

# 2018

# Jaarverslag



Jouw wereld. Ons domein.



# 2018

## Inhoud

<b>01</b>	<b><u>Voorwoord</u></b> .....	4
<b>02</b>	<b><u>.nl</u></b> .....	6
<b>03</b>	<b><u>Oplossingen</u></b> .....	12
<b>04</b>	<b><u>Veilig internet</u></b> .....	16
<b>05</b>	<b><u>SIDN Labs</u></b> .....	20
<b>06</b>	<b><u>Kennis</u></b> .....	24
<b>07</b>	<b><u>SIDN</u></b> .....	28
<b>08</b>	<b><u>Verslag raad van toezicht</u></b> .....	35
<b>09</b>	<b><u>Financieel verslag</u></b> .....	38
<b>10</b>	<b><u>Personalia</u></b> .....	47
<b>11</b>	<b><u>Woordenlijst</u></b> .....	49
	<b><u>Colofon</u></b> .....	53

# O I

## Voorwoord



# Hard gewerkt aan het realiseren van onze missie

Ook in 2018 werkten wij hard aan het realiseren van onze missie: het verbinden van mensen en organisaties voor een zorgeloos digitaal bestaan. De rode draad in al onze activiteiten in 2018 was het verder vergroten van onze toegevoegde waarde voor Nederland; onze impact op onze economie en maatschappij. We deden dat langs 3 hoofdlijnen. Allereerst door de positie van het .nl-domein te versterken, met activiteiten gericht op positionering, kwaliteit, veiligheid en innovatie. Ten tweede door de ontwikkeling en groei van dochterbedrijf Connectis, het realiseren van synergie tussen de 2 bedrijven en door het ontwikkelen van kansrijke nieuwe propositities in de gebieden online security en digital identity. En als laatste – maar zeker niet als minste – door te investeren in ontwikkelingen voor de internetgemeenschap. Dat doen we via het SIDN fonds, met de onderzoeksprojecten van SIDN Labs, door onze inzet in internationale netwerken zoals CENTR, ICANN, IETF en IGF, en met onze betrokkenheid bij een veelheid aan activiteiten en programma's in Nederland gericht op digitale veiligheid en vaardigheid.

Vorig jaar namen we ons voor om onze impact te vergroten. Ik ben van mening dat dit gelukt is. Met ons werk dragen we bij aan het succes, de kwaliteit en de veiligheid van internet in Nederland. In dit jaarverslag lees je alles over de verschillende manieren waarop we dit in 2018 deden. Ik ben ervan overtuigd dat onze toegevoegde waarde voor Nederland en voor de internetgemeenschap het komende jaar alleen maar verder groeit.

Roelof Meijer,  
algemeen directeur SIDN

# 02

# .nl

# .nl-domein stabiel

**Het .nl-domein maakte een kleine groei door. De merkvoorkeur voor het domein steeg, mede dankzij een succesvolle campagne voor .nl. De tevredenheid van registrars en andere klanten was hoger dan ooit.**

## Ontwikkeling .nl-domein

Na een onverwacht hoge groei in 2017 liet het .nl-domein in 2018 een lichte groei zien. Er vonden 802.739 nieuwe registraties plaats en 764.742 opheffingen. Met name in de tweede helft van het jaar groeide de zone. De totale groei kwam uit op 37.997, een groeipercentage van 0,66%. We eindigden het jaar met 5.832.037 .nl-domeinnaamregistraties. De meeste nieuwe registraties waren voor zakelijk gebruik. Het aandeel zakelijke registraties blijft stijgen.

## Marktaandeel blijft stijgen

Het marktaandeel (zie fig. 2) van .nl in Nederland steeg. Dit kwam vooral doordat andere toplevel-domeinen krompen. Met name de nieuwe gTLD's verloren veel domeinnaamregistraties, van circa 210.000 eind 2016 naar zo'n 180.000 registraties begin 2018. Ook gevestigde domeinen als .org lieten krimp zien.

## Stijging IPv6

Het aantal via IPv6 bereikbare .nl-domeinnamen steeg licht, van bijna 1,6 miljoen naar ruim 1,7 miljoen. Wij zetten er flink op in om dit aantal te verhogen, onder meer met een incentive in de Registrar Scorecard (RSC). Toch ondersteunen helaas nog niet alle registrars uit de top-15 IPv6. We zagen het aantal IPv6-queries van resolvers geleidelijk toenemen. Vergeleken met sommige andere landen gaat de adoptie van IPv6 echter

6

Fig. 1 | Ontwikkeling .nl-domein

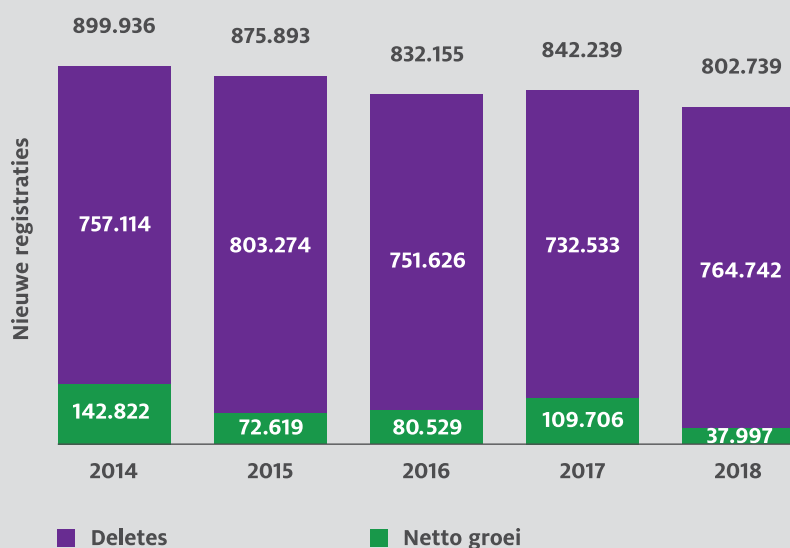
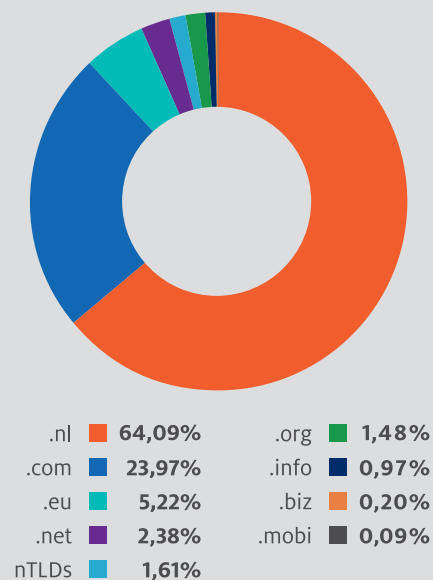


Fig. 2 | Marktaandeel in 2018





langzaam, bleek uit de IPv6-inventarisatie die we in 2018 uitvoerden. Zo is slechts 13% van alle bezoeken aan een Google-pagina in ons land afkomstig van een IPv6-adres.

Dit komt vooral doordat de grootste Nederlandse accessproviders internetgebruikers geen volwaardige IPv6-verbinding aanbieden. Dit is slecht voor de toekomstbestendigheid van de Nederlandse internetstructuur en de positie van het Nederlandse bedrijfsleven, omdat het ons land minder interessant maakt voor investeringen en innovaties op het gebied van onder meer het internet-of-things (IoT).

## Vergeleken met sommige andere landen gaat de adoptie van IPv6 langzaam.

### Hoge beschikbaarheid ondanks grote storing

Onze DNS-systemen, de absolute kern van onze dienstverlening, hadden ook in 2018 een beschikbaarheid van 100%. Het aantal voor onze registrars merkbare onderhoudsvensters van ons registratiesysteem (DRS) was minimaal en alle onderhoudsvensters met downtime werden binnen de aangekondigde tijdspanne afgerond. Eind januari hadden we last van een grote storing als gevolg van een storing in de firmware van een leverancier. Hierdoor was ons registratiesysteem circa 6 uur lang onbereikbaar. Dit was de aanleiding voor verbeteringen in onze infrastructuur waardoor zulke verstoringen in de toekomst voorkomen worden.

