.

Op basis van ENTRADA-data verbeterden we het inzicht in de round-trip time van .nl-query's: het aantal milliseconden dat een DNS-vraag nodig heeft om bij een DNS-server te komen plus de tijd die het DNS-antwoord onderweg is terug naar de vrager. Ook draaiden we samen met het DNS-team van SIDN dagelijks actieve internetmetingen vanaf de productionnameservers van .nl. Met de resultaten konden we de status van .nl in het DNS beter beoordelen en de plaatsing van de .nl-nameservers verder optimaliseren.

RESTful Provisioning Protocol

Het Extensible Provisioning Protocol (EPP) is een protocol voor het beheren van domein-naamobjecten in een registry, bijvoorbeeld om domeinnamen te updaten. EPP is gestandaardiseerd door de IETF en gebaseerd op Extensible Markup Language (XML). Het is een stateful protocol dat gebruikmaakt van het concept van een 'sessie', waarmee de EPP-server informatie over de client bijhoudt. Het is hiermee lastig om goed schaalbare systemen te ontwikkelen die snel een groot aantal EPP-berichten kunnen verwerken. EPP bestaat al zo'n 15 jaar en SIDN volgt deze standaard voor .nl sinds 2010.

Het RESTful Provisioning Protocol (RPP) is een door ons geïnitieerde standaard in ontwikkeling voor een nieuwe domeinnaamregistratie-API. RPP is eenvoudiger in gebruik voor registrars dan EPP en biedt verhoogde schaalbaarheid en betere prestaties en beveiliging voor registry's. Ook is RPP een stateless protocol, wat beter aansluit bij nieuwe software-engineeringtechnologieën, zoals containerisatie en Kubernetes. De verdere ontwikkeling van RPP is een doorstart van ons werk uit 2012.

Tijdens IETF121 in Dublin organiseerden we een bijeenkomst met engineers van onder meer Europese collegaregistry's die interesse hebben in RPP. Er was voldoende overeenstemming om een nieuwe IETF-werkgroep te starten. We maakten samen met de community een start met het charter, waarin de basisprincipes voor de werkgroep staan.

DNS-rootservers

In samenwerking met NLnet Labs voerden we onderzoek uit voor de rootserveroperators Verisign en ISC. Daarbij controleerden we onafhankelijke ICANN-metingen die aangaven dat het rootserversysteem regelmatig haar vereiste beschikbaarheidsniveau niet haalde. Ons onderzoek liet zien dat het ICANN-meetplatform en het netwerkpad tussen het meetplatform en de rootservers de meeste problemen veroorzaakten. Ook ontdekten en verhielpen we een fout in de meetsoftware die de responsetijden van de rootservers slechter weergaven dan ze daadwerkelijk waren. We sloten het project naar tevredenheid van de rootserveroperators af. Met dit derde onderzoek naar de veiligheid en stabiliteit van de DNS-root laten we zien dat we inmiddels worden gezien als experts op dit gebied.

RegCheck

Ons machinelearningsysteem RegCheck kent risicoscores toe aan nieuwe domeinnaam-registraties, zodat ons supportteam en die van andere registry's potentieel malafide domeinnamen op moment van registratie kunnen herkennen. We stapten over op een nieuw classificatiealgoritme dat is gebaseerd op beslisbomen. Ook maakten we het dashboard van RegCheck gebruiksvriendelijker en koppelden we RegCheck aan Microsoft Dynamics 365. Zo kan het supportteam sneller houderonderzoeken starten op basis van RegCheck-scores.

Verder moderniseerden en automatiseerden we de uitrol en training van RegCheck. Daardoor is het systeem flexibel inzetbaar op elk modern computingplatform. We deelden de RegCheck-software met enkele geïnteresseerde registry's, zodat ze het in hun systemen kunnen opnemen en gebruiken.

Onderzoek naar phishing binnen .nl, .be en .ie

In september 2024 publiceerden we samen met DNS Belgium (de registry van .be), IE Domain Registry (de registry van Ierland) en de universiteiten van Twente, Delft, Leuven en Grenoble een peer-reviewed artikel over ons onderzoek naar de evolutie van phishing-aanvallen. In totaal analyseerden we 28.754 phishingmeldingen in het .nl-, .be- en .ie-domein afkomstig van securitybedrijf Netcraft in de periode 2013 tot 2023. Ook vergeleken we het registratie- en mitigatiebeleid van de 3 domeinen.

We presenteerden de onderzoeksresultaten tijdens meerdere bijeenkomsten in de operator-community, waaronder RIPE, DNS-OARC en CENTR. Maar ook tijdens ACM Computer and Communications Security, een bekende wetenschappelijke topconferentie waarvoor ons paper werd geaccepteerd.

We analyseerden ruim 28.000 phishingmeldingen van securitybedrijf Netcraft.

BGP-security

BGP (Border Gateway Protocol) routeert data van bron naar bestemming over de ruim 75.000 netwerken die samen het internet vormen. De security van BGP is cruciaal voor het hele internet, waaronder voor andere kernsystemen zoals het DNS. Helaas lossen bestaande technieken om de veiligheid van BGP te verhogen nog niet alle problemen op. Daarom voegden we BGP-security in 2024 aan ons onderzoeksportfolio toe.

We ontwikkelden een onderzoeksagenda voor BGP-security en versterkten onze samenwerking met de Universiteit Twente op dit gebied. Met hen lieten we bijvoorbeeld zien dat het internet langdurig last heeft van het fenomeen 'serial hijackers': netwerken die regelmatig het verkeer bestemd voor andere netwerken ongeautoriseerd naar zich toe proberen te trekken. Daarnaast onderzochten we welke routerimplementaties BGPsec ondersteunen en hoe we een lokaal BGPsec-testbed inrichten, waarmee we kunnen experimenteren.

Weerbaarheid van kritieke en vitale diensten in Nederland

We onderzochten de weerbaarheid van de DNS-infrastructuur van alle 6,2 miljoen .nl-domeinnamen en 700 organisaties in verschillende sectoren, die kritieke of vitale diensten leveren. Dat deden we door het gebruik van 3 bewezen effectieve maatregelen te meten die de beschikbaarheid van DNS-servers verhogen: het verspreiden van DNS-servers over meerdere netwerken, het gebruik van anycast en het gebruik van meerdere IP-prefixen. Dit zijn groeperingen van IP-adressen.

De resultaten presenteerden we op het ECP Jaarfestival, waar traditioneel ook veel beleids-makers komen. Onze meetsoftware maakten we opensource beschikbaar, zodat organisaties zoals ziekenhuizen zelf hun DNS-weerbaarheid kunnen testen.

Internetsancties tegen Russische media

Via het DNS onderzochten we of EU-sancties om Russische media te blokkeren effectief zijn. Bij dit onderzoek werkten we samen met onderzoekers van de Universiteit van Twente, de University of Illinois Chicago, de Universiteit van Amsterdam en de non-profitorganisatie Open Observatory of Network Interference. De resultaten bundelden we in een peer-reviewed artikel dat experts beoordeelden. Een van onze partners presenteerde dit tijdens de conferentie Free and Open Communications on the Internet.

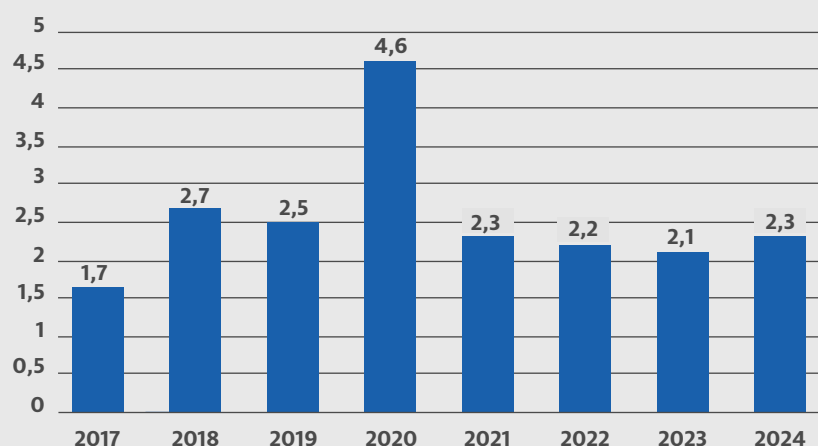
Onze studie illustreert hoe internetmetingen kunnen helpen bij het evalueren van beleid, in dit geval vanuit de Europese Unie. Het is daarbij belangrijk expertises te combineren, in ons geval internetmetingen met expertise rondom Europese en mediastudies.

Met internetmetingen dragen we bij aan het ontwikkelen en evalueren van beleid.

SIDN fonds

Het internet is van grote waarde voor onze huidige en toekomstige maatschappij. Daarom zet SIDN fonds zich in voor een sterk internet voor iedereen. Het fonds steunt innovatieve projecten die bijdragen aan een open, vrij en betrouwbaar internet. De focus ligt op 3 gebieden: een sterk internet, sterke internetgebruikers en de maatschappelijke kant van het internet.

Fig. 11 | Jaarlijkse bijdrage aan SIDN fonds (x 1 mln.)



In 2024 bestond SIDN fonds 10 jaar. Sinds de oprichting steunde het fonds al meer dan 400 projecten, onder meer rondom desinformatie, online weerbaarheid en digitale toegankelijkheid. Een bedrag van bijna € 15 miljoen ging naar deze kansrijke projecten en zo'n € 800.000,- ging naar wetenschappelijk onderzoek. Ook zette het fonds belangrijke samenwerkingsprojecten op, bijvoorbeeld met gemeenten, het ministerie van Binnenlandse Zaken (BZK) en andere fondsen met gemeenschappelijke doelen.

In maart 2024 schreef SIDN fonds de call 'Duurzaam internet' uit voor grote projecten en kleinere pioniersprojecten. Initiatiefnemers konden een voorstel indienen gericht op het verbeteren van de duurzaamheid van het internet of het verminderen van de milieu-impact ervan. Binnen de call gingen 4 projecten van start met de steun van SIDN fonds, waarvan 2 pioniers. Binnen de tweede call 'Meedoen in de Digitale Samenleving' kregen 6 projecten financiering van SIDN fonds. Initiatiefnemers konden een voorstel indienen gericht op het verbeteren van vaardigheden van mensen die niet goed meekomen in de digitale samenleving. Daarnaast konden pioniersprojecten weer het hele jaar door een open aanvraag indienen voor een bijdrage tot € 10.000,-. Net als voorgaande jaren scoutte het fonds projecten met een maatschappelijk belang en die de potentie hebben om impact te maken op een van de 3 aandachtsgebieden.

Driejaarlijkse evaluatie

In 2024 vond de driejaarlijkse evaluatie van SIDN fonds plaats. De raad van advies en stakeholders waren onder andere positief over de aanpak van SIDN fonds. Deze leverde projecten en coalities op met zichtbare impact, zoals de vermenigvuldiging van de financiering van SIDN fonds in de vorm van bedragen die samenwerkingspartners toekenden. Hierdoor kon het fonds projecten met een bredere reikwijdte en impact steunen. Mogelijke verbeterpunten zijn het beter bekendmaken van het pioniersinstrument, het efficiënter inrichten van samenwerkingsprogramma's, het verbeteren van het scoutingproces, meer investeren in de verbinding met registrars en het versterken van de strategische communicatie.

Verder noemden de raad van advies en stakeholders de noodzaak van een stevige financiële basis. Zij adviseren dan ook om de inzet van bredere fondsenwerving en de richting van meerjarige programma's met andere partijen in het veld te verkennen.

Samenwerking tussen SIDN fonds en SIDN Labs

In augustus ging het programma Internetinfrastructuur in Beeld van start. Dit is een samenwerking tussen SIDN fonds en SIDN Labs om het bewustzijn over het belang van de digitale infrastructuur bij stakeholders te vergroten, zoals politici en journalisten. Binnen dit programma maken 3 designers interactieve visualisaties van de digitale infrastructuur: het simulatiespel Packet Panic, de online visualisaties 'Zijn we al digitaal autonoom?', 'de Border Gateway Protocol Travel Guide' en 'Hoe het net werkt'. Het programma is geïnspireerd op de grootschalige internetmetingen die onderzoekers van bijvoorbeeld SIDN Labs, de UT en de TU Delft doorlopend uitvoeren.

Scriptieprijs Responsible Internet

Freedom Internet, Mijndomein, SIDN fonds en de Koninklijke Academie voor Wetenschappen stimuleren een verantwoord internet met de Scriptieprijs Responsible Internet. Deze prijs gaat jaarlijks naar (voormalige) masterstudenten die onderzoek doen naar een verantwoord internet waar veiligheid, privacy en toegankelijkheid centraal staan. In 2024 was de eerste prijs van € 3.000,- voor een wetenschappelijk onderzoek naar regelgeving voor influencers die reclame maken op sociale media. De tweede prijs van € 1.000,- ging naar een onderzoek over het zonder toestemming delen van persoonlijke gegevens door online apotheken in Europa.

Enkele projecten die SIDN fonds in 2024 steunde

Grid-aware-websites

Bij het laden van een website verbruiken de servers en het apparaat van de gebruiker elektriciteit. De CO₂-uitstoot die dat veroorzaakt, is onzichtbaar. The Green Web Foundation bouwt daarom een opensourcetoolkit, waarmee webontwikkelaars hun websites grid-aware maken. Dit betekent dat websites slim reageren op de CO₂-uitstoot per kilowattuur en het energieverbruik van het elektriciteitsnet. Via software waarmee 2 applicaties met elkaar communiceren (API's), halen webontwikkelaars gegevens op over het elektriciteitsnetwerk van de websitegebruiker. Met deze data kunnen zij milieubewuste aanpassingen doen in het ontwerp. SIDN fonds financiert dit volledige project vanuit de call 'Duurzaamheid' uit 2024.

De opensourcetoolkit van The Green Web Foundation maakt websites grid-aware.

DigiPad

DigiPad helpt jongeren in de jeugdzorg, jeugddetentie en speciaal onderwijs bij het ontwikkelen van essentiële digitale vaardigheden in een veilige en toegankelijke leeromgeving. Het project werd toegekend binnen de call 'Meedoen in de digitale samenleving' uit 2024. Met het onlineprogramma kunnen jongeren hun weerbaarheid vergroten en zelfstandiger deelnemen aan de digitale maatschappij. De oprichters ontwikkelden DigiPad in samenwerking met Justitiële Jeugdinrichting Lelystad. SIDN fonds financiert de doorontwikkeling en bredere uitrol.

Campagne Zorgeloos verbinden

In Nederland maken dagelijks veel mensen gebruik van openbare wifi-netwerken, die lang niet altijd veilig en zonder risico zijn. De gemeenten Amsterdam, Eindhoven, Den Haag en Rotterdam richten daarom samen met Publicroam de campagne 'Zorgeloos verbinden' op. Gezamenlijk met de steden ondersteunt en financiert SIDN fonds dit initiatief. Daardoor kunnen lokale partijen, zoals musea, sportlocaties en culturele instellingen, kosteloos kennismaken met de veilige en privacyvriendelijke wifi-roamingdiensten van Publicroam.

Opensource AI-auditing

SIDN fonds steunt samen met het ministerie van BZK het project Opensource AI-auditing dat voortbouwt op eerder ontwikkelde tools door de stichting Algorithm Audit. Deze tools helpen bij het identificeren van normatieve vraagstukken bij de inzet van algoritmische systemen, bijvoorbeeld over wat ethisch is. Het project omvat de ontwikkeling van 2 technische opensourcetools om voordelen in algoritmische systemen te detecteren en te migreren. Ook werken de initiatiefnemers een kwalitatieve werkwijze uit, ofwel algorithmprudentie, om vragen over verantwoorde inzet via overleg af te handelen.

Unlock digitale weerbaarheid

In oktober 2024 lanceerden Nederlandse stichtingen en bedrijven, de politie en de overheid de landelijke campagne Unlock Digitale Weerbaarheid. De Nationale Cursus Digitale Weerbaarheid is hier een groot onderdeel van en werd ontwikkeld met de steun van SIDN fonds. De cursus helpt internetgebruikers bij het herkennen van onveilige online situaties. Bovendien vergroten zij hun kennis over bijvoorbeeld online oplichting, cybersecurity, nepnieuws en online polarisatie.

De Nationale Cursus Digitale Weerbaarheid helpt internetgebruikers bij het herkennen van onveilige online situaties.

Digitaal autonoom

De Nederlandse maatschappij is steeds meer afhankelijk van niet-Europese technologie. Gegevens worden opgeslagen in clouddiensten, waarover we zelf minder controle hebben.

Het project ‘Zijn we al digitaal autonoom?’ brengt in kaart welke Nederlandse organisaties afhankelijk zijn van welke leveranciers en technologie. Deze gegevens maken de afhankelijkheid op grote schaal inzichtelijk en laten zien wat de impact hiervan is op individuen. Maar ook waar kansen liggen rondom het versterken van onze digitale autonomie.

Hash Check Service van Offlimits

Offlimits bestrijdt online seksueel misbruik en werkt aan een veiligere onlinewereld. Het expertisecentrum biedt onder andere de Hash Check Service (HCS) aan, oorspronkelijk een initiatief van de Europese Commissie. Hiermee kunnen gebruikers data scannen op bekend beeldmateriaal van seksueel misbruik van minderjarigen. Dat doen zij via beschikbare hash-lijsten, bijvoorbeeld die van het National Center for Missing and Exploited Children en van de Nederlandse politie. Het project richt zich op het vergroten van het bereik van HCS, het verbeteren van de kwaliteit van de hashes en het inrichten van een duurzame governance en financiering. Hoe meer bedrijven zich aansluiten, hoe hoger het aantal afbeeldingen dat proactief wordt verwijderd. Samen met het ministerie van Veiligheid en Justitie financiert SIDN fonds dit project.

Vooruitblik

SIDN Labs

Post-kwantumcryptografie in het DNS

Samen met SURF en de UT voeren we metingen uit op ons PATAD-testbed. Hiermee bepalen we welke nieuwe en nog niet gestandaardiseerde PQC-algoritmes mogelijk geschikt zijn voor DNSSEC. Dit koppelen we vervolgens terug aan het NIST en de internetgemeenschap. Ook breiden we het PATAD-testbed verder uit. De analyses en resultaten uit de metingen publiceren we in een of meer technische rapporten en peer-reviewed artikelen in samenwerking met SURF en de UT.

Autocast

Een van onze doelen is Autocast breder beschikbaar maken voor DNS-operators. In 2025 opensourcen we de Autocast-dashboards en het datamodel daarachter als extensie van ENTRADA. Ook ontwikkelen we Autocast door van een observatiedashboard naar een anycastcontrolecentrum. Zowel voor ons eigen DNS-team als voor andere DNS-operators, zodat zij hun anycastplatform effectiever kunnen inzetten voor de verdeling van verkeer over verschillende locaties.

RESTful Provisioning Protocol

In 2025 werken we het charter voor RPP verder uit samen met de community en schrijven we mee aan de standaard.

RegCheck

Een van onze plannen is het verbeteren van de risicoscores in RegCheck met DNS-querydata, zoals het IP-adres van de resolver en het type query. Ook onderzoeken we of we phishing en malafide websites sneller kunnen vinden met informatie uit onze webcrawler DMAP (Domain Name Ecosystem Mapper). We blijven in gesprek met registry's en registrars die mogelijk geïnteresseerd zijn in de RegCheck-software.

We verhuizen de onderzoeks- infrastructuur van SIDN Labs naar Nikhef en SURF.

Vervolgstudie naar phishing

In 2025 werken we aan een vervolg van ons phishingonderzoek. Naast de registry's van .be en .ie betrekken we ook die van .eu en .br bij deze studie.

Onderzoeksinfrastructuur

In 2025 verhuizen we de onderzoeksinfrastructuur van SIDN Labs naar onderzoeksinstituut Nikhef in Amsterdam. Daar hebben we bijvoorbeeld de beschikking over een eigen Autonomous System, waarmee we zelf BGPsec-software kunnen installeren om daar vervolgens mee te experimenteren. De DNS-query-data die we voor onze onderzoeken gebruiken, slaan we op bij SURF, de operator van het Nederlandse onderzoeks- en onderwijsnetwerk. Via een snelle verbinding met SURF maken we de data toegankelijk op onze servers bij Nikhef. In dit kader voegen we in 2025 ook een nieuwe lijn toe aan onze onderzoeksagenda: research infrastructure operations. Onze activiteiten binnen dit thema richten we op het beheren en continu verbeteren van ons onderzoeksnetwerk.

SIDN fonds

SIDN fonds brengt een themacall uit gericht op verantwoord gebruik van AI in de praktijk, in samenwerking met Topsector ICT. De tweede call heet 'Grip op Polarisatie 2', in samenwerking met Limelight Foundation en Gieskes Strijbis Fonds. Pioniersprojecten kunnen ook het hele jaar door een open aanvraag tot € 10.000,- indienen die past bij een van de 3 focusgebieden. Verder scout het fonds zelf kansrijke projecten die hierbij aansluiten. SIDN fonds nodigt in het bijzonder projecten uit die zich inzetten voor duurzaamheid, toegankelijkheid en veiligheid. Ten slotte zet het fonds de sponsoring van de Scriptieprijs Responsible Internet en de samenwerking met SIDN Labs voort. Bijvoorbeeld rondom het programma Internet Infrastructuur in Beeld.

“Veel .nl-domeinnaam-beheerders nemen beschikbaarheidsmaatregelen, maar het kan nog beter.”



**Moritz Müller, Thijs van den Hout,
Caspar Schutijser**

Research engineers bij SIDN Labs

Kan digitaal Nederland tegen een stootje?

“Verstoringen van de digitale infrastructuur kunnen maatschappelijk ontwrichtend zijn, zoals de NAFIN-storing in 2024 liet zien. Daarom deden we bij SIDN Labs onderzoek naar de weerbaarheid van digitaal Nederland. We verrichtten daarvoor metingen aan de publieke DNS-infrastructuur van meer dan 700 organisaties op het internet en alle 6,2 miljoen .nl-domeinnamen, om te meten in hoeverre verschillende maatregelen genomen zijn tegen storingen en aanvallen. Veel organisaties in Nederland lijken aandacht te besteden aan maatregelen die de weerbaarheid van hun DNS-servers verhogen, maar we lieten ook zien dat eigenaren van domeinnamen vaak meer kunnen doen, bijvoorbeeld in de ziekenhuissector. We publiceren de meettool die we hiervoor ontwikkelden, zodat organisaties deze analyse ook zelf kunnen maken.”

› Lees meer over [het onderzoek](#)

“Experimenteer met grid-aware-websites voor een duurzamer internet.”



Hannah Smith

Operationeel directeur bij The Green Web Foundation

Project SIDN fonds: Grid-Aware Websites

“Elke keer dat je een website laadt, verbruiken de servers en het apparaat van de gebruiker elektriciteit. De CO₂-uitstoot die dat veroorzaakt, is onzichtbaar. Tegelijkertijd is een oplossing niet eenvoudig, want elektriciteitsnetwerken zijn behoorlijk complex. Daarom bouwt The Green Web Foundation een opensourcetoolkit, waarmee webontwikkelaars hun websites laten reageren op het net waarvan ze stroom afnemen, zodat ze grid-aware worden. We streven naar een fossielvrij internet in 2030. Dankzij de steun van SIDN fonds kunnen ontwikkelaars nu experimenteren met grid-aware-websites, wat eerder niet mogelijk was.”

> Lees meer over [dit project van SIDN fonds](#)



Nationale en internationale partnerschappen
vanuit gedeelde waarden

5 Samenwerken voor de internetgebruiker

Partnerschappen zijn van onmiskenbare waarde voor één wereldwijd veilig en open internet. Bovendien zijn ze nodig om technologische innovaties te versnellen en op brede schaal impact te maken. Want het internet is het grootste samenwerkingsverband ter wereld, waar iedereen een eigen én gezamenlijke verantwoordelijkheid heeft om het door te ontwikkelen. Daarom delen we onze expertise en onderzoeksresultaten met andere partijen in de internet- en academische wereld, bijvoorbeeld op het gebied van abusebestrijding en cybersecurity. We nemen een actieve rol in internationale internetgovernance en technische fora, zoals IGF, ICANN en IETF. Ook steunen we initiatieven die misbruik op het internet bestrijden en de waarde ervan vergroten.

Bijdragen aan organisaties en conferenties

We zijn sterk gericht op samenwerken binnen Nederland, de Europese Unie en daarbuiten. Zo spelen we een actieve rol in verschillende internationale fora, waarvan we de belangrijkste uitlichten in dit jaarverslag.

ICANN

De Internet Corporation for Assigned Names and Numbers (ICANN) voert een aantal belangrijke internetgerelateerde taken uit. Denk aan het bepalen van het beleid voor de uitgifte van gTLD's, zoals .com, .net en .shop en de distributie van IP-adressen. Een belangrijke functie voor SIDN, het beheer van de 'root' en het rootserversysteem, wordt uitgevoerd door ICANN's affiliate IANA. We spelen een actieve rol in meerdere werkgroepen, waaronder vooral de ccNSO (country code Name Support Organization). Dit is de structuur voor registry's van landencodes binnen ICANN.

In 2024 organiseerden we samen met het ministerie van EZ de Nederlandse pre-ICANN-sessies voor belanghebbende partijen. Ook organiseerde ICANN weer 3 meetings. ICANN79 vond plaats in maart in San Juan, Puerto Rico, ICANN80 in juni in Kigali, Rwanda en ICANN81 in november in Istanbul, Turkije. De sessies stonden vooral in het teken van de nieuwe aanvraagronde voor gTLD's in 2026 en de bestrijding van abuse. Tijdens ICANN81 in Istanbul lanceerden we Hello Registry voor alle aanwezige registry's, registrars en andere partijen. SIDN Labs gaf een presentatie over het onderzoek naar post-kwantumcryptografie in het DNS.

RIPE NCC

RIPE Network Coordination Centre (NCC) is onder andere verantwoordelijk voor de uitgifte van IP-adressen aan internetserviceproviders en andere instanties voor Europa, het Midden-Oosten en delen van Centraal-Azië. RIPE organiseerde 2 fysieke meetings in 2024, waar wij ook aan deelnamen. RIPE 88 vond plaats in mei in Krakau, Polen en RIPE 89 vond plaats van eind oktober tot begin november in Praag, Tsjechië. Een teamlid van SIDN Labs is covoorzitter van de DNS-werkgroep bij RIPE. Een andere SIDN Labs-collega schreef in 2024 mee aan het RIPE-rapport 'DNS Resolver Recommendations' (RIPE-823) op basis van ons eigen werk aan DNS4ALL.

IETF

De Internet Engineering Task Force (IETF) houdt zich bezig met de evolutie van internet-protocollen en de internetarchitectuur en het verbeteren van de werking van het internet. Verschillende netwerkoperators, -ontwerpers, -leveranciers en -onderzoekers zijn bij deze open internationale gemeenschap aangesloten. Deelname staat dan ook open voor alle geïnteresseerden. IETF organiseerde 3 fysieke meetings in 2024. IETF 119 was in maart in Brisbane, Australië, IETF 120 in juli in Vancouver, Canada en IETF 121 in november in Dublin, Ierland. SIDN Labs gaf tijdens deze meetings presentaties over onder meer RESTful Provisioning Protocol. SIDN Labs schreef ook mee aan een conceptonderzoeksagenda voor een post-kwantum DNSSEC.

DNS-OARC

Het DNS Operations, Analysis and Research Center (DNS-OARC) is een platform voor belangrijke operators, uitvoerders en onderzoekers. Via DNS-OARC kunnen zij reacties op aanvallen en andere problemen coördineren en informatie en kennis delen. In 2024 organiseerde het platform 2 internationale bijeenkomsten voor betrokken partijen. OARC 42 werd gehouden in februari in Charlotte, Verenigde Staten en OARC 43 vond plaats in oktober in Praag, Tsjechië.

CENTR

CENTR is de vereniging van Europese ccTLD registry's. Samen met haar leden is CENTR verantwoordelijk voor 80% van alle geregistreerde landendomeinnamen wereldwijd.

Wij zijn actief lid van CENTR. Onze CEO, die al lid was van de CENTR-board, werd in 2024 benoemd tot voorzitter van de raad van bestuur van CENTR. Een collega van ICT is covoorzitter van de Tech-werkgroep en een collega van SIDN Labs is covoorzitter van de R&D-werkgroep. In 2024 organiseerde CENTR verschillende workshops in Europa over marketing, security, administratie, wet- en regelgeving, beveiliging en onderzoek en ontwikkeling. Onze medewerkers presenteerden bij de CENTR Jamboree, CENTR GA 72 en bij de CENTR Tech- en R&D-werkgroep. Ook nodigden we .nl-registrars uit voor de jaarlijkse CENTR Registrar Day. Verder is een van onze mensen co-chair van de Tech Working Group.

CENTR-leden vertegenwoordigen ruim 80% van de wereldwijd geregistreerde landendomeinen.

ECP Jaarfestival 2024

ECP | Platform voor de InformatieSamenleving draagt vanuit een neutrale en onafhankelijke positie bij aan een betrouwbare, kansrijke en veerkrachtige digitale samenleving. Dat doet het platform samen met publieke en private organisaties. Het ECP Jaarfestival 2024 vond plaats in november in Den Haag. Het thema was 'Digitaal dat zijn wij?!' en wij waren als een van de partners aanwezig. De directeur van SIDN fonds sprak onder meer over het 10-jarig bestaan van SIDN fonds. Rondom de vraag 'Hoe krijgen we grip op polarisatie en desinformatie?' organiseerden we samen met SIDN fonds 'Cybersecurity 2024 - Samen Sterk tegen Digitale Dreigingen'. Ook presenteerden 2 door SIDN fonds gesteunde projecten hun werk en 2 collega's van SIDN Labs presenteerden resultaten uit hun onderzoek naar de digitale weerbaarheid van Nederland. Verder stond Packet Run op de netwerkvloer, de installatie vanuit een samenwerking tussen SIDN fonds en SIDN Labs die laat zien hoe het internet onder de motorkap werkt.

EuroDIG

Het open platform European Dialogue on Internet Governance (EuroDIG) wisselt standpunten uit met belanghebbenden over het internet en de manier waarop het wordt bestuurd. EuroDIG bevordert gesprekken en samenwerkingen binnen de internet-gemeenschap over openbaar internetbeleid. Wij nemen actief deel aan het platform en sponsorden in 2024 de jaarlijkse EuroDIG-conferentie in Straatsburg, Frankrijk.

Internet Governance Forum

Het Internet Governance Forum (IGF) van de Verenigde Naties brengt stakeholdergroepen uit de hele wereld samen om te discussiëren over internetbestuur en digitaal beleid. In 2024 werden belangrijke thema's besproken, zoals cybersecurity, emergingtechnologieën, databeheer en vertrouwen, AI en internetfragmentatie. Als lid van de Nederlandse delegatie waren we aanwezig tijdens de IGF-bijeenkomst in Riyad, Saoedi-Arabië. In oktober organiseerde NL IGF, een samenwerkingsverband tussen het ministerie van EZ, ECP en SIDN, de jaarlijkse voorbereidende bijeenkomst.

ONE Conference

Het Nationaal Cyber Security Centrum, het ministerie van EZ en de gemeente Den Haag organiseren elk jaar de ONE Conference in het World Forum in Den Haag. Tijdens dit belangrijkste cybersecurityevenement van Europa delen de aanwezigen kennis, best practices en onderzoeksresultaten. De ONE Conference in 2024 stond onder meer in het teken van malwaredetectie, rechtshandhaving, onderzoek naar cyberbeveiliging en partnerschappen tussen het publieke en private domein. SIDN Labs leverde een bijdrage met een artikel voor het ONE Magazine over post-kwantumcryptografie in het DNS.

Internet in Beeld: Verleden, Heden & Toekomst

Het evenement 'Internet in Beeld: Verleden, Heden & Toekomst' is een initiatief van Internet Society Nederland (ISOC NL), Platform Internetstandaarden (PLIS) en NL IGF. Het evenement werd georganiseerd ter ere van het 25-jarig bestaan van ISOC NL, 10 jaar Internet.nl en het bijna 20-jarige bestaan van het IGF. Het programma stond in het teken van de ontwikkeling van het internet. De directeur van SIDN Labs was voorzitter van een panelgesprek over PLIS en Internet.nl en de CEO van SIDN blikte samen met partners terug op onder meer het IGF. Een collega van SIDN fonds verzorgde een presentatie en deelde voorbeelden van projecten die bijdragen aan een veiliger en inclusiever internet.

KVK Startersdag

De Kamer van Koophandel nodigde ons in 2024 weer uit voor de KVK Startersdag op 16 november 2024. Het evenement vond plaats in Ahoy, Rotterdam. Samen met het Benelux-Bureau voor de Intellectuele Eigendom gaven we 5 workshops over het vinden van de juiste bedrijfs-, merk- en domeinnaam. Met hulp van de .nl-registrars Metaregistrar en Team Blue beantwoordden we vragen van ondernemers. Wij gaven de ondernemers onder meer advies over hosting, online veiligheid, moderne internetstandaarden en zakelijke e-mail.