### Marketingactiviteiten

We werken nauw samen met onze registrars op zakelijk gebied. Een goed voorbeeld hiervan is de 'funnel' die we in 2017 bouwden rondom het Whois-gedeelte van onze website. Potentiële domeinnaamhouders worden direct doorgeleid naar een registrar die aan hun wensen voldoet. Bovendien krijgen zij suggesties te zien als hun gewenste domeinnaam niet meer beschikbaar is. In 2018 ontwikkelden we de funnel verder en leidde de tool tot duizenden leads voor onze registrars.

Onder de noemer 'Meer klik met .nl' voerden we een marketingcampagne voor .nl. De campagne zorgde voor een stijging van de merkvoorkeur voor .nl van 72% naar 79%.

Hoewel de campagne nadrukkelijk op (startende) ondernemers was gericht, zorgde het ook voor een stijging van de merkvoorkeur bij particulieren. Dit toont aan dat het onderscheid tussen particulier en zakelijk in de domeinnamenmarkt steeds moeilijker te maken is. Daarnaast organiseerden we in samenwerking met de VvR een marketingactie op de Dag van de Domeinnaam (7 juni).

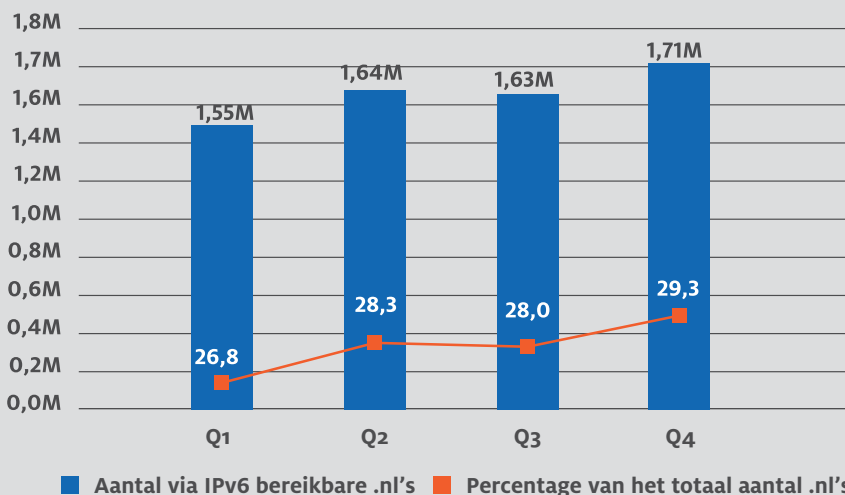
### Geschillenregeling voor .nl-domeinnamen

Onder de Geschillenregeling voor .nl-domeinnamen startten in 2018 69 zaken bij het WIPO Arbitration and Mediation Center. In 37 zaken kwam het tot een uitspraak. De overige zaken zijn vóór de uitspraak beëindigd, bijvoorbeeld omdat de eisende partij de zaak introk of omdat de partijen onderling schikten. 3 zaken lopen nog. Onze mediators behandelden 22 zaken en in 9 gevallen was succesvolle mediation de reden voor een vroege regeling van het geschil.

### Wijzigingen in Whois

We voorzagen onze Whois van een nieuwe backend waarmee we klaar zijn voor het nieuwe Whois-protocol (RDAP) dat ICANN naar verwachting in 2019 invoert.

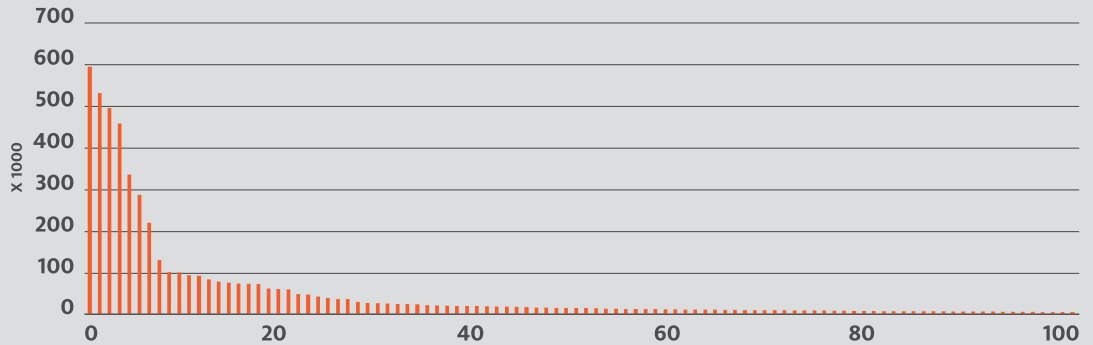
Fig. 3 | Ontwikkeling aantal via IPv6 bereikbare domeinnamen in 2018



## Ontwikkelingen registrarveld

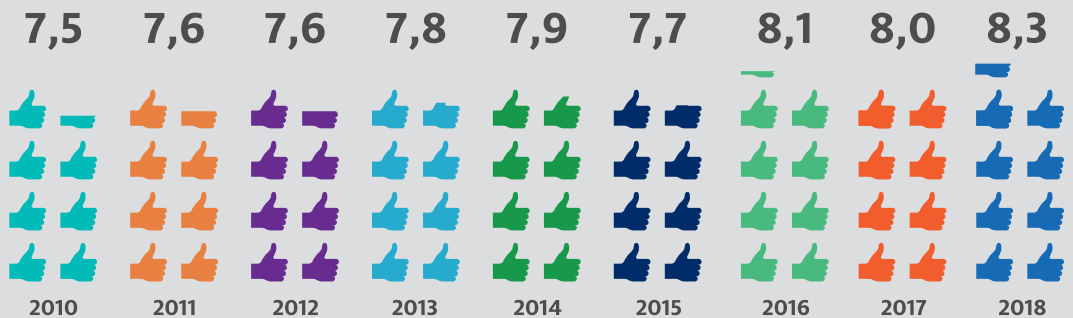
.nl-domeinnamen worden aangeboden door een grote en diverse groep registrars. Al jaren zien we het aantal registrars licht dalen. Deze concentratietendens zette door. In 2018 nam het aantal registrars af van 1.303 tot 1.237. Kenmerkend waren enkele grote overnames en fusies waardoor een aantal zeer grote partijen ontstond.

Fig. 4 | Aantal domeinnamen per registrar



## Registrartevredeheid

Ieder jaar onderzoeken we de tevredenheid van onze registrars. In 2018 waardeerden zij onze dienstverlening met een 8,3, het hoogste cijfer ooit. Vooral het persoonlijk contact met onze supportafdeling en de evenementen die we organiseren werden hoog gewaardeerd. Grote registrars waardeerden onze support zelfs met een 9. Sommige registrars waren kritisch over de beperking van het aantal opvragingen dat een registrar mag doen in de registrar-Whois. De beperking was echter nodig om aan de wettelijke vereisten vanuit de AVG te voldoen.



## Webinars

In een aantal webinars deelden we onze kennis over onder meer de impact van de AVG op domeinnaamregistratie.

## Samenwerking met de Vereniging van Registrars

Onze registrars behoren tot onze belangrijkste stakeholders. De Vereniging van Registrars (VvR) behartigt hun belangen richting SIDN. Wij dragen de kosten van de VvR en werken constructief met de vereniging samen. Regelmatig levert de VvR ons waardevolle ideeën, adviezen en suggesties. In 2018 ontwikkelden we samen met de VvR een juridisch loket voor de bij de VvR aangesloten registrars. De .nl-registrars krijgen hier snel en kosteloos antwoord op vragen over zaken als privacy, algemene voorwaarden, ICT en recht. Daarnaast ontwikkelden we samen met de VvR een privacyportal, een online portal dat registrars ondersteunt om AVG-compliant te worden. Op verzoek van de VvR zorgden we ervoor dat registrars locatie-ongebonden gebruik kunnen maken van het registratiesysteem door via VPN in te loggen. Verder betrokken wij de VvR en onze registrars bij de ontwikkeling van nieuwe propositities. Met het VvR-bestuur richtten we een registrar-klankbordgroep op waarmee we de nieuwe propositities 'eHerkenning' en 'Online security voor het mkb' bespraken. De waardevolle feedback die dit opleverde, nemen we mee in het verdere ontwikkeltraject. Tot slot deelden we onze kennis met registrars via de SIDN Academy. De eerste activiteit in dit nieuwe initiatief was een gratis eendaagse cursus over e-mailstandaarden.