SIDN Inspire

Op 16 mei 2024 organiseerden we editie 4 van SIDN Inspire in LIEMÈS, Utrecht. Het evenement stond in het teken van 'Samen vooruit'. Een cybercrimespecialist en digitaal detective besprak het belang van samenwerkingen tussen de politie, private bedrijven en slachtoffers en ontwikkelingen rondom cybercriminaliteit en AI. Thema's die in de sessies aan bod kwamen, waren de domeinnaambranche, het nieuwe ICANN-contract voor gTLD's in 2026, de NIS2-richtlijn, de Lees Simpel App en de toepassing van AI bij het schrijven van brieven. SIDN Labs besprak post-kwantumcryptografie en presenteerde de voortgang van het PATAD-testbed voor DNS.

SIDN Inspire 2024 stond in het teken van 'Samen vooruit'.

SIDN TechTalks

Elk jaar organiseren we 2 SIDN TechTalks voor technici en studenten op ons kantoor in Arnhem. Tijdens deze bijeenkomsten delen we kennis en nieuwe ontwikkelingen rondom bijvoorbeeld abuse, veiligheid en data. Ook geven onze collega's presentaties over relevante onderzoeken en projecten. In 2024 vonden de TechTalks plaats in april en november. Besproken thema's waren onder andere de ontwikkeling van een anycastmeettool en TimeNL, de NTP-dienst van SIDN Labs.

Deelname aan organisaties

We steunen organisaties en projecten die internetgebruik stimuleren of de ongewenste effecten van het internet bestrijden. Dit doen we als kennispartner of sponsor.

Samenwerking binnen Europa

Samen met 11 andere initiatiefnemers zijn we medeoprichter van het Europese Top-Level Domain Information Sharing and Analysis Centre (TLD ISAC). Sinds de oprichting in 2023 groeide TLD ISAC naar 17 leden eind 2024.

Onze CEO is lid van de TLD ISAC-stuurgroep en CENTR ondersteunt het initiatief. De TLD ISAC bundelt inzichten, kennis en ervaringen rondom cybercriminaliteit. Door deze informatie met elkaar te delen, kunnen we onze diensten en de kritieke infrastructuur beter beschermen en de veiligheid van topleveldomeinen in Europa verder versterken. In oktober 2024 ontmoetten vertegenwoordigers van EU ISAC's elkaar in Athene. Daar wisselden zij expertise en informatie uit over hun activiteiten, successen en uitdagingen. Tijdens het TLD-ISAC jaarcongres in november gaf een SIDN Labs-collega een presentatie over 'Vulnerability Management' in Brussel.

Platform Internetveiligheid

SIDN is lid van het Platform Internetveiligheid (PIV). Dit samenwerkingsverband tussen markt- en overheidspartijen wil structureel bijdragen aan het verbeteren van de internetveiligheid voor alle gebruikers. Belangrijke onderwerpen waar het PIV zich op richt zijn onder andere privacy, phishing en de aanpak van online kindermisbruik en de verspreiding van beelden daarvan. Het platform biedt een neutrale plek voor gesprekken op strategisch niveau, die bijdragen aan concrete afspraken en initiatieven.

Werkgroep Notice-and-Takedown

SIDN is deelnemer van de werkgroep Notice-and-Takedown die valt onder het Platform Internetveiligheid. Het belangrijkste doel van de werkgroep is het beheer van de nationale gedragscode Notice-and-Takedown en het delen van kennis en ervaringen rondom de werking hiervan. In de gedragscode staat hoe betrokkenen omgaan met meldingen van onrechtmatige en strafbare inhoud op het internet.

Offlimits

Offlimits kwam voort uit het Expertisebureau Online Kindermisbruik. De organisatie ondersteunt mensen die te maken hebben (gehad) met online grensoverschrijdend gedrag en misbruik. In het bijzonder uitbuiting en seksueel misbruik van kinderen en volwassenen. Daarnaast werkt de organisatie aan een veiligere onlinewereld en het versterken van de positie van internetgebruikers. SIDN is sponsor van Offlimits.

Publiek Private Samenwerking Online Content Moderatie

Hosting-, registrar- en socialmediaplatformen en SIDN overleggen onderling en met publieke partijen over het optimaliseren van het weghalen of ontoegankelijk maken van illegale content. Dit doen zij op initiatief van het ministerie van Justitie en Veiligheid en in het kader van de Europese Digital Service Act. Daarnaast wordt gewerkt aan de inrichting van een laagdrempelige meldvoorziening voor internetgebruikers.

Alert Online

SIDN is een van de partners van de campagne Alert Online. Dit is een initiatief van het ministerie van EZ, gericht op het creëren van bewustwording rondom online veiligheid en het stimuleren van cyberveilig gedrag van bedrijven, overheden en burgers in Nederland. Alert Online stimuleert in de cybersecuritymaand oktober cyberveilig gedrag en bewustwording rondom online veiligheid. In het kader van Alert Online lieten we Markteffect onderzoeken wat Nederlanders zien als grootste belemmering voor een zorgeloos digitaal bestaan. 50% van de ruim 1.000 respondenten noemde phishingmails en andere vormen van oplichting en 47% noemde onbetrouwbare of verdachte websites.

Bits of Freedom

Bits of Freedom zet zich in voor internetvrijheid van de gebruikers en een open en rechtvaardige informatiesamenleving. De stichting beïnvloedt beleid en wetgeving door juridische actie, campagnes en belangenbehartiging in Nederland en Brussel. Als een van de sponsors zorgen we dat Bits of Freedom zich onafhankelijk kan inzetten voor privacy en communicatievrijheid.

TUCCR

De Twente University Centre for Cybersecurity Research (TUCCR) is een samenwerkingsverband van kennispartners, experts, professionals, ondernemers, onderzoekers en

studenten uit de industrie op het gebied van cybersecurity. Het expertisecentrum streeft naar het versterken van de veiligheid en digitale autonomie van onze samenleving. Als partner dragen we bij aan toegepast onderzoek naar cybersecurity en ondersteunen we wetenschappelijk onderzoek binnen TUCCR. Onze CEO is lid van het TUCCR-bestuur en een van de teamleden van SIDN Labs is covoorzitter van de pijler Network Security. We cofinancieren een PhD-student die onderzoek doet naar zogeheten routing hijacks.

DINL

Binnen stichting Digitale Infrastructuur Nederland (DINL) zetten organisaties zich samen in voor een sterke digitale infrastructuur als basis van de Nederlandse digitale economie en maatschappij. DINL helpt overheden, bedrijven en burgers hun weg te vinden in de online-economie en laat zien hoe zij de positie van Nederland als internationale digitale voorloper kunnen versterken. Wij zijn een van de oprichters en partners van DINL. In 2024 werden we opnieuw deelnemer van de stichting en trad onze CEO toe tot het bestuur. De samenwerking met andere deelnemers zorgt ervoor dat we gezamenlijke standpunten rondom een sterke digitale infrastructuur beter kunnen inbrengen binnen het politieke debat.

Wij zijn een van de oprichters en partners van de stichting Digitale Infrastructuur Nederland.

ECP | Platform voor de InformatieSamenleving

Binnen ECP geven betrokken bedrijven, overheden, maatschappelijke organisaties en kennisinstellingen samen vorm aan onze digitale samenleving. Als partner waren we in 2024 betrokken bij het Nederlands Internet Governance Forum (NL IGF), het Platform Internetveiligheid, de website veiliginternetten.nl en het ECP Jaarfestival. Ook zijn we betrokken bij de tool ScamCheck, het Platform Internetstandaarden en de doorontwikkeling van Internet.nl.

Nationale Coalitie Duurzame Digitalisering

In 2024 werden we lid van de Nationale Coalitie Duurzame Digitalisering. Deze publiek-private samenwerking richt zich op het wegnemen van knelpunten rondom duurzame digitalisering en heeft als doel de milieu-impact van en door digitalisering te verminderen.

NLnet Labs

De non-profitorganisatie NLnet Labs ontwikkelt gratis opensourcesoftware voor het DNS en BGP-routing. Het NLnet Labs-team doet daarnaast onderzoek, ontwikkelt standaarden en ondersteunt de internetgemeenschap. Wij sponsoren dit belangrijke werk en onze CTO is lid van de raad van toezicht. Ook werkt SIDN Labs veel samen met NLnet Labs aan onderzoeksprojecten, zoals het contractonderzoek voor de rootserveroperators Verisign en ISC in 2024.

European Summer School on Internet Governance

Net als voorgaande jaren sponsorden we de European Summer School on Internet Governance. Dit is een non-profitorganisatie die elk jaar een introductieprogramma organiseert voor studenten, academici, bedrijven en overheidsinstanties. EuroSSIG helpt hen om de wereldwijde discussies over internetgovernance beter te begrijpen en kennis op te doen over de verschillende onderdelen hiervan. In juli 2024 vond de achttiende editie plaats in Meißen, Duitsland.

Dutch Cloud Community

Dutch Cloud Community is de belangenvereniging voor de Nederlandse cloud- en internet-sector. De vereniging behartigt de belangen van de meer dan 100 leden en biedt hen toegang tot onder meer vakinhoudelijke publicaties, kennissessies, marktinzichten en juridisch advies. Wij zijn een van de sponsors van Dutch Cloud Community. In 2024 voerden we regelmatig gesprekken met het bestuur van de vereniging. Deze gingen over hun reacties in de media op ons voorgenomen besluit rondom de migratie van ons registratiesysteem.

Nederlandse Anti-DDoS-Coalitie

De Nederlandse Anti-DDoS-Coalitie is een publiek-privaat samenwerkingsverband tussen overheden, internetproviders, non-profitorganisaties, banken, internet exchanges en academische instanties. Wij zijn een van de partners. De 20 deelnemende organisaties zetten zich samen in om de impact van DDoS-aanvallen op de samenleving te verminderen. Dat doen zij door kennis te delen, DDoS-aanvallen te onderzoeken en te oefenen met deze aanvallen. In 2024 maakten we deel uit van de werkgroepen Clearinghouse, Legal en Intel & Attributie. Ook namen we deel aan de jaarlijkse landelijke anti-DDoS-oefening.

2STiC

SIDN Labs is een van de oprichters van 2STiC (Security, Stability, and Transparency in inter-network Communication). Binnen deze community doen we samen met partners onderzoek naar uitbreidingen en vernieuwingen van de internetinfrastructuur. Waaronder ook infrastructuren die de veiligheid van communicatie via het internet vergroten op basis van een heel andere architectuur, zoals SCION.

Liaison Nationaal Cyber Security Centrum

Het Nationaal Cyber Security Centrum (NCSC) is onderdeel van het ministerie van JenV en streeft naar een digitaal veilig Nederland. Als een van de liaisons van het NCSC dragen we hieraan bij door onze kennis te delen en het NCSC met andere partners te verbinden.

“Als een afbeelding eenmaal geïdentificeerd is als strafbaar materiaal, krijgt deze een unieke digitale vingerafdruk, oftewel een ‘hash’.”



Yvette Velzeboer

Projectcoördinator bij Offlimits

SIDN steunt het werk van Offlimits

Wij maken al sinds jaar en dag het werk van het Meldpunt Kinderporno van Offlimits mede mogelijk. Via SIDN fonds steunen we ook verschillende initiatieven van Offlimits, zoals de Hash Check Service. Yvette Velzeboer, projectleider van de Hash Check Service bij Offlimits: “Als een afbeelding eenmaal geïdentificeerd is als strafbaar materiaal, krijgt deze een unieke digitale vingerafdruk, oftewel een ‘hash’. Deze hash wordt opgeslagen in een database en gebruikt om nieuwe uploads te controleren. Als eenzelfde afbeelding opnieuw wordt geüpload, wordt deze direct geblokkeerd. Aangesloten partijen, zoals hostingproviders, kunnen op vrijwillige basis controleren of geüpload materiaal op hun servers in de database van de Hash Check Service voorkomt.”

> Lees meer over [de Hash Check Service](#)



Innoveren vanuit onze maatschappelijke missie

6 Ontwikkelingen binnen SIDN

Onze focus lag voor een groot deel op onze technische basis. Zo werken we sinds 2024 met de nieuwe structuur van onze ICT-afdeling onder de noemer SIDN Tech. Ook stond 2024 in het teken van de voorgenomen migratie naar de publieke cloud en werkten we met CIRA aan het nieuwe registratiesysteem. De veranderingen op technisch vlak en de publieke aandacht voor onze migratieplannen zorgden voor de nodige discussies in onze teams, zo bleek uit ons medewerkersonderzoek. Verder maakten we sidn.nl digitaal toegankelijker in het kader van de Web Content Accessibility Guidelines (WCAG).

ICT-transitie en IT-sourcingstrategie

Sinds 1 januari 2024 werken we met onze nieuwe IT-sourcingstrategie en de nieuwe structuur van onze ICT-afdeling onder de naam SIDN Tech. Deze afdeling bestaat uit 3 teams met elk een eigen focus: ICT & security operations, software-engineering en cloudengineering. De teams richten zich op 5 uitdagingen:

1. de .nl-zone veilig houden;
2. de continuïteit van onze diensten borgen;
3. onze processen en systemen verder standaardiseren en stroomlijnen;
4. een nieuw domeinnaamregistratiesysteem ontwikkelen; en
5. onze registratie-applicatie naar de publieke cloud migreren.

2024 stond grotendeels in het teken van het proces dat volgde op de aankondiging van ons voorgenomen besluit: het migreren van een deel van de infrastructuur van ons registratiesysteem naar de publieke cloud van AWS in Europa. We werkten mee aan de quickscan van het Nederlandse en Europese cloudaanbod door het ministerie van EZ. Ook lieten we een Data Protection Impact Assessment (DPIA) uitvoeren en deed de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) een risicoanalyse. Hierbij hebben we geen onomkeerbare stappen gezet vóór de afronding hiervan in januari 2025.

Het beheer van .nl, inclusief de ontwikkeling en het beheer van ons registratiesysteem, ons primaire DNS en eigen DNS anycast, blijven we te allen tijde zelf uitvoeren. Voor en vanuit Nederland. Onze absolute focus ligt op zorgen dat .nl altijd beschikbaar is en dat onze data veilig zijn. Onze kerndienst resolving en de daarbij behorende DNS-infrastructuur migreren we niet naar de publieke cloud van hyperscalers. Het registratiesysteem maken we zoveel mogelijk onafhankelijk van cloudeleveranciers door open standaarden en opensourcetechnologie te gebruiken. En door de database voor de zonefile onder te brengen bij een Nederlandse provider. Deze database vormt de primaire, betrouwbare en vertrouwde bron op basis waarvan de generatie, signing en publicatie van de zonefile buiten AWS bij een Nederlandse provider plaatsvindt. Dit is onderdeel van onze architectuur en exitstrategieën. Zo kunnen we relatief eenvoudig naar een Nederlandse of Europese cloudeleverancier verhuizen als die mogelijkheid zich voordoet.

- > [Lees onze toelichting op de migratie naar de publieke cloud](#)

Daarnaast werkten we in 2024 aan het verder versterken van de DNS-infrastructuur, onder meer door de capaciteit van ons anycastplatform verder te

verhogen. De Deense registry Punktum dk, beheerder van het .dk-domein, nam dit platform ook in gebruik. Technische verbeteringen in de DNS-infrastructuur zijn cruciaal voor een veilig, beschikbaar en robuust .nl-domein.

Nieuw registratiesysteem

In de eerste helft van 2024 kregen we complete toegang tot onder meer de broncode van het Fury Registry Platform van onze partner CIRA. Op basis van dit huidige platform werkten we samen met onze collega's van CIRA aan de ontwikkeling van het nieuwe registratiesysteem Hello Registry, dat geschikt is gemaakt voor cloudechnologie. Het doel is om .amsterdam, .politie en .aw en .nl eind 2025, begin 2026 hierop te gaan draaien. Ook op andere vlakken dan ICT werken we met CIRA samen.

Met CIRA werken we aan het Hello Registry-platform dat werkt met generieke cloud-technologie.

Dataplatform van SIDN

Met het dataplatform van SIDN maken we data beter beschikbaar voor registrars en onze eigen organisatie. Registrars hebben toegang via 'SIDN Insights'. We rondten het fundament van het dataplatform af en richtten rapportages in voor onder andere onze supportafdeling. Ook bereidden we de koppeling van Hello Registry met het dataplatform voor, zodat het platform uiteindelijk ook de data uit dit nieuwe systeem kan verwerken. Aan de kant van de gebruiker ontsluiten we nieuwe data-bronnen die van waarde zijn voor de .nl-registrars.

SIDN is digitaal toegankelijker

We vinden het belangrijk dat iedereen, met of zonder functiebeperking, gebruik kan maken van onze producten en diensten. Met een interne presentatie en workshop voor medewerkers en ontwikkelaars zorgden we daarom voor meer bewustwording over digitale toegankelijkheid. Zowel van onze websites als van onze andere communicatiemiddelen. Daarnaast voerden we samen met onze leverancier verbeteringen door op sidn.nl, met als doel te gaan voldoen aan de WCAG. Deze Europese

wet moet ervoor zorgen dat alle Europeanen vanaf juni 2025 toegang hebben tot online producten en diensten. Zo voegden we een toegankelijkheidsverklaring toe aan de website. Ook kunnen gebruikers op sidn.nl kiezen uit 3 kleurvarianten van de website.