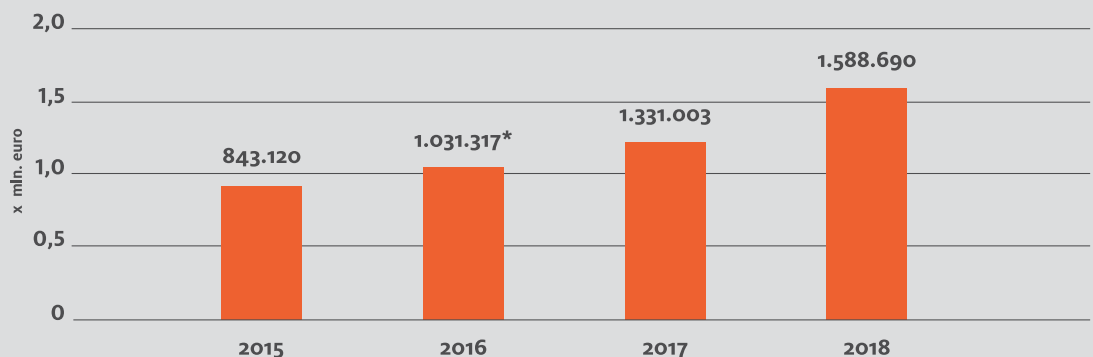


## In 2018 waardeerden registrars onze dienstverlening met een 8,3, het hoogste cijfer ooit.

### Registrar Scorecard

De Registrar Scorecard (RSC) beloont registrars voor investeringen in de waarde van het .nl-domein. Het programma bevordert de kwaliteit van registratiegegevens en het actief gebruik van .nl, ontmoedigt opheffingen, en stimuleert investeringen in veiligheid en moderne standaarden en de bestrijding van phishing en malware. Deze financiële incentives hadden in 2018 een waarde van € 1,5 miljoen. 370 registrars doen inmiddels mee met de RSC.

Fig. 5 | Uitgekeerd bedrag aan incentives



\*Vanaf 2016 is de korting op met DNSSEC beveiligde domeinnamen onderdeel geworden van de RSC.

### Notice-and-Take-Down-regeling

De Notice-and-Take-Down-regeling beschrijft welke stappen je moet doorlopen als de inhoud van een website onmiskenbaar onrechtmatig of strafbaar is. Als uiterste maatregel kunnen wij een domeinnaam buiten gebruik stellen. We kregen 35 verzoeken onder de Notice-and-Take-Down-procedure. In 7 gevallen gingen we over tot buitengebruikstelling van een domeinnaam. In alle andere gevallen ondernam een andere partij in de keten actie of was er geen sprake van onmiskenbaar onrechtmatige of strafbare inhoud. Eind 2018 werd, in samenwerking met het Expertisebureau Online Kindermisbruik, een addendum toegevoegd aan de nationale Gedragscode Notice en Take Down waardoor kinderpornografisch materiaal makkelijker van het internet verwijderd kan worden.

### College voor Klachten en Beroep

Registrars en houders van .nl-domeinnamen kunnen tegen beslissingen van SIDN in beroep gaan bij het College voor Klachten en Beroep (CvKB). Dit onafhankelijke college behandelt daarnaast ook

klachten over domeinnaamregistraties die in strijd zouden zijn met de openbare orde of de goede zeden. In 2018 ontving het college 3 beroepen. Deze leidden niet tot een inhoudelijke beoordeling door het CvKB omdat de indieners ervan het beroep introkken of niet doorzetten.

### Vooruitblik

In samenwerking met onze registrars ontwikkelen we de funnel en de suggestietool op onze website verder, zodat registranten makkelijker de juiste domeinnaam en registrar kunnen vinden. Ook blijven we met de Registrar Scorecard investeren in de adoptie van open standaarden zoals IPv6. Samen met het registrarkanaal zetten we op basis van data marketingacties op ter versterking van .nl. Om de veiligheid van .nl op het huidige hoge niveau te houden, gaan we, mede op basis van DBS, partijen helpen om beter op te treden tegen misbruik van domeinnamen.



# Berend van Dalfzen

CEO van Realtime Register

“De website van SIDN wordt maandelijks bezocht door duizenden mensen die daar checken of een domeinnaam nog vrij is. Maar SIDN verkoopt geen domeinnamen, dat doen de registrars en hun resellers. Daarom heeft SIDN een funnel gebouwd op haar website. Als je nu een domeinnaam zoekt en hij is nog vrij, krijg je de logo's van een aantal registrars te zien. Klik je daarop, dan ga je direct het verkoopproces in op de website van de registrar. De logo's die getoond worden, zijn steeds willekeurig gekozen – zo maakt elke registrar evenveel kans op extra websitebezoek.

De funnel kan een registrar soms wel honderden nieuwe registraties per maand opleveren. Als het bij die registraties bleef, dan stelde het allemaal niet veel voor. Maar elke registratie is het begin van een relatie. Klanten nemen bijvoorbeeld ook een hostingpakket of VPS af. En dan wordt het interessant.

Naast de verkoopfunnel heeft SIDN ook een suggestietool op de website. Als de domeinnaam van je keuze niet vrij is, geeft deze tool een aantal suggesties die wel vrij zijn. Het is heel goed dat deze tool er is. We hebben hem ook geïntegreerd in onze eigen suggestietool ADAC die wij onze resellers ter beschikking stellen. Maar de suggesties waarmee de suggestietool van SIDN komt, zijn vaak niet goed genoeg. Dat komt voor een deel omdat de tool gebaseerd is op een retro-tool: hij put voor zijn suggesties uit domeinnamen die in het verleden al eens geregistreerd zijn geweest. Wij hebben hier feedback op gegeven en mede op basis hiervan wordt de suggestietool verbeterd. Het is mooi dat SIDN de registrars serieus neemt en hen op deze manier faciliteert.”

*De funnel kan een registrar soms wel honderden nieuwe registraties per maand opleveren.*

# 03

## Oplossingen



# Focus op security en identity

**We gingen samenwerken met nieuwe partijen en scherpten onze doelstellingen aan. Nieuwe activiteiten zoeken we vooral binnen de groeidomeinen online security en digital identity.**

## IRMA

We startten een samenwerking met Privacy by Design, de stichting die de techniek achter het identiteitsplatform IRMA ontwikkelt. IRMA staat voor 'I Reveal My Attributes'. Een attribuut kan elk persoonlijk kenmerk zijn, zoals leeftijd, woonplaats, of burgerservicenummer. Met IRMA kun je bepaalde attributen van jezelf wel laten zien en andere juist niet. Samen met Privacy by Design zoeken we naar proposities en toepassingen om IRMA verder in de markt te zetten.

---

*SPIN geeft eindgebruikers grip op wat slimme apparaten in hun thuisnetwerk doen.*

---

## SPIN

SPIN is een opensource systeem voor de beveiliging van IoT-apparaten in huis, die SIDN Labs in 2017 ontwikkelde. SPIN beschermt het internet door IoT-apparaten in thuisnetwerken automatisch, tijdelijk te blokkeren als ze afwijkend verkeer versturen of ontvangen, en geeft eindgebruikers grip op wat IoT-apparaten in hun thuisnetwerk doen. In 2018 zochten we naar de beste manier om SPIN op grote schaal te introduceren. Het eerste concrete resultaat is de samenwerking met een fabrikant van modems, die de SPIN-software zal aanbieden op al hun apparaten. Inmiddels verkennen we de samenwerking met meerdere aanbieders in deze markt. We denken via dit businessmodel de meeste impact te bereiken. We onderzoeken de mogelijkheden voor een verdienmodel dat zal draaien om extra services.

## Mkb veilig online

Internetcriminelen wisten in 2018 bij 52% van de bedrijven in het mkb geld of gegevens buit te maken. Desondanks blijven maatregelen vaak uit. Het ontbreekt veel ondernemers aan de tijd, kennis of financiële middelen. Eind 2018 gingen we een samenwerking aan met Guardian360, specialist in het beveiligen van IT-infrastructuren. In een co-creatietraject ontwikkelen we een nieuwe propositie die het mkb helpt om hacks en datalekken te voorkomen en de risico's slachtoffer te worden van een cyberaanval te verkleinen. Voor deze nieuwe propositie willen we onze registrars betrekken als kanaal richting de markt.

### **Domeinnaambewakingservice**

De Domeinnaambewakingservice, kortweg DBS, is een monitoringdienst die bedrijven waarschuwt voor domeinnaamregistraties die sterk lijken op bijvoorbeeld hun eigen domeinnaam of merknaam. Hiermee kunnen bedrijven sneller actie ondernemen tegen typosquatting, phishing en inbreuk op merkrechten. In 2018 was er veel media-aandacht voor dit soort fraude.

---

## *We identificeerden maar liefst 450 phishing sites die misbruik maakten van de namen van zorgverzekeraars.*

---

Vooraf de ceo-fraude die het Pathé-concern maar liefst 19 miljoen euro kostte werd breed uitgemeten. Mede hierdoor zagen we een flinke stijging in het aantal gebruikers van DBS. Daarnaast gebruikten we DBS voor een analyse van de websites van zorgverzekeraars. We identificeerden maar liefst 450 phishing sites die misbruik maakten van de namen van zorgverzekeraars. Deze zijn gemeld en aangepakt op basis van de notice-and-takedown procedure. We deelden tips voor het herkennen van dergelijke phishing sites met zorgverzekeraars en consumenten.

### **Samenwerking met Simplerinvoicing beëindigd**

Simplerinvoicing is een afsprakenstelsel dat e-facturatie tussen verschillende ERP- en boekhoudpakketten en factureringsdiensten mogelijk maakt. Sinds 2014 beheerden wij dit stelsel voor de stichting Simplerinvoicing. Sindsdien is de stichting verder geprofessionaliseerd waardoor onze ondersteuning niet langer noodzakelijk was. Zoals gepland beëindigden we in 2018 onze samenwerking met de stichting.

### **Vooruitblik**

In 2019 willen we 4 proposities in de markt verder ontwikkelen. We zoeken naar concrete toepassingen voor IRMA. Ook zullen we de SPIN-software doorontwikkelen; we gaan samenwerkingen aan met meer partners en richten het verdienmodel verder in. Het doel is om minimaal 2 proposities tot een succes te maken. Daarnaast blijven we nieuwe mogelijkheden voor toekomstige proposities verkennen die passen binnen onze strategie.

### **eHerkenning**

eHerkenning is het 'DigiD voor bedrijven'. Binnenkort moeten bedrijven verplicht eHerkenning gebruiken om in te loggen bij overheidsdiensten, zoals de Belastingdienst, en andere organisaties. Nog zeker 700.000 bedrijven, verenigingen en stichtingen moeten zo'n eHerkenningmiddel aanschaffen.

Connectis is een van de 5 Nederlandse aanbieders. Registrars gaan eHerkenning afnemen bij Connectis en aanbieden aan hun klanten. Zo profiteren zij van de kansen die onze overname van Connectis oplevert.



# Bart Jacobs

Hoogleraar computerbeveiliging en voorzitter Privacy by Design

“Sinds kort werken we samen met SIDN. SIDN gaat ons helpen om IRMA verder te brengen. IRMA is een door ons ontwikkeld identiteitsplatform dat werkt op basis van attributen. IRMA staat dan ook voor ‘I Reveal My Attributes’. Een attribuut kan elk persoonlijk kenmerk zijn, zoals leeftijd, woonplaats, of burgerservicenummer. Vaak hoeven organisaties maar enkele kenmerken van je te weten. Om een bepaald computerspel te mogen spelen, is het niet belangrijk wie je bent, maar alleen of je wel oud genoeg bent. Voor een medische verklaring is vooral de BIG-registratie van de arts van belang. IRMA geeft gebruikers controle over welke gegevens verwerkt worden. Het beschermt je privacy door alleen de strikt noodzakelijke gegevens te verstrekken.

Wij zijn goed in de techniek aan de achterkant. Maar niet in de operationele kant, in marketing bijvoorbeeld. Daar komt bij dat we een kleine organisatie zijn. In gesprekken met partijen die overwegen om met IRMA te gaan werken, krijgen we regelmatig vragen over onze stabiliteit. Bestaat Privacy by Design over 5 jaar nog wel? Wat gebeurt er als ik eruit stap? Kunnen jullie garanderen dat het altijd werkt? Met SIDN halen we niet alleen veel operationele kennis in huis, maar ook een grote stabiele organisatie. Een organisatie die onze missie deelt. Het is mooi dat SIDN net als wij geen winstoogmerk heeft. IRMA is open source en dat moet het blijven.”

*Met SIDN halen we niet alleen veel operationele kennis in huis, maar ook een grote stabiele organisatie.*

# 04

## Veilig internet

# Proactief bijdragen aan veiligheid

**We speurden proactief naar fakewebshops, verbeterden de veiligheid van onze systemen en droegen bij aan de toepassing van veilige internetstandaarden.**

## Interne ICT-systemen

Abuse204.nl (spreek uit als 'abuse to zero for .nl') is een programma waarmee we, samen met registrars en hostingproviders, de strijd aangaan met phishing en malware in de .nl-zone. Abuse204.nl brengt registrars en hostingproviders op de hoogte van abuse in hun netwerk, zodat zij in actie kunnen komen. Onze afdeling Registratie & Services houdt een vinger aan de pols en ondersteunt waar mogelijk. In 2018 werkten we aan een verdere verkorting van de levensduur van phishing sites en websites met malware. Desondanks liep de gemiddelde levensduur op van 17 uur eind 2017 naar 18 uur aan het einde van 2018. Voor de start van het programma was dit gemiddelde nog 144 uur. In december is opeens een piek zichtbaar. Die piek wordt veroorzaakt door het toevoegen van nieuwe categorieën (shopping site skimmer en cryptojacker) aan de scan waarmee we de zone controleren.

## Validatie DNSSEC blijft achter

Het is enorm belangrijk dat de DNSSEC-standaard geadopteerd wordt. DNSSEC lost een aantal kwetsbaarheden in het DNS op door een extra beschermingslaag toe te voegen aan het bestaande DNS-protocol. Bezoekers van domeinnamen die beveiligd zijn met DNSSEC, zijn beter beschermd tegen omleiding naar IP-adressen die misbruikt worden om bijvoorbeeld malware te verspreiden. Ook vormt DNSSEC de basis voor nieuwe veiligheids-toepassingen, zoals DANE. Begin 2018 waren 49,27% van alle geregistreerde .nl-domeinnamen met

DNSSEC beveiligd. Dat percentage steeg naar 53,49% eind december. Net als in 2017 bleef de validerende zijde ver achter: de 2 grootste Nederlandse accessproviders bieden nog steeds geen DNSSEC-validatie voor hun klanten. In 2017 luidden wij hier de noodklok over. Aan deze situatie is helaas nog weinig tot niets veranderd. Uitgebreide DNSSEC-statistieken zijn te vinden op [stats.sidnlabs.nl](https://stats.sidnlabs.nl).

---

## *DNSSEC lost een aantal kwetsbaarheden in het DNS op.*

---

## Hercertificering ISO27001

Het ISO27001-certificaat is een kwaliteitsstandaard voor informatiebeveiliging die bewijst dat de beschikbaarheid, continuïteit, vertrouwelijkheid en integriteit van informatie op hoog niveau worden gehouden. In 2011 waren we de eerste registry ter wereld die volgens deze standaard werd gecertificeerd. De jaarlijkse audit leverde in 2018 geen bevindingen op en de certificering werd voor de 8e keer verstrekt.