We maakten sidn.nl digitaal toegankelijker voor website-bezoekers met een beperking.

Nieuwe statuten

Medio 2024 werden de statuten van SIDN en de onderliggende BV's aangepast. Het doel hiervan was om de statuten aan te laten sluiten bij de Wet bestuur en toezicht rechtspersonen. Deze wet voorziet in maatregelen om de kwaliteit van het bestuur en toezicht bij onze stichting te verbeteren. De statuten van de BV's zijn nu volledig gelijk aan elkaar. Daarnaast vonden in de statuten van onze stichting enkele inhoudelijke veranderingen plaats. Zowel onze doelstellingen als de rechten van .nl-registrars bleven ongewijzigd.

> Lees verder over [de nieuwe statuten](#) op sidn.nl

Cyberoefeningen en securityactiviteiten

Proactieve cyberbeveiligingsmaatregelen worden steeds belangrijker. Zeker omdat cyberbedreigingen blijven evolueren en uitdagingen vormen voor het digitale landschap. SIDN was een van de initiatiefnemers van het in 2023 opgerichte Europese Top-Level Domain Information Sharing and Analysis Center (TLD-ISAC). Hierbinnen werken registry's samen om de cyberweerbaarheid te verhogen.

Jaarlijks nemen we deel aan de landelijke DDoS-oefening van de Nationale Anti-DDoS-coalitie. De coalitie heeft als doel om DDoS-aanvallen vanuit verschillende hoeken te onderzoeken en bestrijden. Zo kunnen we ons beter voorbereiden op dergelijke dreigingen. Voor onze medewerkers organiseren we gedurende het jaar bewustwordingsacties, om het bewustzijn op cyberrisico's te vergroten.

ISO27001-certificering

Certificering volgens de ISO27001 is dé standaard voor informatiebeveiliging. In 2024 is de controle op het naleven van deze standaard weer uitgevoerd en hebben we die met goede resultaten afgesloten. Ook staken we veel energie in de voorbereiding van de transitie naar de 2022-versie van de ISO-standaard. De overgang naar de nieuwe versie van deze standaard stond gepland voor 2025, maar is al in 2024 afgerond.

Overdracht Yivi aan Privacy by Design

Yivi is het privacyvriendelijke platform, waarmee burgers en organisaties veilig online inloggen, gegevens uitwisselen en documenten digitaal ondertekenen en goedkeuren. Onze investeringen in Yivi de laatste 5 jaar resulteerden in een professioneler platform met hoge beschikbaarheid en een vernieuwde app, die aansluit bij behoeften van gebruikers. Maar ook in de bredere adoptie van het Yivi-gedachtegoed, dat uitgaat van de principes privacy by design, opensource en decentraal. De principes werden beter vastgelegd in het wetsvoorstel voor de Wet digitale overheid (Wdo) en de Europese Commissie nam het gedachtegoed over voor de ontwikkeling van nieuwe Europese identity wallets.

Na een geleidelijke overdracht gaven we Yivi in april 2024 formeel terug aan stichting Privacy by Design die weer eigenaar van Yivi werd. Het technisch beheer van het platform voerden wij nog uit in opdracht van Privacy by Design, terwijl we de overdracht aan Caesar Groep begin 2025, voorbereidden.

Personeelsbestand en verzuim

We richtten onze afdeling SIDN Tech verder in. In lijn daarmee kregen enkele collega's een andere of zelfs een voor SIDN nieuwe functie, zoals de rol van cloud engineer. Ook verwelkomden we een nieuwe financieel directeur (CFO) en een manager public affairs.

Daarnaast verbeterden we onze voorbereidings- en inwerkprocessen voor nieuwe collega's en versterkten we onze contacten met hogescholen en universiteiten. Vanuit deze samenwerkingen willen we startersfuncties en stageplekken vervullen. In totaal verwelkomden we 16 collega's en namen we afscheid van 20 collega's. We sloten 2024 af met 99 medewerkers (90 FTE). Het ziekteverzuim was 6,14%, dat is hoger dan het landelijk gemiddelde van 4,9%. Dit percentage kwam door langdurig ziekteverzuim, waarvan de oorzaken niet-werkgerelateerd zijn.

Welzijn van medewerkers

In 2024 ondersteunden we het welzijn van SIDN'ers op allerlei manieren. Zo deed 59% van de medewerkers een preventieve medische controle bij onze

arbodienst. De uitkomsten geven inzicht in hun fysieke en mentale gezondheid en mogelijke risico's op verzuim. Op basis van hiervan helpen we medewerkers bij het verbeteren van hun leefstijl. Ook bieden we fruit aan op kantoor en konden medewerkers onder andere deelnemen aan bootcamps georganiseerd bij ons kantoor en fysieke activiteiten tijdens het SIDN-weekend.

Medewerkersonderzoek

In 2024 hielden we een onderzoek onder onze medewerkers. Hieruit bleek dat collega's de werksfeer en samenwerking binnen het eigen team als positief ervaren. In de samenwerking en communicatie tussen teams zien ze verbeterpunten. Ook lieten de resultaten zien dat veranderingen in functies binnen SIDN Tech en de reacties vanuit onze omgeving op onze voorgenomen cloudmigratie zorgden voor onduidelijkheid en onrust bij collega's. Daarnaast voelden collega's zich over het algemeen minder gehoord door het management. Daarom startten we onder andere met feedbacksessies, zodat we effectiever gebruikmaken van de expertise en mening van collega's voordat het management een besluit neemt.

Professionele ontwikkeling

Een opleidingsbudget is onderdeel van ons brede pakket aan arbeidsvoorwaarden. In 2024 gaven we meer dan 75% uit van het gereserveerde budget voor opleidingen en trainingen. Via ons learning-managementsysteem bieden we opleidingen aan, bijvoorbeeld over data-engineering en cloud-engineering en -technologie. Collega's behaalden gezamenlijk 15 certificeringen op het gebied van cloudtechnologie. In het kader van onze samenwerking met CIRA stimuleerden we opleidingen en trainingen in de Engelse taal.

Persoonlijk sponsorbudget

Onze mensen ontvangen jaarlijks een persoonlijk sponsorbudget om te besteden aan een zelfgekozen goed doel. We doneerde een groot deel van de medewerkers aan GIRO555 voor de slachtoffers in Gaza en het Midden-Oosten. Dit bedrag verdubbelden we naar € 22.000,-. Daarnaast steunden medewerkers onder andere de Koninklijke Hondenbescherming, de Nederlandse Cystic Fibrosis Stichting, Team Bijzondere Kinderen en Stichting Komma.

Privacyboard

Als beheerder van het .nl-domein verwerken we persoonsgegevens om de veiligheid en stabiliteit van de .nl-zone verder te vergroten. Onze eigen privacyboard toetst of we dit verantwoord en zorgvuldig doen. De privacyboard vraagt de eigenaar van nieuwe onderzoeken, projecten en systemen om een privacy-policy op te stellen, die de boardleden vervolgens

beoordelen. Zowel de policy's als de beoordeling ervan publiceren we op onze website. In 2024 toetste de privacyboard een policy over RegCheck, het systeem dat onze supportafdeling gebruikt.

> Lees verder over [de privacyboard](#) op [sidn.nl](#)

Ondernemingsraad

De ondernemingsraad (OR) was onder meer betrokken bij het medewerkersonderzoek en de samenstelling van het profiel voor een preventie-medewerker. Deze functie richt zich op het bevorderen van de veiligheid en gezondheid van onze mensen. De OR ontving een adviesvraag over de vorming en positionering van Team Security. In januari en september vergaderde de OR met de raad van toezicht.

Vooruitblik

ICT-transitie

Eind 2024 zijn de quickscan, de DPIA en de risico-analyse van de AIVD afgerond. Op basis hiervan besloot de ministerraad begin 2025 dat SIDN het .nl-registratiesysteem onder strikte voorwaarden en voor een beperkter deel mag migreren naar de publieke cloud van AWS. Mede op basis van het advies van de AIVD maakten we afspraken met het ministerie van EZ, vooral over maatregelen die we doorvoeren om de beschikbaarheid van .nl onafhankelijk van AWS te borgen. Sleutelcomponenten van onze dienstverlening, zoals de generator en signer van de DNS-zonefile en de verborgen primaire nameserver (hidden primary), brengen we onder bij een Nederlandse provider. De verdere invoering van de maatregelen en voorbereiding op de migratie van een beperkt deel van onze technische infrastructuur doen we in nauwe samenspraak met het ministerie van EZ, de betrokken Nederlandse provider, de VvR en registrars.

Samen met registrars zetten we een test-omgeving op voor Hello Registry.

Toekomst domeinnaamregistratiesysteem

Samen met CIRA bouwen we verder aan het gezamenlijke registryplatform. Het plan is om vanaf eind 2025 eerst .amsterdam, .politie en .aw te

migreren en het proces waar nodig verder te optimaliseren. Zodat we .nl in 2026 soepel kunnen migreren naar Hello Registry en de beschikbaarheid ervan kunnen blijven garanderen. Ook zetten we in 2025 samen met registrars een testomgeving op, zodat zij het nieuwe registratiesysteem kunnen testen.

Technisch beheer van Yivi

In 2025 dragen we ook het technisch beheer van Yivi volledig over aan Caesar Groep, die Yivi verder doorontwikkelt in opdracht van Privacy by Design. We verwachten dat dit in april volledig is afgerond.

Medewerkerstevredenheid en duurzame inzetbaarheid

Met ingang van 2025 voeren we ons uitgebreide medewerkersonderzoek jaarlijks uit en we doen elk kwartaal een korte meting. Op die manier krijgen we een beeld van verbeterpunten en zaken die bij medewerkers spelen, zodat we daarop kunnen anticiperen. De resultaten gebruiken we om de samenwerkingen verder te verbeteren.

Learningmanagementsysteem

In 2025 ronden we het opleidingsplan af voor onze afdeling SIDN Tech. Hiermee brengen we verder in kaart welke kennis en opleidingen nodig zijn in het kader van de migratie en het werken met cloud-technologieën.

Digitale toegankelijkheid van onze websites

In 2025 zorgen we ervoor dat onze pdf's en formulieren voor alle websitebezoekers toegankelijk zijn. Daarnaast maken we de websites van SIDN fonds en het CvKB toegankelijker, zodat ze ook voldoen aan de WCAG.

“Dan kan iedereen, met of zonder beperking, gebruikmaken van onze producten en diensten.”



Nicole Wedler

Online communicatieadviseur bij SIDN

SIDN digitaal toegankelijker

“De missie van SIDN is ‘een kansrijk en zorgeloos digitaal bestaan voor IEDEREEN’. Daarom willen we natuurlijk dat ook onze website digitaal toegankelijk is. Dan kan iedereen, met of zonder beperking, gebruikmaken van onze producten en diensten. We hebben daarvoor flinke stappen gezet, zodat sidn.nl kan gaan voldoen aan de wereldwijde standaard voor goede toegankelijkheid. Met hulp van Stichting Accessibility hebben we onderzoek gedaan naar de toegankelijkheid van sidn.nl. Op basis van de bevindingen zijn we samen met onze partner Us Media aan de slag gegaan om de verbeterpunten op te pakken. Heb je feedback op de veranderingen of suggesties voor verdere verbeteringen? Laat het ons vooral weten. De beste testers zijn immers de gebruikers zelf. Mail je bevindingen naar communicatie@sidn.nl.”

› Lees meer over [hoe we \[sidn.nl\]\(https://sidn.nl\) toegankelijker maken](#)

Onze Sustainable Development Goals



Betaalbare en duurzame energie



Goede gezondheid en welzijn



Industrie, innovatie en infrastructuur



Klimaatactie



Kwaliteitsonderwijs



Partnerschap om doelstellingen te bereiken

Onze impact op een duurzame en digitale samenleving

7 Duurzaamheidsverslag

Ook bij SIDN werken we aan een duurzame en digitale samenleving. Dat betekent dat we ons samen met klanten, partners en leveranciers inzetten voor een kansrijke, veilige en gezonde leef- en werkomgeving voor iedereen binnen SIDN en daarbuiten. We geven invulling aan onze duurzaamheidsambitie door ons te richten op de Sustainable Development Goals (SDG's) van de Verenigde Naties. Uit deze SDG's selecteerden we 6 relevante doelen waarop we de meeste impact kunnen maken.

SDG 3: Goede gezondheid en welzijn

SDG 3 gaat over het verzekeren van goede gezondheid en het bevorderen van welzijn voor alle leeftijden. Onze impact op dit doel bespreken we hiervoor in hoofdstuk 6, zoals onze inzet op ziekteverzuim en het stimuleren van preventief medisch onderzoek.

SDG 4: Kwaliteitsonderwijs

SDG 4 richt zich op het verzekeren van gelijke toegang tot kwaliteitsonderwijs en het bevorderen van levenslang leren voor iedereen. Onze impact op dit doel bespreken we hiervoor in hoofdstuk 6. Zo bieden we medewerkers een opleidingsbudget, waarmee we professionele ontwikkeling stimuleren.

SDG 7: Betaalbare en duurzame energie

SDG 7 gaat over het verzekeren van toegang tot betaalbare, betrouwbare, duurzame en moderne energie voor iedereen. In dit kader zetten we in op energiereductie per FTE. In 2024 kwam ongeveer 15% van de elektriciteit die we gebruiken voor ons kantoorpand van onze zonnepanelen. Ook draaien ons kantoorpand en onze datacenters op 100% duurzame energie. We onderzochten de mogelijkheden van een windturbine die windenergie omzet in elektriciteit voor ons eigen kantoor. De investering in een windturbine staat nog niet in verhouding met de energie die dit systeem oplevert, maar we houden de ontwikkelingen hiervan in de gaten. Ook zijn we in gesprek met de Vereniging van Eigenaren (VvE) over gezamenlijke energiewinning voor bedrijven op het terrein waarop ons kantoor is gevestigd en de langetermijnmogelijkheden.

Ons kantoorpand en onze datacenters draaien op 100% duurzame energie.

SDG 9: Industrie, innovatie en infrastructuur

SDG 9 richt zich op het bouwen van een veerkrachtige infrastructuur, het bevorderen van inclusieve en duurzame digitalisering en het stimuleren van innovatie. In dit kader richten we ons op het hergebruik en recyclen van apparatuur en andere materialen. Minimaal 95% van onze eigen apparatuur wordt gerecycled of hergebruikt en we gebruiken gerecyclede materialen voor de inrichting van ons kantoor. Bij de aanschaf van hardware geven we de voorkeur aan de meest duurzame en circulaire opties. Over materialen en apparatuur boven de € 10.000,- neemt onze inkoopspecialist een goed onderbouwd besluit.

In 2024 richtten we ons in het bijzonder op de catering voor ons kantoorpand, omdat deze service zo'n 12% van onze totale jaarlijkse CO₂-uitstoot veroorzaakt. We bespraken samen met de cateraar de mogelijkheden voor verduurzaming, zoals meer lokaal inkopen en het aanbieden van producten met een lagere CO₂-voetafdruk. Hierdoor daalde de CO₂-uitstoot door de catering met zo'n 12,5% in 2024.

Door verduurzamingsacties daalde de CO₂-uitstoot door onze catering met zo'n 12,5%.

SDG 13: Klimaatactie

SDG 13 gaat over het ondernemen van actie om klimaatverandering en de impact daarvan te bestrijden. In dit kader richten we ons op het reduceren van onze CO₂-uitstoot per .nl-domeinnaam. Een van onze grootste uitdagingen is het woon-werkverkeer, dat 41% van onze CO₂-uitstoot veroorzaakt. Daarom stimuleren we collega's door middel van een leasefietsregeling en met NS-Business Cards om vaker met de fiets of trein naar kantoor te komen. En om bij zakelijke vluchten korter dan 750 km te kiezen voor reizen per trein of met de elektrische leaseauto. Met ingang van 2024 kunnen medewerkers die in aanmerking komen voor een leaseauto alleen nog kiezen voor een elektrisch model.

Verder investeren we in 100% duurzame energie (zie SDG 7) en sluiten we op rustige dagen 1 of 2 etages op ons kantoor. Zo gaan de verlichting en klimaatbeheersing op deze afdelingen niet aan. In 2024 plaatsten we afvalscheidingsbakken in ons kantoorpand en we stimuleren waterbesparing met onder andere stickers op de toiletten. Op een digitaal scherm bij onze entree geven we inzicht in het watergebruik en het restafval binnen SIDN. Het waterverbruik, dat al vrij laag was, is dit jaar met 10% afgenomen en het scheiden van afval gaat nu beter dan een jaar geleden.