## Veilige e-mailstandaarden

We breidden de Registrar Scorecard, onze incentiveregeling voor .nl-registrars, uit met verschillende standaarden om e-mail te beveiligen. Registrars krijgen een incentive als ze de standaarden StartTLS, DKIM, SPF en DMARC toepassen op de domeinnamen in hun portfolio. Met deze standaarden kunnen verschillende vormen van abuse, waaronder phishing en spam, worden tegengegaan.





### **Volledig over op anycast**

Een onderzoek uit 2017 van SIDN Labs naar de manier waarop DNS-resolvers in het veld autoritatieve nameservers selecteren, was voor ons operations-team de aanleiding om de unicast nodes voor .nl uit te faseren en volledig over te gaan op anycast. Dit verhoogt de snelheid van het DNS-verkeer en voegt redundantie toe, wat het systeem robuuster maakt.

### **Fakewebshops**

Op basis van onderzoek van SIDN Labs en onze supportdesk wijzen we registrars op domeinnamen met fakewebshops. Registrars ondernemen vervolgens in de meeste gevallen zelf actie. Zo werden ten minste 12.000 fakewebshops offline gehaald. Ook voeren we bij fakewebshops controles uit naar de identiteit van de domeinnaamhouder. De registratiegegevens van fakewebshops blijken vaak niet te kloppen. Naar aanleiding van deze controles haalde onze supportdesk samen met onze registrars nog eens minimaal 5.000 fakewebshops uit de lucht.

---

*Zo werden ten minste  
17.000 fakewebshops  
offline gehaald.*

---

### **Awareness voor online veiligheid**

Op verschillende manieren droegen we bij aan de awareness op het gebied van online veiligheid. Dat deden we allereerst met onze nieuwsbrief en tal van artikelen op onze website. Daarnaast startten we de online campagne 'Hackman'. In films op social media toonden we hoe actrice en presentatrice Lieke van Lexmond gehackt werd door een ethisch hacker. Bij de campagne hoorden een website met tips en een test die mensen liet ervaren hoe zij omgingen met hun veiligheid online. Met bijna 1,3 miljoen views was de campagne zeer succesvol. Zo'n 30.000 gebruikers vulden de tests op hackman.nl in. Uit dit onderzoek bleek dat Nederlanders zich wel bewust zijn van de risico's van onveilig smartphonegebruik maar dat er nog een wereld te winnen is. Zo maakt slechts 33% gebruik van 2 factor authenticatie bij het mobiel inloggen op social media. Positief is dat 60% van de Nederlanders een software-update van de smartphone direct installeert.

### **Liaison NCSC**

Als een van de liaisons van het Nationaal Cyber Security Centrum (NCSC) vormen we de verbinding tussen het NCSC en verschillende andere samenwerkingspartners. We delen kennis en informatie met het NCSC.

### **Vooruitblik**

In 2019 blijven we investeren in een veilig .nl-domein en een veilig internet. We zetten hierbij nadrukkelijk in op samenwerking. Met overheden, met anti-abuse initiatieven en binnen de domeinnaamsector. Daarnaast vullen we de werkzaamheden van ons security operations centre verder in en verstevigen we de rol van het team. We blijven proactief speuren naar fakewebshops en abuse.

### **Fakewebshops**

We intensiveren onze aanpak van fakewebshops. Met een nieuwe tool van SIDN zullen we fakewebshops nog eerder detecteren. Een procedurele verandering maakt het mogelijk om ze eerder offline te halen als de gegevens van de domeinnaamhouder niet kloppen. Dit alles zal ervoor zorgen dat fakewebshops weken minder lang actief kunnen zijn en dus minder slachtoffers kunnen maken.

A close-up portrait of Lynn van Herp, a woman with long brown hair and blue eyes, smiling warmly. The background is a solid light blue.

# Lynn van Herp

Voorzitter liaisonoverleg Nationaal Cyber Security Center

“Digitale veiligheid raakt alle sectoren van de samenleving. Voor een effectieve aanpak van cybersecurity is het dan ook belangrijk dat alle sectoren samenwerken. Daarom heeft het NCSC liaisons in het leven geroepen: personen van publieke en private organisaties die een sector of een doelgroep vertegenwoordigen.

Zij vormen een ‘linking pin’ tussen het NCSC en hun eigen sector/organisatie.

Elke donderdag is er een liaisonoverleg. Hier bouwen we aan onderling vertrouwen, aan het versterken van ons netwerk en wisselen we informatie uit. Je wil dat alle organisaties elkaar in zowel de ‘warme’ als ‘koude’ fase weten te vinden: in crisissituaties, maar ook daarbuiten. Er wordt gesproken over actuele ontwikkelingen, welke trends, dreigingen en kansen zien we en hoe kunnen we daarop acteren? Het gaat er niet zozeer om dat de liaisons zelf acties opzetten, maar meer dat zij dingen in gang zetten.

SIDN is een van de liaisons. Het bedrijf brengt specifieke kennis en expertise in en is de aangewezen partij voor vragen over het .nl-domein en domeinnaamregistratie. Hiernaast zijn er goede banden tussen NCSC en SIDN Labs ten aanzien van research & development. De kennis die zij ontwikkelen en onderzoeksresultaten die zij opleveren, zijn voor veel partijen nuttig en kan onder andere via het liaisonschap verder worden verspreid.”

*Het bedrijf brengt specifieke kennis en expertise in en is de aangewezen partij voor vragen over het .nl-domein en domeinnaamregistratie.*

# 05

## SIDN Labs

# Steeds meer impact

**Ook in 2018 droeg het onderzoek van SIDN Labs bij aan het verder verhogen van de veiligheid en stabiliteit van .nl, het DNS en het internet. De impact van ons werk neemt toe en we worden steeds vaker gezien als erkend expertisecentrum. We startten met een nieuwe onderzoekslijn op het gebied van nieuwe internetsystemen.**

## Root Canary tool

In 2017 sloten we ons aan bij het Root Canary-project, een project van 7 partners: SURFnet, de Universiteit Twente, Northeastern University, NLnet Labs, SIDN Labs, RIPE NCC en ICANN. Het doel van het internationale samenwerkingsproject was om de geplande wisseling van de DNS root key zorgvuldig te bewaken. Op 11 oktober vond deze DNS root key rollover plaats en verving ICANN het huidige cryptografische sleutelbaar dat de basis vormt voor de DNSSEC-infrastructuur door een nieuw sleutelbaar. Wij gebruikten onze Root Canary-tool om de wisseling te monitoren. We publiceerden onze resultaten in real-time op ons twitter-account en presenteerden ze op OARC29. Daarnaast gebruikten we onze Root Canary-tool ook om de algoritme-rollover bij onze collega's van .se (Zweden) en .br (Brazilië) te monitoren.

## Metingen DNS

Samen met de Universiteit Twente, University of Southern California, University of Passo Fundo en NLnet Labs onderzochten we de effecten van DDoS-aanvallen op het gedrag van DNS-resolvers. We brachten in kaart hoe caching van DNS-verzoeken in DNS-resolvers de weerbaarheid van het DNS verhoogt. De keuze voor de time-to-live (TTL) die resolvers gebruiken voor hun caches speelt hierbij een cruciale rol. Te kleine TTLs blijken DDoS-aanvallen te kunnen verergeren. Ons artikel over dit onderzoek werd geaccepteerd voor de ACM Internet

Measurement Conference 2018, een prestigieuze internationale conferentie. We zijn in IETF-verband bezig om ons onderzoek op dit gebied samen te vatten in de vorm van een best current practice voor operators van autoritatieve DNS-servers.

## SPIN

We voerden een nieuw ontwerp door voor SPIN, ons open sourceplatform om het internet en eindgebruikers te beschermen tegen onveilige slimme apparaten in het internet of things (IoT). Met het nieuwe ontwerp is SPIN op meerdere manieren in te zetten, onder meer als basiscomponent in netwerkapparatuur. We hielpen ons propositie-development-team om op basis hiervan een product te ontwikkelen om SPIN op grote schaal te introduceren op modems en routers.

Daarnaast ontwikkelden we de SPIN-software verder, onder meer met een eerste versie van een module voor de automatische detectie van onveilige apparaten, zodat ze bijvoorbeeld niet mee kunnen doen in een DDoS-aanval. We presenteerden SPIN op verschillende congressen, zoals de CENTR R&D workshop, het RIOT-congres, ICT.Open en het Innovatiecongres van het ministerie van Justitie en Veiligheid.

Ook startten we samen met de TU Delft het MINIONS-project, dat zich onder meer richt op het meten van concentraties van onveilige apparaten op het internet, het in kaart brengen van IoT-botnets en het herstellen van de veiligheid van geïnfecteerde apparaten.

## DMAP: verbeteringen en detectie fakewebshops

In 2017 ontwikkelden we DMAP (Domain name ecosystem MAPper), een tool die automatisch alle domeinnamen in een zone bezoekt en doormeet, bijvoorbeeld om te bepalen of ze beveiligingscertificaten gebruiken of bereikbaar zijn via IPv6. In 2018 verbeterden we DMAP.



Daarnaast zetten we de tool in om mogelijke fake-webshops te herkennen onder de 5,8 miljoen domeinnamen in de .nl-zone. Met deze informatie probeert onze supportafdeling samen met onze registrars de fakewebshops uit de lucht te halen. We presenteerden onze resultaten op verschillende conferenties, zoals het Jaarcongres ECP en het DHPA TechFest. Tot slot schreven we een onderzoeksartikel over DMAP, dat werd geaccepteerd en gepubliceerd in de IFIP/IEEE Network Traffic Measurement and Analysis Conference (TMA 2018).

### **Nieuwe internet-systemen**

In het vierde kwartaal startten we met een onderzoek naar nieuwe open inter-netwerken. Deze alternatieve internet-systemen zijn gebaseerd op andere technologieën dan het Internet Protocol (IP) van het huidige internet en verkeren in een experimenteel stadium.

---

## *Ons doel is Nederland (en Europa) op dit gebied voorop te laten lopen.*

---

Nieuwe internet-systemen zouden transparanter en veiliger kunnen zijn en beter gebruikmaken van de nieuwe technische mogelijkheden van bijvoorbeeld open en programmeerbare router-hardware. Ons doel is Nederland (en Europa) op dit gebied voorop te laten lopen door vroegtijdig op deze systemen aan te sluiten en eraan bij te dragen. Als eerste stap sloten we ons labnetwerk aan op het testbed van SCION. Ook verzamelden we community-feedback tijdens 3 workshops: op het partnerevent van registrar OpenProvider, het Jaarcongres ECP en bij ons eigen evenement SIDN Connect.

### **Een collectieve anti-DDoS-strategie**

Samen met de Universiteit Twente en SURFnet schreven we een voorstel voor een proactieve en collectieve anti-DDoS-strategie voor de Nederlandse vitale infrastructuur. Ons voorstel draaide om een 'DDoS clearinghouse', een systeem waarmee serviceproviders voortdurend en automatisch de karakteristieken van DDoS-aanvallen met elkaar delen in de vorm van zogenaamde 'DDoS fingerprints'. Hiermee kunnen zij hun infrastructuur proactief aanpassen. Mede door dit voorstel lanceerden zo'n 25 partijen een nieuw nationaal

initiatief om gezamenlijk de nieuwe anti-DDoS-strategie te realiseren. We brachten het concept van het DDoS-clearinghouse ook onder in het Europese onderzoeksproject CONCORDIA.

### **Stats.sidnlabs.nl verbeterd**

We verbeterden onze statistiekensite. We kunnen metingen uit onderzoeksprojecten nu makkelijker delen en op een aantrekkelijkere en begrijpelijker manier aanbieden.

## **Vooruitblik**

### **Nieuwe internet-systemen**

We gaan met onze partners (Universiteit Twente, Universiteit van Amsterdam, SURFnet en NLnet Labs) experimenteren met nieuwe soorten internet-systemen.

### **SPIN**

Samen met de TU Delft gaan we aan de slag met het onderzoeken en evalueren van SPIN-modules om automatisch verkeer van onveilige IoT-apparaten te herkennen.

### **DNS operations**

Samen met onder andere de University of Southern California gaan we een Internet Draft schrijven voor de IETF. Hierin zullen we uiteenzetten hoe DNS-operators op basis van metingen de weerbaarheid van hun DNS-infrastructuur kunnen verhogen.

### **Domeinnaamabuse**

We gaan nieuwe algoritmes ontwikkelen om misbruik van domeinnamen beter te detecteren. Hiermee kunnen onder meer DDoS-for-hire-services worden opgespoord.

### **DDoS clearinghouse**

We gaan met Nederlandse en Europese partners een pilot uitvoeren met een DDoS clearinghouse om automatisch en continu de karakteristieken van DDoS-aanvallen uit te wisselen.

### **Nieuwe onderzoeksagenda**

Begin 2019 publiceren we onze nieuwe onderzoeksagenda. We richten ons op 3 gebieden: core internet systems, evolutie van het internet en inter-domain trust infrastructuur. Dat laatste gebied is nieuw en is gerelateerd aan het vakgebied van Connectis. We starten daarmee in de tweede helft van 2019.



# Aiko Pras

Hoogleraar Internet Security, Universiteit Twente

“Op een universiteit kunnen we heel goed rekenen en modellen maken, maar de praktijk is altijd anders dan de theoretische werkelijkheid. Je kunt niet zonder feedback uit de operationele praktijk. Daarom is het voor een technische universiteit essentieel om samen te werken met bedrijven. En omdat wij ons richten op DNS security kunnen en willen we natuurlijk niet om SIDN heen. Daar komt bij dat het gewoon heel goed klikt met de mensen van SIDN Labs. We zitten inhoudelijk op één lijn en we kunnen snel schakelen.

Een ontzettend leuk project dat we nu samen met SIDN Labs oppakken is een onderzoek naar ‘future internets’. Dat is maatschappelijk van groot belang. Europa wordt steeds afhankelijker van China en de VS. De backbone van het internet is in hun handen. Je moet er niet aan denken dat we ooit de controle over ons internet kwijtraken. We onderzoeken nieuwe internet-structuren die Europa weer de controle geven. Dat doen we in Europees verband. Ik heb hoge verwachtingen van dit onderzoek. Dit kan een enorme impact hebben.”

*We zitten inhoudelijk op één lijn en we kunnen snel schakelen.*

# 06

# Kennis



# Kennis delen op elk niveau

**We beschikken over unieke kennis en expertise. Die delen we graag. Dat deden we in 2018 onder meer via een collegereeks aan de Universiteit Twente en cursussen voor onze registrars. Daarnaast voerden we verschillende onderzoeken uit.**

## Onderzoek digitale vaardigheden basisschoolleerlingen

Voor de toekomst van ons land en van het Nederlandse bedrijfsleven is het belangrijk dat meer mensen kiezen voor een carrière in ICT. Daarom sponsorden we de Codeweek (7 tot 22 oktober). Tijdens deze week werden er door het hele land activiteiten georganiseerd om kinderen kennis te laten maken met programmeren. We hielpen bij de totstandkoming van 'www.wat?', een boek dat kinderen leert hoe de wereld van het internet in elkaar zit. Tijdens de Week van de Mediawijsheid (17 - 24 november) konden kinderen een exemplaar van het boek winnen. En we steunden het RTL4-programma 'Later als ik groot ben'.

Elke aflevering draait om een kind en zijn of haar droomberoep. Bij elk droomberoep laten de programmamakers zien hoe belangrijk ICT is. Het maakt niet uit welk beroep je kiest, digitale vaardigheden zijn belangrijk voor alle beroepen.