SDG 17: Partnerschap om doelstellingen te bereiken

SDG 17 gaat over het nieuw leven inblazen van samenwerkingen en wereldwijd partnerschap voor duurzame ontwikkeling. Onze focus ligt op samenwerkingsvormen die direct te maken hebben met duurzaamheid. Zo maken we sinds 2024 deel uit van de Nationale Coalitie Duurzame Digitalisering. Ook zijn we lid van de sustainability-mailgroep van CENTR. Samen met andere leden wisselen we kennis uit over duurzaamheid en zetten we ons in voor een breder draagvlak voor duurzaamheid binnen de CENTR-gemeenschap. Ten slotte zijn we partner van het duurzame bedrijvennetwerk MVO-Nederland.

We bereidden ons in 2024 verder voor op de Corporate Sustainability Reporting Directive (CSRD). Deze Europese richtlijn geldt naar verwachting vanaf 2026 indirect voor organisaties zoals SIDN. De CSRD stelt dat we moeten rapporteren over onze impact op Environmental, Social en Governance (ESG).

Sinds 2024 zijn we lid van de Nationale Coalitie Duurzame Digitalisering.

Vooruitblik

Vernieuwde invulling van duurzaamheidsambities

In 2025 geven we opnieuw invulling aan onze duurzaamheidsambities, maar nu op basis van de ESG's. We maken onze impact meetbaar door de ESG verder te verdelen op basis van de SDG's. Daarnaast scherpen we in 2025 onze Key Performance Indicators (KPI's), doelen en rapportagemethode aan, zodat ze uitdagend en realistisch blijven.

Een van onze doelen is om in 2025 maximaal 25 gram CO₂-uitstoot per domeinnaam te hebben. Hiermee realiseren we een reductie van 75% ten opzichte van ons referentiejaar 2019.



Marjet van Zijlen
Voorzitter raad van toezicht SIDN

8 Verslag raad van toezicht

De raad van toezicht (rvt) houdt toezicht op de strategie, het beleid en de algemene gang van zaken binnen de organisatie. Zo bewaakt de rvt de strategie en de risico's van onze ondernemingsactiviteiten, de opzet en de effectiviteit van onze risicobeheersing- en controlesystemen en het behalen van onze doelstellingen. Ook is de rvt sparringpartner voor en werkgever van de raad van bestuur.

Bijeenkomsten

In 2024 hield de rvt 4 reguliere vergaderingen en 2 extra online vergaderingen. Tijdens deze extra vergaderingen besprak de rvt de verdere uitwerking van de afspraken uit de samenwerkingsovereenkomst, die SIDN in oktober 2023 met CIRA sloot.

Verder werden onder andere de volgende zaken goedgekeurd of vastgesteld:

- Jaarrekening en jaarverslag 2023 van SIDN en alle onderliggende vennootschappen.
- Jaarverslagen van de rvt, de selectie-, voordrachts- en remuneratiecommissie, de auditcommissie, de veiligheids- en stabiliteitscommissie en de verklaring van bestuurders in het kader van corporate governance.
- Jaarplan en budget 2025 van SIDN.

Wat betreft de vaststelling van de jaarrekening 2023, stond de rvt stil bij de risico's die zijn verbonden aan de onderneming. Maar ook bij de uitkomsten van de opzet en de werking van de interne risicobeheersings- en controlesystemen, die voortkwamen uit de beoordeling door de directie.

Voorafgaand aan de aprilvergadering sprak de rvt met de voorzitter en de directeur van het bestuur van de Vereniging van Registrars (VvR). Ook had de rvt voorafgaand aan de septembervergadering een gesprek met de ondernemingsraad van SIDN. Vervolgens vond in het najaar de reguliere zelfevaluatie van de rvt plaats. De belangrijkste onderwerpen die via een enquête naar voren kwamen, besprak de rvt voorafgaand aan de decembervergadering.

Leden van de rvt namen deel aan de door SIDN georganiseerde bijeenkomsten van de strategieklinkbordgroep. Maar ook aan andere interne en externe activiteiten die SIDN organiseerde.

Besproken onderwerpen

De samenwerking met CIRA was een vast punt op de rvt-agenda. In 2024 besprak de rvt onder meer hoe de samenwerking met CIRA in een reeks aanvullende overeenkomsten invulling krijgt. De rvt verleende goedkeuring aan de bestuurders om deze overeenkomsten te sluiten. In de gesprekken was specifieke aandacht voor:

- de governance van de samenwerking;
- de waarborgen rond een eventuele toekomstige exit;
- de focus op het in gebruik nemen door SIDN van het gezamenlijke registratiesysteem;
- de keuze, het doel en het kader om in de toekomst samen met CIRA registrydiensten aan derden aan te bieden.

Verder stond de rvt regelmatig stil bij de ontwikkelingen rond de publieke en politieke discussie over het voornemen van SIDN om een deel van het registratiesysteem te migreren naar de cloud van AWS. De rvt ontving hierover geregeld updates vanuit de bestuurders. Ook was de rvt in de vergaderingen en via een ad-hoccommissie betrokken bij de ontwikkelingen.

Daarnaast besprak de rvt de daling in het aantal geregistreerde .nl-domeinnamen en de (financiële) gevolgen hiervan voor SIDN. Verder was het verbeteren van de aandacht voor de afstemming met stakeholders aan de orde en is SIDN Merkbewaking geëvalueerd.

Op organisatorisch vlak besprak de rvt de uitkomsten van het medewerkersonderzoek van SIDN met de bestuurders. Ook stelde de rvt een vernieuwd beleid vast met betrekking tot de onkosten van de bestuurders.

In de reguliere vergaderingen ontving de rvt steeds terugkoppeling van de auditcommissie en veiligheids- en stabiliteitscommissie, waaruit de relevante zaken werden besproken.

Commissies

De selectie-, voordrachts- en remuneratiecommissie heeft in 2024 meerdere keren overlegd. De commissie besprak de jaarlijkse evaluatie van het functioneren van de leden van de raad van bestuur en voerde gesprekken met kandidaten voor de invulling van de positie van de CFO. Dit laatste deed de commissie in wisselende samenstelling met de bestuurders, andere betrokken leden van de rvt en deels met de HRM-manager. Deze vacature is per september 2024 definitief ingevuld.

De auditcommissie vergaderde 4 keer. Deze vergaderingen vonden plaats in het bijzijn van de CEO, de interim-CFO en, na haar aantreden in september, de nieuwe CFO van SIDN. Tijdens de vergaderingen besprak de commissie onder andere de jaarrekening en het jaarverslag over 2023, de accountantsverklaring en de analyse van de jaarcijfers met het bestuur en de accountant. In november besprak de commissie het controleplan 2024 met de accountant. Andere onderwerpen die aan de orde kwamen, zijn het budget 2025 en de indexatie van de tarieven per 1 januari 2025. De auditcommissie sprak daarnaast over de procuratieregeling 2025, het voorstel voor een nieuw declaratiebeleid voor de bestuurders en het voornemen om in 2025 een nieuwe treasurybeleid te ontwikkelen. Ten slotte besprak de auditcommissie in iedere vergadering de tussen-tijdse financiële cijfers en de effecten daarvan op de verwachtingen voor het lopende boekjaar en daarna.

De veiligheids- en stabiliteitscommissie vergaderde 4 keer in 2024. Na de toetreding per 19 juni van Olaf Kolkman bestond de commissie uit 4 leden. De CTO en de CISO van SIDN waren bij de vergaderingen aanwezig. De commissie stond onder andere stil bij:

- het auditplan van de interne auditor en zijn bevindingen;
- de strategische risico's van SIDN en de acties en voortgang;
- de reguliere rapportage door SIDN aan de commissie;
- de securityontwikkelingen;
- de ICT-transitie;
- de ISO27001-hercertificering;
- de ontwikkelingen rondom het voornemen om een deel van het registratiesysteem te migreren naar de cloud van AWS.

In 2024 had de rvt 2 ad-hoccommissies. De commissie die in 2023 werd ingericht voor de uitwerking van de samenwerking met CIRA, rondde in 2024 haar werk af. De commissie die bestaat uit Gerben van Leeuwen en Dennis Raithel, volgde namens de rvt de voortgang van het verder uitwerken van de afspraken tussen SIDN en CIRA in een reeks implementatieovereenkomsten. De commissie was daarbij het klankbord voor de bestuurders. Maar bereidde ook de benodigde besluiten voor tot goedkeuring voor het aangaan van deze overeenkomsten.

De tweede ad-hoccommissie bestaat uit Marjet van Zuijlen en Mark Frequin. Deze was het klankbord voor de bestuurders. Ook ondersteunde de commissie hen in het kader van de publieke discussie en de daaropvolgende betrokkenheid vanuit de politiek, de ministeries en de AIVD door het voorgenomen besluit van SIDN om een deel van het registratiesysteem te migreren naar AWS.

Samenstelling

De raad van toezicht bestond per 31 december 2024 uit 8 leden.

- Marjet van Zuijlen, voorzitter, selectie-, voordrachts- en benoemingcommissie (vz)
- Mark Frequin, vicevoorzitter, selectie-, voordrachts- en benoemingcommissie
- Wim Hafkamp, veiligheids- en stabiliteitscommissie
- Olaf Kolkman, veiligheids- en stabiliteitscommissie
- Sandra Konings, veiligheids- en stabiliteitscommissie
- Gerben van Leeuwen, veiligheids- en stabiliteitscommissie (vz)
- Jeannine Peek, auditcommissie
- Dennis Raithel, auditcommissie (vz)

In 2024 vonden de volgende wijzigingen plaats:

- Mark Frequin is per 1 april 2024 herbenoemd voor 2 jaar*, vanwege zwaarwegende overwegingen.
- Olaf Kolkman trad per 19 juni 2024 toe tot de veiligheids- en stabiliteitscommissie.
- Jeannine Peek is per 1 juli 2024 herbenoemd voor 1 jaar*, vanwege zwaarwegende overwegingen.
- Dennis Raithel is per 5 november 2024 herbenoemd voor 3 jaar.

De leden van de rvt moeten onafhankelijk zijn. Dit is geborgd in de statuten van SIDN en de reglementen van de rvt. Volgens de huidige reglementen is het mogelijk dat een van de leden als niet-onafhankelijk lid kan deelnemen. In 2024 is geen van de leden als niet-onafhankelijk aangemerkt. Ook meldden de leden binnen de rvt geen potentieel tegenstrijdige belangen.

Rooster van aftreden en herbenoemen leden van de raad van toezicht

In overeenstemming met artikel 29 van de statuten heeft SIDN een rooster van aftreden en herbenoemen van de leden van de rvt. Het rooster per 1 april 2025 ziet er als volgt uit:

	Eerste benoeming	Uiterlijke benoemingstermijn	Zitting in
Jeannine Peek*	1 juli 2015	1 juli 2025	Auditcommissie
Wim Hafkamp	1 januari 2023	1 januari 2026	Veiligheids- en stabiliteitscommissie
Mark Frequin*	1 april 2015	1 januari 2026	Selectie-, voordrachts- en remuneratiecommissie
Gerben van Leeuwen**	16 april 2021	1 juli 2029	Veiligheids- en stabiliteitscommissie
Dennis Raithel	5 november 2021	1 januari 2030	Auditcommissie
Marjet van Zuijlen	1 september 2022	1 januari 2031	Selectie-, voordrachts- en remuneratiecommissie
Sandra Konings	1 januari 2023	1 januari 2032	Veiligheids- en stabiliteitscommissie
Olaf Kolkman	1 januari 2024	1 januari 2033	Veiligheids- en stabiliteitscommissie

* Om te voorkomen dat er te veel kennis en ervaring binnen de raad verloren zou gaan, besloot de rvt in maart 2024 om Mark Frequin voor 2 jaar en Jeannine Peek voor 1 jaar te herbenoemen na afloop van hun derde zittingstermijn van 3 jaar.

** Gerben van Leeuwen is benoemd op voordracht van de VvR. Volgens artikel 24 lid 3 sub C van de statuten van SIDN wordt de VvR om advies gevraagd, voordat de rvt een besluit neemt over herbenoeming. Volgens artikel 24 lid 3 sub A en B wordt de VvR, aan het einde van de laatste benoemingstermijn van Gerben van Leeuwen, gevraagd een kandidaat voor te dragen c.q. gevraagd een advies uit te brengen over een door de rvt voorgenomen benoeming.



9 Financieel verslag

Toelichting bij het financieel verslag

Ons doel is om maximale toegevoegde waarde te leveren met een verantwoord en uitlegbaar positief resultaat. Ons financieel beleid is niet gericht op een zo hoog mogelijke winst, maar op de maximalisatie van onze maatschappelijke bijdrage. Het positieve resultaat van 2024 wordt toegevoegd aan het eigen vermogen van de stichting. Het eigen vermogen bevat een continuïteitsreserve zoals overeengekomen met de Nederlandse overheid en ter ondersteuning van de doelstellingen van de stichting. Daarnaast is een deel van het eigen vermogen nodig voor de migratie van .nl naar het Hello Registry-platform in 2026 (zie verdere toelichting bij de vooruitblik).

Vergelijking met budget

Het resultaat voor belastingen over het boekjaar bedraagt € 2,3 miljoen positief en is hiermee substantieel hoger dan het gebudgetteerde resultaat voor belastingen van € 22.000,- positief. Het verschil is vooral te verklaren doordat de personeelskosten in het boekjaar € 1,0 miljoen en de overige bedrijfskosten € 0,9 miljoen lager zijn dan gebudgetteerd. Deze lagere personeelskosten worden veroorzaakt doordat er minder formatieplaatsen zijn ingevuld dan initieel begroot. Dit is in lijn met de keuze om voor enkele functies gebruik te maken van de diensten van derden, vooral als het taken betreft die niet meer langdurig bij SIDN nodig zijn. De kosten voor externe inhuur waren hierdoor hoger dan gebudgetteerd. De overige bedrijfskosten zijn afgenomen als gevolg van minder uitgaven aan (online)marketing. Daarnaast hield de begroting 2024 rekening met een snellere overgang naar de cloud. Door de stijging van de spaarrente in 2024 zijn de financiële baten € 0,1 miljoen hoger dan gebudgetteerd.

Vergelijking met 2023

Het resultaat voor belastingen over het boekjaar is € 2,4 miljoen hoger dan in 2023.

Deze verbetering is vooral toe te schrijven aan de omzettoename en het efficiënter aansturen van de bedrijfsvoering, maar ook de rentestijgingen hebben bijgedragen. Waar banken in 2022 nog rente in rekening brachten op spaargelden, werd in 2023 weer rente vergoed en nam in 2024 de spaarrente verder toe. Naast de toename van de netto-omzet van € 2,6 miljoen (inclusief € 0,7 miljoen eenmalige subsidie-opbrengst) en de licht stijgende bedrijfslasten van € 0,3 miljoen bedrijfslasten, dragen de financiële baten en lasten voor € 0,1 miljoen bij aan de verbetering van het resultaat voor belastingen.

Binnen de bedrijfslasten laten de personeelskosten een daling zien van € 0,9 miljoen en een toename bij de algemene kosten van € 0,5 miljoen. Op bepaalde specialistische functies maakten we bewust gebruik van externen. Zo zijn we flexibel genoeg om in te kunnen spelen op incidenten, ontwikkelingen en fluctuerende inzet op de beheersing van onze systemen en kunnen we gemakkelijk afschalen als dat kan. Op deze manier zorgen we ervoor dat de continuïteit van onze dienstverlening altijd is geborgd en de beschikbaarheid van onze kernsystemen

altijd zeer hoog zijn en voldoet aan de afspraken met onze klanten. Bij de algemene kosten is een toename van kosten te zien ten opzichte van 2023. Dit betrof vooral externe consultancykosten voor het cloudtraject of het outsourcen van bepaalde diensten.

Belastingen

Als gevolg van de doorgevoerde juridische herstructurering vond de berekening van de vennootschapsbelasting tot 28 februari 2023 bij elke entiteit afzonderlijk plaats. Vanaf 1 maart 2023 is sprake van een fiscale eenheid en vindt de berekening van de vennootschapsbelasting plaats over het geconsolideerde resultaat op niveau van SIDN Groep BV. Stichting Internet Domeinregistratie Nederland is vanaf 1 januari 2023 niet langer belastingplichtig voor de vennootschapsbelasting. Bij berekening van de vennootschapsbelasting wordt rekening gehouden met beperkte aftrekbare kosten. In 2022 vernieuwden we de vaststellingsovereenkomst met de Belastingdienst voor de periode 2021-2025. De verschuldigde vennootschapsbelasting over 2024 bedraagt € 908.000,-.

Bestedingen naar activiteiten en diensten

We vinden het belangrijk om transparant te zijn over waar we ons geld aan besteden. Hiervoor maken we jaarlijks een overzicht van de kosten die aan de activiteiten en diensten worden besteed. Hieronder geven we een weergave van de kosten naar activiteiten en diensten.