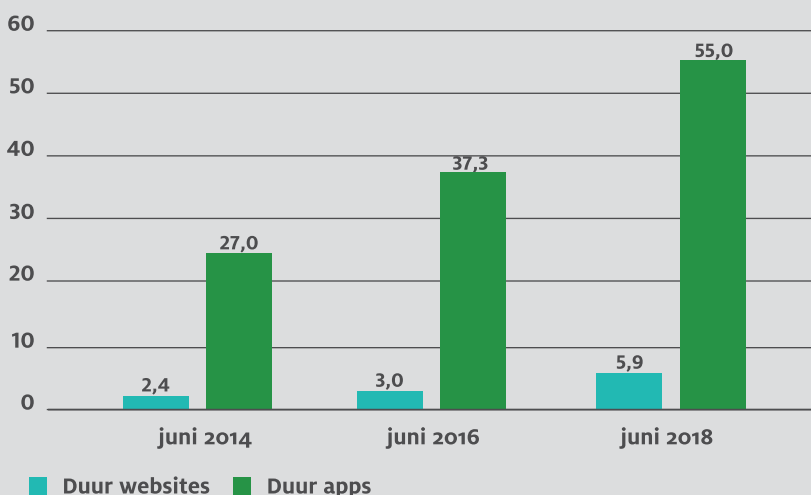
## Trends in internetgebruik

Onze belangrijkste activiteit is het beheer van de .nl-zone. De manier waarop Nederlanders het internet gebruiken en omgaan met domeinnamen, is van grote invloed op ons werk. Daarom doen we regelmatig onderzoek naar de trends in internetgebruik. In 2018 deden we dat voor de vijfde keer. Enkele opvallende conclusies:

- De smartphone wordt steeds serieuzer gebruikt. Steeds meer zaken die mensen eerst alleen op een pc deden, zoals het boeken van een hotel, doen ze tegenwoordig mobiel.
- Gebruikers brengen meer tijd online door. Daarbij valt op dat de bezoeken aan websites korter worden en de tijd die men aan een app besteedt langer.
- Apps zijn de drijvende kracht achter zakelijk succes in het mobiele internettijdperk. Mensen plaatsen echter slechts een beperkt aantal apps op hun telefoon. De concurrentie is moordend.
- Een sterk online merk wordt steeds belangrijker. Daarom stappen veel bedrijven over van meerdere productsites naar 1 corporate brand.
- Steeds meer internetgebruikers gebruiken een domein om in Google te beoordelen of een onbekende website te vertrouwen is. In Nederland wordt een .nl-domein als het betrouwbaarst gezien.

24

Fig. 6 | Totale tijd online op smartphone in uren







### **SIDN Academy**

We startten met de SIDN Academy, een initiatief om onze kennis te delen met onze registrars via cursussen en workshops. De eerste activiteit was een cursus over de toepassing van internetstandaarden voor veilige e-mail. Vanwege de grote populariteit is deze later in het jaar herhaald. Op deze manier willen we de kennis over internetstandaarden vergroten en de adoptie ervan stimuleren.

---

## *In Nederland wordt een .nl-domein als het betrouwbaarst gezien.*

---

### **Colleges door SIDN Labs**

Naar aanleiding van SPIN gaven we het vak 'Security Services for the IoT' (SSI) op de Universiteit Twente voor studenten die de Master Cybersecurity volgen. Zij beoordeelden het vak met een 8.

### **Onderzoek naar DDoS-aanvallen**

Samen met de Stichting Nationale Beheersorganisatie Internet Providers (NBIP) deden we onderzoek naar DDoS-aanvallen in Nederland. We analyseerden aanvallen op meer dan 60.000 sites over een periode van 12 maanden. De studie geeft inzicht in de achtergrond van DDoS-aanvallen, maar maakt ook een inschatting van de schade die deze aanvallen kunnen veroorzaken.

## **Vooruitblik**

### **SIDN Academy**

In 2019 willen we met een nieuwe editie van de SIDN Academy de kennis over IPv6 bij onze registrars verhogen.

### **Vervolgonderzoek trends in internetgebruik**

We breiden ons jaarlijkse trendonderzoek uit met een onderzoek naar de trends in e-identity en online security. Door hier separate onderzoeken van te maken geven we de verschillende onderzoeksvelden de aandacht die ze verdienen.



26

# Kasper Schoonman

Managing Partner HostingU2 en bestuurslid Vereniging van Registrars

“SIDN Academy is als het ware een branchebrede investering in kennis, iets dat ik toejuich, en een mooie invulling van de doelstelling van de stichting. De cursus was goed georganiseerd en het eerste onderwerp, veilige e-mail-standaarden, was goed gekozen omdat deze standaarden tegelijk werden opgenomen in een nieuwe incentive in de Registrar Scorecard. Dat maakt het voor de registrars makkelijker om aan deze eis te voldoen.

We hebben nu één SIDN Academy gehad. Persoonlijk vind ik dat SIDN nu moet doorpakken en dit vaker moet doen. En dan liefst met een bredere set onderwerpen. Dit is ook de mening van de Vereniging van Registrars, waarvan ik een van de bestuursleden ben. In het verleden heeft de VvR regelmatig moeite gehad met activiteiten van SIDN, maar de SIDN Academy juichen we toe. De VvR was ook betrokken bij de totstandkoming van de Academy. We praten graag mee over een vervolg.”

*SIDN Academy is als het ware een branchebrede investering in kennis, iets dat ik toejuich, en een mooie invulling van de doelstelling van de stichting.*

# 07

## SIDN

# Midden in de (digitale) maatschappij

**We gingen steeds meer agile werken en wisten veel nieuwe medewerkers aan ons te binden. Zoals elk jaar speelden we een belangrijke rol in internationale fora.**

## **Aanbieder van essentiële diensten**

De Wet beveiliging netwerk- en informatiesystemen (Wbni) werd van kracht. De wet beoogt de digitale weerbaarheid van Nederland te vergroten en de gevolgen van cyberincidenten te beperken. De wet verplicht aanbieders van essentiële diensten (AED's) en digitale dienstverleners (DSP's) maatregelen te nemen om hun ICT te beveiligen tegen incidenten.

---

*Als registry voor het .nl-domein en verlener van DNS-diensten worden wij gezien als AED.*

---

Als registry voor het .nl-domein en verlener van DNS-diensten worden wij gezien als AED. Bij security-incidenten geeft ons dit een meldplicht bij het NCSC en het Agentschap Telecom.

## **AVG**

Op 25 mei werd de Algemene verordening gegevensbescherming (AVG) van toepassing. We zorgden er tijdig voor dat onze organisatie aan

alle wettelijke eisen voldeed. Hoewel we niet wettelijk verplicht zijn om een functionaris voor gegevensbescherming in te stellen, hebben we dat toch gedaan. We vinden dat we als registry aan de allerhoogste standaarden moeten voldoen. Dat was ook de reden om enkele jaren terug een privacyboard in te stellen toen we startten met het analyseren van ons DNS-verkeer.

## **Intern**

### **Personeelsbestand en verzuim**

We werkten in 2018 hard aan onze naamsbekendheid op de arbeidsmarkt. We breidden onze samenwerking met universiteiten en hogescholen uit en zetten nadrukkelijker in op afstudeerplekken en stages. Deze aanpak wierp zijn vruchten af. In 2018 hadden we maar liefst 24 vacatures, vooral in moeilijke vakgebieden als ICT. Aan het einde van het jaar waren 22 van deze vacatures vervuld. Het aantal medewerkers kwam hiermee op 104 (94,09 fte). 28,8% van onze collega's is vrouw en 70,2% man. Met 7,2 % was het verzuimpercentage dit jaar hoog. Voor een deel gaat het hier om niet-arbeidsgerelateerd verzuim.

### **Agile werken**

Agile werken vergroot onze wendbaarheid en verkort de 'time to market'. We hebben grote stappen gezet om deze manier van werken in de hele organisatie uit te rollen. Zo hebben we beslissingsbevoegdheden lager in de organisatie gelegd en werken we steeds meer met multidisciplinaire, zelfsturende teams. We hebben een aantal agile rollen toegevoegd aan ons functiehuis en werken steeds meer met agile methodieken als Scrum en Kanban.