1. Een waarde(n)vol .nl-domein

Dit betreft vooral de bestedingen aan de activiteiten in het kader van het beheer en ontwikkeling van het .nl-domein. Andere uitgaven die we hiertoe rekenen zijn:

- .nl-activiteiten en onderzoek en ontwikkeling die SIDN Labs voor onze kerntaak uitvoert;
- Kortingen: incasso- en staffelkorting;
- Registrar Scorecard-incentives;
- Financiering van projecten voor registrars en bijdrage aan de Vereniging van Registrars (VvR).

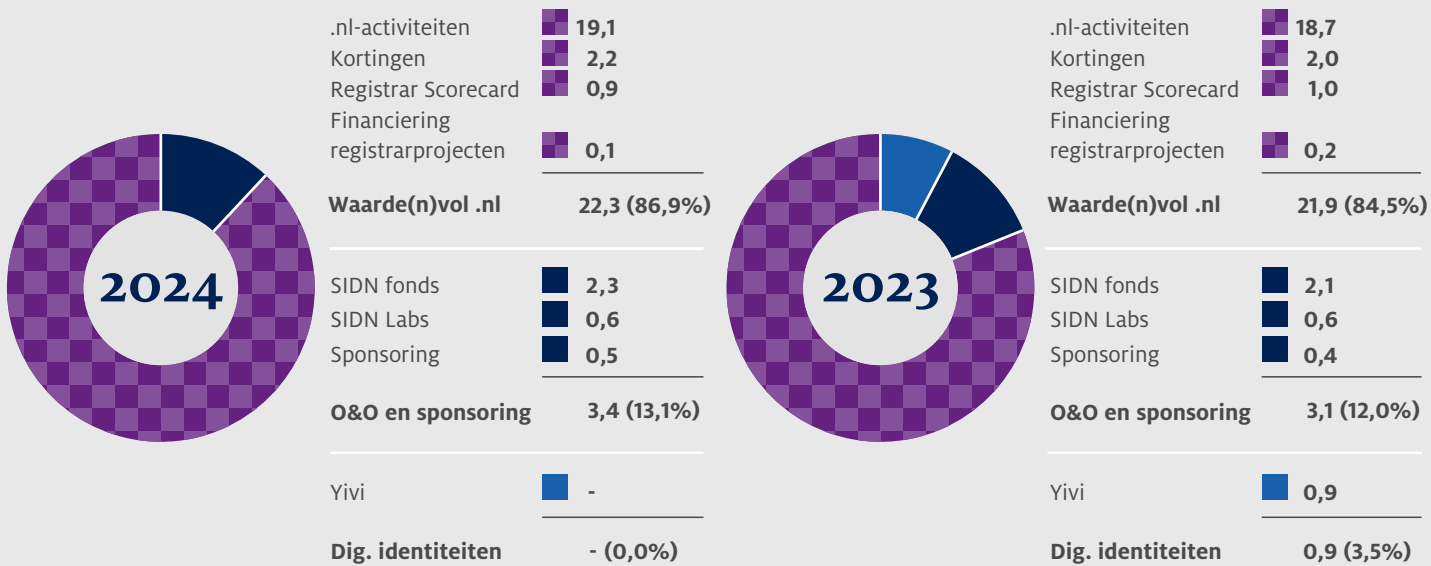
2. Onderzoek, ontwikkeling en investeringen in de internet-gemeenschap

Het positieve rendement uit de exploitatie van .nl zetten we in ten behoeve van de Nederlandse en internationale internet-gemeenschap. Dit zijn onze bijdragen aan SIDN fonds, de financiering van een deel van het werk van SIDN Labs en andere investeringen in de internetgemeenschap. Dit betrof in 2024 onder andere NLnet Labs, ECP, Offlimits/Meldpunt Kinderporno en Bits of Freedom.

3. Digitale identiteiten

Dit omvat onze bestedingen aan Yivi. Yivi is per april 2024 overgedragen aan de Stichting Privacy by Design.

Fig. 12 | Bestedingen naar activiteiten en diensten (x mln. euro's)



Financieel beleid

De prijs van een .nl-domeinnaam voor 12 maanden bedroeg in 2024 € 4,15; een toename van 10% ten opzichte van 2023 (€ 3,76). Deze prijsstijging was nodig de aankomende jaren vanwege de kostenstijging door inflatie en om investeringen in onze ICT-systemen te kunnen doen. Door de prijsstijgingen in 2024 is onze omzet met € 1,9 miljoen toegenomen tot € 25,6 miljoen, ondanks de afname in domeinnamen in 2024. Voor het eerst sinds de oprichting van SIDN nam de omvang van de .nl-zone af en zonder prijsverhoging zou de omzet zijn afgenomen, terwijl de kosten bleven stijgen.

De omzetstijging en de efficiëntere bedrijfsvoering hebben ervoor gezorgd dat ons bedrijfsresultaat sterk is verbeterd. Het resultaat is substantieel hoger dan vooraf begroot maar is passend bij het benodigde weerstandsvermogen voor de jaren 2025 en 2026. Een deel van dit weerstandsvermogen is benodigd voor de eenmalige kosten bij de overstap naar Hello Registry. Per 1 januari 2025 wordt de prijs van een .nl-domeinnaam voor 12 maanden: € 4,25; een toename van 2,5% ten opzichte van 2024.

Vooruitblik

Door aanhoudende inflatie verwachten we in 2025 verdere kostenstijgingen. Daarnaast is het noodzakelijk om te investeren in de vernieuwing van het domeinnaamregistratie-systeem.

Het aantal domeinnamen nam voor het eerst sinds de oprichting van SIDN af en we verwachten dat dit in 2025 verder doorzet.

Door de migratie naar Hello Registry en AWS (die grotendeels in 2025/2026 zal vallen), moeten de huidige infrastructuur en DRS-zaken, die nog boekwaarde hebben bij buitengebruikstelling, in een keer worden afgeschreven in 2026. Hierdoor nemen de afschrijvingskosten structureel toe op het moment van ingebruikname van Hello Registry. Deels vanwege eenmalige kosten en deels vanwege structurele kostenstijgingen,

laat de huidige prognose voor 2026 dan ook een ander beeld zien. Om een gezonde en stabiele positie te behouden, was het daarom noodzakelijk de tarieven in 2025 met 2,5% verhogen. Het gebudgetteerde resultaat voor 2025 voor belasting en interest is € 357.000,- positief. Dit positieve resultaat is bedoeld voor onvoorziene kosten 2025/2026 met betrekking tot de migratie naar Hello Registry/AWS. Zo houden we ons eigen vermogen stabiel met een gezonde financiële bedrijfsvoering.

Risicomanagement

Het risicomanagementinformatiesysteem Vanta ondersteunt ons bij het monitoren van de risico's en beheersmaatregelen. Deze risico's variëren van IT-risico's, financiële risico's, fraude-risico's tot het voldoen aan wet- en regelgeving. Periodiek worden risico's met de raad van bestuur, het management en de rvt besproken en vindt er een actualisatie van het risico-profiel plaats.

Binnen ons risicomanagement maken we onderscheid tussen zachte en harde controles. Beide zijn van cruciaal belang om de doelstellingen van de organisatie te realiseren en risico's te beheersen.

Harde controles

Harde controles zijn de formele, gestructureerde maatregelen die we implementeren om risico's te minimaliseren en de naleving van wet- en regelgeving te waarborgen. Deze omvatten bijvoorbeeld automatische controles in onze IT-systemen, het afdwingen van functiescheiding binnen het betalingsverkeer, salarisbetalingen en het autoriseren en betalen van facturen, of gedetailleerde procedures die medewerkers moeten volgen. Deze controles zorgen voor een concrete, meetbare aanpak van risico's en dragen bij aan de transparantie en verantwoording binnen de organisatie. Interne- en externe audits toetsen de aanwezigheid en effectiviteit van deze beheersingsmaatregelen.

Zachte controles

Zachte controles zijn minder formeel en meer gericht op cultuur en gedrag binnen de organisatie. Dit betreft het toezicht houden op de manier waarop medewerkers en management omgaan met risico's, de ethiek binnen de organisatie en het bevorderen van een open communicatieklimaat. Zachte controles omvatten bijvoorbeeld leiderschap, training en het versterken van het risicobewustzijn binnen teams. Ze zijn van groot belang voor het ontwikkelen van een cultuur waarin medewerkers zich verantwoordelijk voelen voor risicobeheersing en integriteit. We verwachten van al onze medewerkers, evenals van de partijen die namens ons optreden, dat zij integer handelen. Integriteit speelt een cruciale rol in het professioneel functioneren van onze organisatie. Gedragsnormen zijn ook vastgelegd in onze gedragscode. Er is een interne klokkenluidersregeling om misdragingen of onregelmatigheden bij een externe vertrouwenspersoon te melden. De combinatie van harde en zachte controles versterkt onze risicobeheersing en waarborgt dat risicomangement niet alleen een administratieve taak is, maar een gedeelde erantwoordelijkheid binnen de gehele organisatie. Dit stelt ons in staat om zowel interne als externe risico's te identificeren, mitigeren en tegelijkertijd onze organisatiecultuur te versterken.

Governance

Onze raad van toezicht (rvt) houdt toezicht op de strategie, het beleid en de algemene gang van zaken binnen SIDN. Risicobeheersing krijgt hierbij expliciet aandacht. De rvt heeft hiervoor een auditcommissie en een veiligheids- en stabiliteitscommissie aangesteld. De veiligheids- en stabiliteitscommissie ondersteunt de raad bij zijn toezicht op de integriteit, vertrouwelijkheid en stabiliteit van onze dienstverlening en op het controlesysteem voor de naleving van de wet- en regelgeving en de gedragsregels. Daarnaast ziet veiligheids- en stabiliteitscommissie toe op de belangrijke bedrijfsrisico's met betrekking tot veiligheid en stabiliteit en let daarbij vooral op de resultaten van de jaarlijkse interne en externe audits (onder andere: de ISO27001:2022 audit), zoals de audit door de Rijksinspectie Digitale Infra-

structuur (voorheen Agentschap Telecom), en de uitvoering van de ICT- en de securityroadmap. De auditcommissie houdt namens de rvt toezicht op de integriteit van de financiële verslaggeving, het controlesysteem voor naleving van de wet- en regelgeving en de gedragsregels en de financiering van SIDN.

Organisatie

Het managementteam is verantwoordelijk voor het risico-beleid, de risicotolerantie en de (bij)sturing op de beheersingsmaatregelen. Specifiek voor de informatiebeveiligingsrisico's worden we bijgestaan door de chie information security officer. De werkorganisatie is verantwoordelijk voor de primaire risico-beheersing en de rapportering daarover. Sinds 2022 is een interne auditfunctie ingericht. Hierdoor beschikken we over een sterke systematiek van interne beheersing. De interne auditor toetst de doelmatigheid van het managementsysteem en de processen. Bij het selecteren van de auditonderwerpen is gebruikgemaakt van een inschatting van het risico dat een proces onvoldoende wordt beheerst met als gevolg dat mogelijkheden onvoldoende worden benut. Om het management aanvullende zekerheid te geven is in het verslagjaar een aantal operationele audits uitgevoerd. Hierbij lag de focus op de beoordeling van het managementsysteem, de interne beheersing van informatiebeveiligingsprocessen en het aantoonbaar voldoen aan de privacywetgeving. Eind 2024 onderwierp DEKRA ons aan de jaarlijkse audit in het kader van de ISO-certificering voor informatiebeveiliging (27001). Hierbij zijn we succesvol overgestapt op de 2022-versie van de ISO27001-certificering.

Omgaan met risico's

Ons risicobeleid is gericht op het stellen van kaders, normen en waarden, voor het zo effectief mogelijk behalen van onze doelstellingen. We vinden het belangrijk dat er integer en transparant wordt gehandeld.

Risico's en risicotolerantie

Hieronder zijn de voor ons belangrijkste risico's opgenomen. Per risico maakten we vervolgens een afweging ten aanzien van

Fig. 13 | Risicobereidheid van SIDN

Categorie	Risico	Laag	Midden	Hoog
Strategisch	Afhankelijkheid van .nl		•	
Operationeel	Verstoring in de beschikbaarheid van onze dienstverlening	•		
	Inbreuken op de vertrouwelijkheid of integriteit van belangrijke data	•		
Financieel	Solvabiliteit	•		
	Liquiditeitsrisico	•		
	Marktrisico		•	
	Valutarisico		•	
	Renterisico		•	
	Kredietrisico		•	
	Debiteurenrisico		•	
	Schadeclaims en boetes	•		
Wet- en regelgeving	Risico op niet voldoen aan de wet- en regelgeving	•		
Reputatie	Reputatierisico		•	
Vereist eigen vermogen	Het eigen vermogen is lager dan het gestelde minimum		•	

onze risicotolerantie. Het doel hiervan is om vast te stellen of en in welke mate we een specifiek risico wel of niet willen lopen. Deze risicotolerantie staat in verband met de besluitvorming, de beheersingsmaatregelen en de bijsturing, als extra maatregelen nodig zijn om de risico's terug te brengen naar het gewenste niveau.

Voor elk risico beschrijven we de belangrijkste risico's en onzekerheden. Ook gaan we kort in op de ontwikkelingen en beheersing van deze risico's.

Risico's ten aanzien van de strategie

De belangrijkste risico ten aanzien van de strategie zijn de sterke afhankelijkheid van (de omzet uit) het .nl-domein. De verkoop van .nl-domeinnamen gaat via de registrars. We werken daarom nauw samen met registrars via de Vereniging van Registrars (VvR), voor het promoten van .nl-domeinnamen en het verder verhogen van de veiligheid en kwaliteit van .nl.

De coronapandemie zorgde voor een sterkere groei in het aantal domeinnaamregistraties. Deze groei vlakke af in de jaren na corona en het aantal domeinnamen is in 2024 zelfs afgenomen. Voor de komende jaren verwachten we dat de omvang van de .nl-zone verder afneemt. We hebben met onze inzet een relatief beperkte invloed op de eindmarkt, waardoor onze risicotolerantie ten aanzien van strategische risico's gemiddeld is. We kijken naar mogelijkheden om onze impact te vergroten en de dienstverlening te verbreden. Binnen het thema 'Digitale identiteiten en cybersecurity' besloten we om de investeringen in SIDN Merkbewaking voort te zetten.

Risico's ten aanzien van operationele activiteiten

De belangrijkste risico's ten aanzien van operationele activiteiten zijn verstoringen in de beschikbaarheid van onze dienstverlening en inbreuken op de vertrouwelijkheid of integriteit van belangrijke data. Deze risico's kunnen veroorzaakt worden door technisch en/of menselijk falen of – al dan niet doelgerichte – menselijke opzet. Dergelijke calamiteiten kunnen de continuïteit van de organisatie op 2 manieren in gevaar brengen, als ze grootschalig en langdurig zijn. Aan de ene kant door ernstige reputatieschade en het ontstaan van maatschappelijke en politieke discussie over de legitimiteit van SIDN als registry van het .nl-domein. Aan de andere kant door omvangrijke claims voor vergoeding van de schade die onze klanten ondervonden.

Sinds 2011 zijn we ISO27001-gecertificeerd. In het kader van ons Information Security Management System (ISMS) voeren we business-impactanalyses uit. Dat doen we in een jaarlijkse cyclus en volgens het vastgestelde informatiebeveiligingsbeleid. Ook identificeren we risico's, treffen we maatregelen en beoordelen we restrisico's. We nemen bevindingen, rapportages en interne en externe audits mee in onder andere het tactisch securityoverleg en voeren eventuele verbeterpunten uit. De opvolging bewaken we aan de hand van halfjaarlijks managementreviews. Hierbij bespreken we onder andere de resultaten van de audits en performance-metingen en de status van audit-actiepunten en eventueel opgetreden security-incidenten.

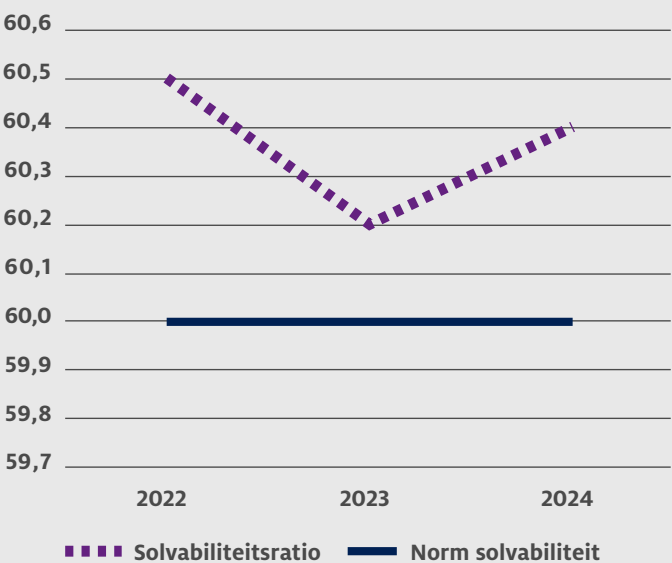
Het belang van sleutelprocessen voor de dienstverlening stellen we vast met business-impactanalyses, die onderdeel zijn van het ISMS. Onze DNS-diensten, die de basis vormen voor het daadwerkelijk functioneren van bestaande domeinnamen, zijn daarbij het meest kritisch. Registratiediensten volgen deze diensten direct voor het registreren van nieuwe en het muteren en opheffen van bestaande domeinnamen. Naast de DNS-diensten en het domeinnaamregistratiesysteem zijn de Whois/Is (zowel de publieke versie als de versie voor registrars), de energievoorziening, kantoorautomatisering, onze website www.sidn.nl, communicatie en telecommunicatie als kritisch gewaardeerd. Om de beschikbaarheid, integriteit en vertrouwelijkheid te waarborgen, troffen we een breed scala aan beheersmaatregelen. Deze richten zich op het verkleinen van de kans op calamiteiten, het mogelijk maken van snel herstel en het beperken van de gevolgen van deze calamiteiten. Onze risicotolerantie ten aanzien van operationele risico's is laag als het gaat om verstoringen in de beschikbaarheid van onze dienstverlening en inbreuken op de betrouwbaarheid en vertrouwelijkheid van belangrijke data.

Financiële risico's

Solvabiliteit

De solvabiliteit berekenen we als de verhouding tussen het eigen vermogen en balanstotaal. Onze solvabiliteit bedraagt 60,4% (2023: 60,2%) en ligt hiermee boven de vastgestelde norm van 60%. Het eigen vermogen nam de afgelopen jaren af door gebudgetteerde verliezen. In 2024 is een positief saldo gerealiseerd. Hiermee blijft het weerstandsvermogen op peil met een surplus van circa € 3 miljoen. Hiermee verwachten we dat het eigen vermogen stabiel zal blijven binnen de gestelde norm.

Fig. 14 | Solvabiliteit



Liquiditeitsrisico (inclusief concentratierisico)

Dit betreft het risico dat we over onvoldoende liquide middelen beschikken om aan onze verplichtingen te kunnen voldoen. Eind 2024 bedraagt het saldo liquide middelen € 28,5 miljoen (2023: 29,4 miljoen), een afname van € 0,9 miljoen ten opzichte van 2023. Het saldo van de liquide middelen is ruim voldoende voor de financiering op de korte en lange termijn. Het concentratierisico hebben we gemitigeerd door onze liquide middelen te spreiden over 3 Nederlandse banken.

Marktrisico

Dit betreft het risico van een waardedaling van de aangekochte staatsobligaties en de overige effecten. De Nederlandse en Duitse staatsobligaties worden tot het einde van de looptijd aangehouden. Als het nodig blijkt om de staatsobligaties eerder te verkopen, dan lopen we het risico dat de waarde van de staatsobligaties daalt ten opzichte van de aankoopwaarde. Met de overige effecten lopen we een risico van waardedaling. We identificeerden geen indicaties (trigger events) van een mogelijke waardedaling van deze effecten.

Valutarisico

Dit is het risico dat de waarde van de overige effecten daalt als gevolg van veranderingen in de valutakoers van de Noorse Kronen. Daarnaast betreft dit het koersrisico bij in- of verkoop in een andere valuta dan de euro. De prijzen van onze .nl-dienstverlening luiden in euro's, waardoor we hier geen valutarisico lopen. We kopen beperkt in bij leveranciers die andere valuta dan de euro hanteren. Daardoor is het valutarisico hier zeer beperkt.

Renterisico

Hier gaat het om het risico dat de waarde van de staatsobligaties en/of leningen verandert als gevolg van veranderingen in marktresen. De staatsobligaties worden tot het einde van de looptijd aangehouden, waardoor het renterisico nauwelijks aanwezig is.

Kredietrisico

Dit is het risico dat tegenpartijen niet aan de contractuele verplichtingen kunnen voldoen. Dit betreft de overige effecten, debiteuren en overige vorderingen. Het debiteurenrisico is beperkt aangezien ruim 75% van de registrars via automatische incasso betaalt. In onze algemene voorwaarden definiëren we vervolgstappen als een registrar niet aan zijn financiële verplichtingen voldoet.

Schadeclaims en boetes

Dit is het risico op onderbrekingen in de dienstverlening en verlies van vertrouwelijkheid of integriteit van data. Onze algemene voorwaarden beperken een dergelijke aansprakelijkheid of sluiten deze uit. Onze risicotolerantie ten aanzien van deze risico's is gemiddeld tot laag.

Risico's ten aanzien van wet- en regelgeving

Wijzigingen in nationale en internationale wet- en regelgeving beïnvloeden onze organisatie en bedrijfsprocessen. We nemen in een vroeg stadium kennis van (initiatieven tot) wijzigingen in wet- en regelgeving die ons raken. Deze variëren van

wijzigingen in arbeids- en belastingwetgeving tot informatiebeveiliging. Gevolgen brengen we in kaart, vertalen we naar de organisatie en voeren we in. De HR-manager en de legal & policy manager adviseren bij risico's op het gebied van wet- en regelgeving. Daarnaast hebben we een functionaris gegevensbescherming en een privacyboard in het kader van de Algemene verordening gegevensbescherming. Onze risicotolerantie ten aanzien van risico's op het gebied van wet- en regelgeving is laag.

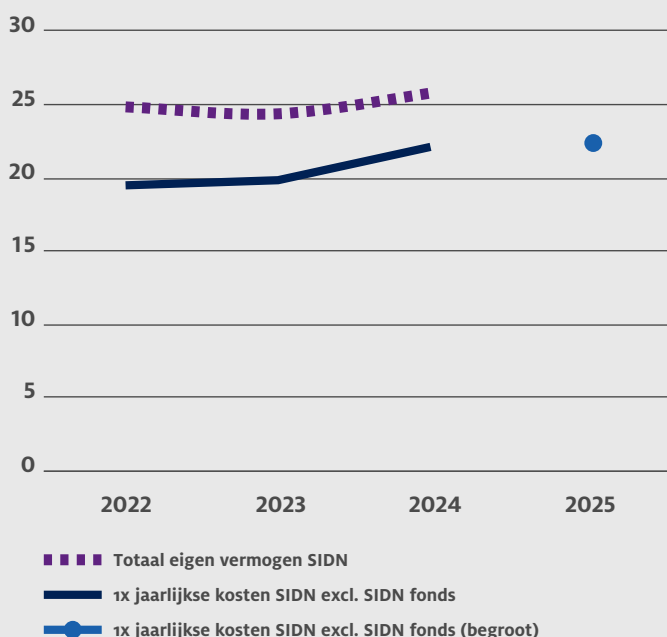
Reputatierisico

Om het reputatierisico te beheersen, werken we nauw samen met onze stakeholders, waaronder de .nl-registrars, de VvR en het ministerie van Economische Zaken en Klimaat. We voeren actief stakeholdermanagement met de registrars via de VvR. We hechten veel belang aan de kwaliteit van onze dienstverlening en hoe we deze kunnen vasthouden en verbeteren. Daarom voeren we jaarlijks de Registrartevredenheidsmonitor uit. Daarnaast monitoren we actief de mediaexposure van onze organisatie.

Weerstandsvermogen

Om de continuïteit van onze organisatie te waarborgen, is het van belang dat we over voldoende financiële buffer beschikken in het geval een aanzienlijk deel van onze inkomsten wegvalt. Het weerstandsvermogen is ook belangrijk om mogelijke financiële gevolgen van geïdentificeerde risico's te kunnen dragen. Daarnaast dienen we in geval van discontinuïteit over voldoende vermogen te beschikken voor het ordentelijk afwikkelen en/of overdragen van de .nl-activiteiten. De norm voor het minimum eigen vermogen is gelijk aan

Fig. 15 | Eigen vermogen i.r.t. weerstandsvermogen (x mln. euro's)



éénmaal de jaarlijkse kosten. De huidige omvang van het eigen vermogen ligt boven de vastgestelde ondergrens. Onze financiële afdeling bewaakt de toereikendheid van het aanwezige eigen vermogen ten opzichte van het vastgestelde minimum en rapporteert hier periodiek over. Op basis van het weerstandsvermogen, ratio's, begroting aankomend jaar en de huidige stand van zaken binnen SIDN zijn wij van mening dat het terecht is dat de jaarrekening wordt opgesteld op basis van het continuïteitsbeginsel.

Fraude en onregelmatigheden

Als organisatie beheren wij maatschappelijk kapitaal. Onze stakeholders mogen van ons verwachten dat wij middelen efficiënt, effectief en op een rechtmatige manier besteden en verantwoorden. Fraude ondermijnt dit principe en is dan ook onaanvaardbaar. Het voorkomen van wangedrag en fraude is van cruciaal belang om een integere, veilige en verantwoorde werkomgeving te waarborgen. Wangedrag en fraude kunnen niet alleen de reputatie, veiligheid en financiële stabiliteit van SIDN schaden, maar ook het vertrouwen van medewerkers, de overheid, klanten en andere belanghebbenden ondermijnen. Onze organisatie heeft diverse maatregelen getroffen om fraude en onregelmatigheden te voorkomen. Dit wordt onder meer toegelicht in de paragraaf over risicomanagement, waarin zowel zachte als harde controles worden besproken. De maatregelen omvatten de implementatie van een gedragscode, uitvoering van regelmatige interne audits en de beschikbaarheid van een interne klokkenluidersregeling, waarmee medewerkers anoniem onregelmatigheden kunnen melden. In 2025 wordt dit uitgebreid met een externe klokkenluidersregeling en zal de frauderisico-analyse worden geïntegreerd in Vanta, ons risicomanagementsysteem. De raad van bestuur en de raad van toezicht dragen de primaire verantwoordelijkheid voor het voorkomen en tijdig opsporen van fraude. Over 2024 tot het vaststellen van het jaarverslag en de jaarrekening hebben wij binnen onze organisatie geen gevallen van fraude of onregelmatigheden geconstateerd.



Geconsolideerde jaarrekening over 2024

Geconsolideerde balans per 31 december 2024

Vaste activa

Immateriële vaste activa

Immateriële vaste activa in uitvoering
Software

31 december 2024 (in €)

3.363.989
447.052

3.811.041

31 december 2023 (in €)

1.008.273
183.058

1.191.331

Materiële vaste activa

Bedrijfsgebouwen en -terreinen
Machines en installaties
Andere vaste bedrijfsmiddelen

4.384.912
523.034
372.424

5.280.370

4.613.717
840.023
516.439

5.970.179

Financiële vaste activa

Deelnemingen in overige verbonden partijen
Andere deelnemingen
Vorderingen op overige verbonden partijen
Overige effecten

3
1.300.000
158.148
1.386.229

2.844.380

-
1.300.000
-
622.436

1.922.436

Flottende activa

Vorderingen

Handelsdebiteuren
Belastingen en premies sociale verzekeringen
Overlopende activa

728.524
-
1.561.880

2.290.404

736.259
18
1.306.420

2.042.697

Liquide middelen

28.479.022

29.362.816

Totaal

42.705.217

40.489.459



Passiva

Groepsvermogen

Kortlopende schulden

Crediteuren

Belastingen en premies sociale verzekeringen

Overlopende passiva

Totaal

31 december 2024 (in €)

25.825.090

25.825.090

512.017

1.911.452

14.456.658

16.880.127

42.705.217

31 december 2023 (in €)

24.424.224

24.424.224

572.552

1.357.292

14.135.391

16.065.235

40.489.459



Geconsolideerde winst- en verliesrekening over 2024

	2024 (in €)	2023 (in €)
Netto-omzet	25.609.819	23.004.433
Som van de bedrijfsopbrengsten	25.609.819	23.004.433
Inkoopwaarde van de omzet	63.439	111.558
Personeelskosten	12.063.380	12.922.996
Afschrijvingen en waardeveranderingen	1.630.451	928.342
Overige bedrijfskosten		
Huisvestingskosten	470.572	416.484
Exploitatiekosten	2.392.723	2.216.159
Verkoopkosten	1.355.329	1.600.840
Kantoorkosten	741.508	705.184
Algemene kosten	4.874.811	4.360.082
Som van de bedrijfslasten	23.592.213	23.261.645
Bedrijfsresultaat	2.017.606	-257.212
Rentebaten en soortgelijke opbrengsten	326.122	166.891
Rentelasten en soortgelijke opbrengsten	-34.597	-
Financiële baten en lasten	291.525	166.891
Resultaat vóór belastingen	2.309.131	-90.321
Belastingen	-908.266	-282.214
Nettoresultaat na belastingen	1.400.865	-372.535



Geconsolideerd kasstroomoverzicht over 2024

	2024 (in €)	2023 (in €)
Bedrijfsresultaat	2.017.606	-257.212
Aanpassing voor afschrijvingen	1.630.451	928.342
Mutatie van handelsdebiteuren	7.735	-549.377
Mutatie van overige vorderingen	-255.442	617.792
Mutatie van handelscrediteuren	-60.535	137.992
Mutatie van overige kortlopende schulden (excl. schulden kredietinstellingen)	875.427	415.833
Kasstroom uit bedrijfsoperaties	4.215.242	1.293.370
Ontvangen interest	326.122	166.891
Betaalde interest	-34.597	-
Betaalde winstbelasting	908.266	-282.214
Kasstroom uit operationele activiteiten	3.598.501	1.178.047
Investerings in immateriële vaste activa	-3.836.562	-255.578
Desinvesteringen in immateriële vaste activa	377.456	-
Investerings in materiële vaste activa	-105.304	-540.702
Desinvesteringen in materiële vaste activa	4.057	5.535
Verwervingen van niet-geconsolideerde maatschappijen	-3	-
Mutatie overige financiële vaste activa	-1.007.939	-35.431
Ontvangst uit hoofde van effecten	86.000	273.777
Kasstroom uit investeringsactiviteiten	-4.482.295	-552.399
Mutatie in liquide middelen	--883.794	625.648



io Personalia



Bestuur

Roelof Meijer (CEO)
Loek Bakker (CTO)

Bijzondere raadgevers

Piet Beertema
Boudewijn Nederkoorn
Ted Lindgreen
Eddy Schuyer

Directie

Laura van der Bij (financieel directeur)
Cristian Hesselman (directeur SIDN Labs)
Arjan Middelkoop (commercieel directeur)

Ondernemingsraad

Jeroen Roosen (voorzitter)
Carolien Bruggeman
Chris Faber
Romana Siebers (secretaris)
Angelika Takes
Thymen Wabeke (vicevoorzitter)

College voor Klachten en Beroep

Doeke Kingma (voorzitter)
Elmar Besselink
Klaas Bisschop
Huib Gardeniers (secretaris)
Sylvia Huydecoper
Elisabeth Thole

Raad van toezicht

Marjet van Zuijlen (voorzitter)
Mark Frequin (vicevoorzitter)
Wim Hafkamp
Olaf Kolkman
Sandra Konings
Gerben van Leeuwen
Jeannine Peek
Dennis Raithel



II Woordenlijst

Abuse

Misbruik op het internet. Bekende vormen van abuse zijn spamware, phishing en botnets.

Anycast

Globale anycast is een bewezen en effectieve technologie die de netwerk-belasting verspreidt over meerdere exemplaren van wat dezelfde server lijkt. De werking is even simpel als doeltreffend: verschillende servers delen één IP-adres, de routers 'denken' dat het dezelfde server is. IP-pakketten worden doorgestuurd naar het 'dichtstbijzijnde' punt. Lokale anycast maakt gebruik van zogenaamde lokale nodes: computers of andere apparaten die zijn aangesloten op een bepaald netwerk en alleen lokaal benaderd kunnen worden. Hierdoor kan wereldwijd DDoS-verkeer niet bij een lokale node uitkomen. Dat kan alleen lokaal gegenereerd DDoS-verkeer, en dit is beter onder controle te krijgen. Daarmee vormt lokale anycast een effectief antwoord op het risico van DDoS-aanvallen.

Artificial intelligence (AI)

AI, ook wel kunstmatige intelligentie genoemd, is het concept waarbij computers taken uitvoeren waar normaal gesproken menselijke intelligentie voor nodig is.

Autonomie

Autonomie betekent dat je zelf bepaalt hoe je handelt, zonder dat je beperkt, gedwongen of beïnvloed wordt door anderen.

AWS

AWS staat voor Amazon Web Services en is een bedrijfsonderdeel van Amazon.com dat voorziet in webdiensten en cloud-computing.

BGP

Het Border Gateway Protocol (BGP) is het belangrijkste routeringsprotocol van het internet: het wordt gebruikt om verkeer tussen verschillende providers te routeren.

ccTLD

Een topleveldomein, uitsluitend bedoeld voor landen. Voorbeelden zijn .nl (Nederland), .de (Duitsland) en .fr (Frankrijk).

CENTR

CENTR is een vereniging van registry's van Country Code Top Level Domeinnamen (ccTLD's), zoals SIDN. Het is een discussieforum op het gebied van beleid dat betrekking heeft op de registratie van ccTLD's en fungeert als communicatiekanaal richting partijen die bij de (verdere) ontwikkeling van het internet betrokken zijn, zoals ICANN. Zie ook centr.org.

CIRA

CIRA is de registry van het Canadese .ca-domein.

College voor Klachten en Beroep (CvKB)

Een onafhankelijk college waar registrars en houders van een .nl-domeinnaam in beroep kunnen gaan tegen bepaalde beslissingen van SIDN. Het CvKB behandelt ook klachten, als de klager vindt dat een domeinnaam is geregistreerd in strijd met de openbare orde of de goede zeden. Zie ook cvkb.nl.

Cloud native

De term cloud-native verwijst naar het concept van het bouwen en uitvoeren van applicaties om te profiteren van het gedistribueerd computergebruik dat wordt aangeboden door het cloud-leveringsmodel. Cloud-native apps zijn ontworpen en gebouwd om te profiteren van de schaal, rekbaarheid, veerkracht en flexibiliteit die de cloud biedt.

DANE

DNS-based Authentication of Named Entities (DANE), is een protocol voor het veilig publiceren van publieke sleutels en certificaten.

DDoS

Distributed denial-of-service-aanvallen zijn pogingen om een computer, netwerk of dienst onbruikbaar te maken voor de bedoelde gebruiker. Deze aanvallen kunnen op meerdere manieren uitgevoerd worden.

DKIM

DomainKeys Identified Mail (DKIM) voorkomt vervalsing van e-mails. Als iemand knoeit met de inhoud van een e-mail, detecteert DKIM dat.

DMARC

Domain-based Message Authentication, reporting and Conformance (DMARC) vertelt je mailserver wat hij moet doen als hij een verdachte e-mail ontvangt. Bijvoorbeeld verwijderen of doorsturen naar een bepaald mailadres. Ook zorgt DMARC ervoor dat een organisatie informatie krijgt over vervalste e-mail die uit naam van de organisatie verstuurd is.

DNS

Afkorting van Domain Name System (Domein Naam Systeem) of Domain Name Server. Het wereldwijde DNS is het systeem en protocol dat op het internet gebruikt wordt om domeinnamen naar IP-adressen te vertalen en omgekeerd.

DNSSEC

Domain Name System Security Extensions (DNSSEC) is een uitbreiding op het DNS. Deze cryptografische beveiliging voor het DNS-protocol is bedoeld om te voorkomen dat internet-criminelen gebruikers ongemerkt omleiden naar nepsites. Het huidige DNS-protocol is daar niet optimaal tegen beschermd.

Domeinnaam

Een naam in het Domain Name System (DNS), het naamgevingssysteem op internet. Een domeinnaam, zoals sidn.nl, bestaat uit verschillende gedeeltes: het topleveldomein, '.nl', en het second-leveldomein, 'sidn'.

Domeinnaamhouder

De persoon of organisatie op wiens naam een domeinnaam geregistreerd is. Alleen de domeinnaamhouder heeft recht op diensten van SIDN.

Domeinnaamregistratiesysteem (DRS)

Het systeem dat wij beschikbaar stellen voor .nl-registrars voor de registratie en het beheer van .nl-domeinnamen.

Data Protection Impact Assessment (DPIA)

Een data protection impact assessment is een instrument om vooraf, dus voordat er daadwerkelijk gegevens uitgewisseld worden, de privacyrisico's van een gegevensverwerking in kaart te brengen en te beoordelen.

ECP

Binnen ECP, Platform voor de Informatie-Samenleving, werken bedrijfsleven, overheid en maatschappelijke organisaties samen om het gebruik van ICT in de Nederlandse samenleving te versterken. Zie ook ecp.nl.

ENTRADA

Een open source big data-platform dat ontwikkeld is door SIDN Labs om grote hoeveelheden DNS-data te analyseren. De database waarvan ENTRADA gebruik maakt, bevat meer dan 100 miljoen DNS-zoekopdrachten.

Geschillenregeling voor .nl-domeinnamen

Wie een domeinnaam registreert, moet ervoor zorgen dat hij daarmee geen inbreuk maakt op de rechten van een ander. Hierover kunnen geschillen ontstaan. Bijvoorbeeld op basis van merkrechten, handelsnamen, namen van overheidsorganen of eigennamen. De Geschillenregeling biedt in zo'n geval een snel en goedkoop alternatief voor een gang naar de rechter.

gTLD

Generic top-level domain, een van de soorten internetdomeinen. Voorbeelden zijn .com, .org of .edu. Vanaf 2014 zijn veel nieuwe generieke topleveldomeinen gestart, waaronder .amsterdam.

Hostingprovider

Een hostingprovider is een bedrijf dat zich heeft gespecialiseerd in het aanbieden van webhosting. De dienst hosting bestaat uit het aanbieden van opslagruimte, rekenkracht en netwerkverkeer met behulp van een webserver. Behalve het laten hosten van websites en e-mail op een eigen of gedeelde server kun je bij vrijwel elke hostingprovider je domeinnaam laten registreren.

ICANN

De Internet Corporation for Assigned Names and Numbers is een non-profitorganisatie die een aantal belangrijke taken uitvoert, zoals het toekennen en specificeren van topleveldomeinen, het toewijzen van domeinnamen en de distributie van IP-nummers. ICANN beheert zelf geen domeinnamen. Dit gebeurt door registry's zoals SIDN (.nl) of VeriSign (.com en .net). Zie ook icann.org.

IETF

De Internet Engineering Task Force is een internationale gemeenschap van netwerkontwerpers, -operators, -leveranciers en -onderzoekers die zich bezighoudt met de ontwikkeling van internetstandaarden. Zie ook ietf.org.

(Internet)extensie

Een ander woord voor topleveldomein, het meest rechtse deel van een domeinadres na de punt, zoals '.nl' in 'sidn.nl'.

Interne governance

De ontwikkeling en toepassing van gedeelde principes, normen, regels, besluitvormingsprocedures en programma's die het gebruik van internet vormgeven.

Internet Governance Forum (IGF)

Het Internet Governance Forum (IGF), een onderdeel van de Verenigde Naties, is een jaarlijkse vergadering van overheden, marktpartijen en burgerorganisaties. Hier worden publieke beleidsproblemen besproken met het doel het internet beheersbaar, robuust, veilig en stabiel te houden. Het IGF stelt zelf geen beleid vast. Zie ook intgovforum.org.

Internet Protocol (IP)-adres

Een IP-adres is een unieke combinatie van cijfers en of letters. Elke computer of server die verbonden is met internet heeft een eigen IP-adres waarmee het vindbaar is. Op de website www.whatismyip.com kun je zien wat het adres is van de computer waar je nu achter zit.

IPv6

Elke computer of server die verbonden is met internet heeft een eigen IP-adres waarmee het vindbaar is. Internet Protocol versie 6 ondersteunt een nagenoeg oneindige hoeveelheid IP-adressen. De adressen met IPv4 (versie 4) raken op.

ISP

Een internetserviceprovider (ISP) biedt andere organisaties en particulieren toegang tot internet. Daarnaast kan de provider ook andere diensten aanbieden, bijvoorbeeld e-mailadressen, webhosting en het wegfilteren van spam.

Malware

Een verzamelnaam voor kwaadaardige software, zoals computervirussen of worms.

Nameserver

Een computer op het internet die ervoor zorgt dat een domeinnaam wordt 'vertaald' naar een IP-adres, een uniek nummer op het internet. Deze computer maakt onderdeel uit van het DNS.

Nepwebwinkel

Een malafide webshop, bedoeld om te frauderen. Fake webshops zijn op het eerste gezicht vaak niet te onderscheiden van echte webshops.

NL IGF

Een samenwerking van het ministerie van Economische Zaken, SIDN en ECP. Het doel is enerzijds om de uitkomsten van het internationale Internet Governance Forum (IGF) een goede inbedding te geven in het nationale beleid en anderzijds om de Nederlandse stem internationaal te laten horen en Nederlandse thema's in te brengen in het IGF.

Notice-and-Take-Down-procedure

Een vrijwillige gedragscode voor het omgaan met meldingen van onrechtmatige en strafbare inhoud op websites, zoals kinderporno, plagiaat, discriminatie of aanbod van illegale goederen. De gedragscode beschrijft welke stappen doorlopen moeten worden met een klacht over de inhoud van een website. Men kan eerst terecht bij de aanbieder van de bewuste inhoud. Als deze niet bereikbaar is of niet wil meewerken, kan men zich wenden tot de partij daarboven in de keten. De keten ziet er als volgt uit:

- aanbieder van de content
- aanbieder van de website (domeinnaamhouder)
- hoster van de website
- aanbieder van de internettoegang
- SIDN (registry)

Als alle partijen in de keten zijn benaderd om de strafbare of onrechtmatige inhoud van een website te verwijderen, kan SIDN als uiterste maatregel een domeinnaam buitengebruikstellen.

NTP

Het Network Time Protocol (NTP) is een protocol waarmee computers die onderling met elkaar in verbinding staan, hun interne klok kunnen synchroniseren met andere computers.

Opensource

Een manier van ontwikkeling waarbij men vrije toegang geeft tot de bronmaterialen. Bij opensourcesoftware is de broncode van de software voor iedereen vrij beschikbaar, zodat iedereen het kan kopiëren, aanpassen en verspreiden zonder kosten voor bijvoorbeeld auteursrechten.

Phishing

Een vorm van internetcriminaliteit. Internetgebruikers worden misleid met vervalste e-mails en websites die sterk lijken op uitingen van bekende en betrouwbare bedrijven. Hierin wordt hen gevraagd naar bijvoorbeeld logingegevens of creditcardinformatie, met alle gevolgen van dien.

Polarisatie

Polarisatie is het toenemend wij-zij-denken. Het is een proces waarbij de tegenstellingen tussen groepen in de samenleving sterker worden, waardoor groepen steeds meer tegenover elkaar komen te staan.

Post-quantumcryptografie

Post-quantumcryptografie (PQC), ook wel kwantumbestendig, kwantumveilig of kwantumbestendig genoemd, is de ontwikkeling van cryptografische algoritmen (meestal algoritmen met publieke sleutels) waarvan wordt aangenomen dat ze veilig zijn tegen een cryptanalytische aanval door een kwantumcomputer.

RegCheck

Een systeem dat interpreteerbare risicoscores toekent aan nieuwe domeinnaamregistraties.

Registrar

Een tussenpersoon die namens de (potentiële) domeinnaamhouder het contact onderhoudt met de registry (voor .nl is dat SIDN). Meestal zijn dit hostingbedrijven, internet-service- of accessproviders.

Registrar Scorecard

Incentiveprogramma voor de .nl-registrars waarbij de registrars in aanmerking kunnen komen voor financiële incentives als zij bijvoorbeeld moderne internetstandaarden zoals IPv6 en DNSSEC ondersteunen voor de .nl-domeinnamen in hun portfolio.

Registry

Ook wel domain name registry. Het register met alle internetdomeinnamen voor een topleveldomein, of de organisatie die dit register beheert.

Registryserviceprovider

Het verlenen van registrydiensten voor andere topleveldomeinen dan het eigenlijk toplevel waarvoor de registry is opgericht. In ons geval verlenen wij registrydiensten voor bijvoorbeeld het .amsterdam- en .politie-domein.

Resolving

Antwoord geven op een DNS-vraag.

Resolver

Op het moment dat je een webadres (url) invult in de adresbalk van je browser, dan wordt dit adres vertaald naar het IP-adres dat bij de domeinnaam hoort. Deze vertaalslag wordt ook wel resolving genoemd.

RIPE NCC

Het Réseaux IP Européens Network Coordination Centre is als Regional Internet Registry (RIR) verantwoordelijk voor de uitgifte van IP-adressen voor Europa en het Midden. Naast RIPE NCC zijn er nog vier andere RIR's: APNIC (voor Azië en Australië), AfriNIC (voor Afrika), LACNIC (Latijns-Amerika) en ARIN voor (Noord-Amerika). Zie ook ripe.net.

SCION

SCION is een nieuwe internetarchitectuur die is ontworpen om routecontrole, foutisolatie en expliciete vertrouwensinformatie voor end-to-endcommunicatie te bieden.

SDG

De Sustainable Development Goals (SDG's), zijn zeventien doelen om van de wereld een betere plek te maken in 2030. Ze zijn een mondiaal kompas voor uitdagingen als armoede, onderwijs en de

klimaatcrisis. In 2015 hebben alle 193 landen die lid zijn van de Verenigde Naties (VN) de Sustainable Development Goals aangenomen. De doelen gelden voor alle landen en voor alle mensen.

Security.txt

Security.txt is internetstandaard in de vorm van een eenvoudig tekstbestand met de contactgegevens van de beheerder van een website dat op de webserver staat. Ethische hackers of cyberonderzoekers met goede bedoelingen die de website-beheerder willen waarschuwen kunnen de contactgegevens gebruiken. Zo komt een melding meteen op de juiste plek terecht.

Server

Een krachtige computer met een snelle verbinding die is ingericht om informatie te leveren. Een webserver is rechtstreeks met het internet verbonden.

Serviceprovider

Een internet-serviceprovider (ISP) biedt internetdiensten aan, zoals digitale televisie en internettelefonie. Ook leveren ISP's netwerkkapitaal voor huisnetwerken.

Signeren

DNSSEC werkt met digitale handtekeningen, zogenaamde private keys. Voor een goede beveiliging moeten DNS-gegevens eerst met zo'n handtekening ondertekend worden (signeren) en daarna dient deze geverifieerd te worden (valideren).

Spam

Verzamelnaam voor ongewenste e-mailberichten.

SPF

Sender Policy Framework (SPF) voorkomt dat iemand in naam van iemand anders een e-mail kan versturen. SPF controleert de afzender van een e-mail op echtheid.

StartTLS

StartTLS zorgt voor een beveiligde verbinding tussen de verzendende en ontvangende mailserver.



TLD

Afkorting voor Top Level Domain. Dit is het meest rechtse deel van een domeinadres na de punt. Bijvoorbeeld 'nl' in de domeinnaam 'sidn.nl'.

Topleveldomein

Het meest rechtse deel van een domeinadres na de punt, zoals 'nl' in 'sidn.nl'.

Typosquatting

Een vorm van internetmisbruik, gebaseerd op het feit dat mensen zich vergissen bij het intypen van een web- of e-mailadres. De gebruiker wordt dan naar een andere site geleid, vaak met een criminele intentie. Zo gaat phishing dikwijls gepaard met typosquatting.

Valideren

DNSSEC werkt met digitale handtekeningen, zogenaamde private keys. Voor een goede beveiliging moeten DNS-gegevens eerst met zo'n handtekening ondertekend worden (signeren) en daarna dient deze geverifieerd te worden (valideren).

Vereniging van Registrars (VvR)

Deze vereniging vertegenwoordigt de belangen van registrars richting SIDN en overlegt regelmatig met SIDN over de hoofdlijnen van diens beleid.

Whitelisten

IP-adressen op een 'witte lijst' zetten zodat internetverkeer van of naar die bepaalde adressen wordt doorgelaten.

Whois

Een protocol om domeinnaamgegevens, zoals de naam en het adres van de eigenaar en de provider, uit een database te halen. SIDN beheert de Whoisgegevens voor alle .nl-domeinnamen. Zie sidn.nl/whois.

WIPO Arbitration and Mediation Center

Een onafhankelijke, internationale non-profitorganisatie die zich bezighoudt met de arbitrage in onder meer conflicten rondom domeinnamen. Zie ook wipo.int.

Yivi

Yivi biedt een oplossing om op een privacyvriendelijke manier in te loggen bij organisaties. Een gebruiker zet gevalideerde attributen in de Yivi-app

en maakt zich bij het inloggen via de app alleen bekend met relevante kenmerken van zichzelf. Zo deelt de gebruiker alleen het hoognodige en houdt hij grip op welke gegevens hij verstrekt aan organisaties. Yivi heette voorheen in IRMA. De naam veranderde in 2022.

Zonefile

Een tekstbestand waarin domeinnamen en de bijbehorende IP-adressen van web-servers staan.



Uitgave

SIDN

Meander 501

6825 MD Arnhem

Postbus 5022

6802 EA Arnhem

026 352 55 00

communicatie@sidn.nl

www.sidn.nl

www.sidnlabs.nl

Concept en vormgeving

[Lumen Ontwerpersnetwerk](#)

Tekst

[Kilay Brands](#)

Vertalingen

[G & J Barker Translations](#)

Auteursrechten

©SIDN

Teksten en cijfers uit dit jaarverslag mogen overgenomen worden, maar wij willen dan wel graag als bron vermeld worden.

Ook worden wij graag vooraf geïnformeerd via communicatie@sidn.nl.

Colofon