## Ontwikkeling en opleiding

We willen medewerkers een inspirerende werkomgeving en voldoende ontwikkelingsmogelijkheden bieden. Daarom reserveren we 7% van de loonsom voor opleidingen. In 2018 werden veel Scrum-trainingen en opleidingen op het gebied van agile werken gevolgd

## Wij reserveren 7% van de loonsom voor opleidingen.

### Persoonlijk sponsorbudget medewerkers

We stimuleren medewerkers in hun ontwikkeling, investeren in een inspirerende werkomgeving, besteden veel aandacht aan een goede balans tussen werk en vrije tijd, en zorgen voor een breed en goed pakket arbeidsvoorwaarden. Onderdeel van dit pakket is een persoonlijk sponsorbudget dat medewerkers elk jaar aan een zelfgekozen goed doel kunnen besteden. Hier wordt actief gebruik van gemaakt.

### Ondernemingsraad

Net als ieder jaar hebben we de OR geïnformeerd over ons jaarplan en onze begroting voor 2018. In september vergaderde de OR met de raad van toezicht van SIDN. De OR ontving instemmingsaanvragen voor een klokkenluidersregeling, voor een waakdienstregeling voor de ICT-afdeling en voor een alternatieve regeling om het wegvallen van de ANW-compensatie van het ABP op te vangen. Daarnaast behandelde de OR een adviesaanvraag in het kader van een wijziging van de organisatiestructuur en was de raad betrokken bij de transitie naar een meer agile opererende organisatie.

### Connectis

In januari 2017 verwierven we een meerderheidsbelang van 65% in Connectis, één van de grootste leveranciers van veilige inlogoplossingen in Nederland. In 2018 zette Connectis grote stappen met haar productontwikkeling en realiseerde een omzetgroei van bijna 50%. Het bedrijf implementeerde een nieuwe commerciële strategie en versterkte de bedrijfsvoering. Daarnaast zetten we verder in op synergie met onze organisatie. Een voorbeeld hiervan is de private cloud die we sinds april aan Connectis leveren. Dankzij deze robuuste technische infrastructuur kan Connectis zich vooral richten op de applicaties die zij aanbiedt. In november startte Remco Coenen als ceo van Connectis. Tot die tijd fungeerde algemeen directeur

Roelof Meijer als interim ceo. Naast Remco Coenen werd Jeroen de Bruijn benoemd tot commercieel directeur van het bedrijf.

## Bijdragen aan organisaties en conferenties

We spelen een actieve rol in verschillende belangrijke internationale fora. Ook in 2018 namen we deel aan tal van nationale en internationale bijeenkomsten en waren we betrokken bij de organisatie van enkele daarvan.

### ICANN

Er waren ICANN-meetings in San Juan (10-15 maart), Panama City (25-28 juni) en Barcelona (20-25 oktober). Stakeholders uit de hele wereld kwamen hier bijeen om te werken aan de beleidsmatige aspecten van met name het domeinnaamsysteem. Samen met het ministerie van Economische Zaken en Klimaat organiseerden we voorafgaand aan twee ICANN-meetings een pre-ICANN-meeting voor de Nederlandse afvaardiging.

### IETF/IRTF

We bezochten de IETF-meetings in Londen (17-23 maart), Montreal (14-20 juli) en Bangkok (3-9 november). We leverden actieve bijdragen aan verschillende IETF/IRTF-werkgroepen in de vorm van presentaties en een Internet Draft.

### RIPE

We werken al vele jaren samen met RIPE. In 2018 namen we deel aan beide RIPE meetings, in Marseille (14-18 mei) en Amsterdam (15-19 oktober). SIDN Labs hield een lezing over ons onderzoek naar de impact van DDoS-aanvallen op het DNS.

### CENTR

We zijn actief lid van CENTR, de organisatie voor Europese ccTLD's. Onze security officer is voorzitter van CENTR's Security Workgroup en onze legal and policy manager is vicevoorzitter van de Legal and Regulatory Workgroup. CENTR organiseert diverse bijeenkomsten waar leden ervaringen uitwisselen en ontwikkelingen bespreken, waaronder ook een Registrar Day. Wij nodigen .nl-registrars uit deze met ons te bezoeken. Tijdens de CENTR Jamboree in Moskou op 1 juni organiseerden we verschillende succesvolle sessies, onder meer over IoT-security en het bestrijden van fakewebshops. Ook waren we gastheer voor de CENTR Marketing-workshop in februari en de R&D-workshop in november.

### Jaarcongres ECP

Zoals elk jaar ondersteunden we het Jaarcongres ECP. Tijdens het Jaarcongres op 16 november passeerden thema's als cloud computing, big data, blockchain,

privacy en cybersecurity de revue. Wij deelden onze kennis in een SIDN fonds-sessie en een SIDN Labs-sessie. Enkele projecten die SIDN fonds ondersteunt, hielden demonstraties.

### **One Conference 2018**

Bedrijven, overheden en wetenschappers uit de hele wereld wisselden hun kennis en ervaring over cybersecurity uit tijdens deze bijeenkomst op 2 en 3 oktober in Den Haag. Wij gaven meerdere presentaties, waaronder een over de bestrijding van DDoS-aanvallen, samen met NBIP.

### **Platform Internetveiligheid**

Het Platform Internetveiligheid is een samenwerkingsverband tussen de overheid en marktpartijen. Het platform wil de internetveiligheid verbeteren. Ook in 2018 namen we actief deel in dit platform, onder meer in de stuurgroep voor de site Internet.nl.

### **Werkgroep Notice and Take Down**

Deze werkgroep valt onder het Platform Internetveiligheid en beheert de in 2008 tot stand gekomen nationale Gedragscode Notice and Take Down. Onze legal & policy manager is voorzitter van deze werkgroep. Op verzoek van de Minister van Justitie en Veiligheid paste de werkgroep de Gedragscode eind 2018 aan om kinderpornografisch materiaal sneller van het internet te verwijderen.

### **RIOT Summit 2018**

RIOT is een operating system voor het internet-of-things. SIDN Labs hield een presentatie over SPIN op de Summit in Amsterdam op 13 en 14 september.

### **DHPA TechFest 2018**

De stichting DHPA vertegenwoordigt de Nederlandse cloud- en hosting providers. Tijdens het DHPA Techfest 2018, op 24 mei in Naarden, verzorgden we een presentatie over de detectie van fakewebshops.

### **ICT.Open 2018**

ICT.Open is een event voor ICT-onderzoek in Nederland. SIDN Labs hield een presentatie over SPIN op de 6e editie, op 19 maart in Amersfoort.

### **Innovatiecongres**

Op het Innovatiecongres van het ministerie van Justitie en Veiligheid, op 20 november in Rotterdam, hield SIDN Labs een presentatie over SPIN.

### **SIDN Connect**

Op 29 november organiseerden we voor de tweede keer SIDN Connect. Op deze dag ontmoetten relaties van SIDN, Connectis en SIDN fonds elkaar op de KNVB Campus in Zeist. Zij konden genieten van inspirerende sprekers en prikkelende sessies. De dag werd door bezoekers beoordeeld met een 8,1.

## **Samenwerking en sponsoring**

We werken samen met en/of dragen bij aan organisaties, projecten en campagnes die de digivaardigheid stimuleren, negatieve bijeffecten van internet bestrijden of bijdragen aan innovaties rondom internet.

### **Alert Online**

De jaarlijkse campagne Alert Online, een gezamenlijk initiatief van overheid, bedrijfsleven en wetenschap, geeft mensen meer kennis over online veiligheid. De campagne richt zich op iedereen die het internet gebruikt: van jong tot oud en van werkvloer tot boardroom.

### **Bendoo Box**

De Bendoo Box is een compleet onderwijspakket waarmee we kinderen willen interesseren om te leren programmeren. In 2018 kregen maar liefst 2700 scholen een gratis Bendoo box.

### **Bits of Freedom**

Bits of Freedom komt op voor vrijheid en privacy op internet. Deze grondrechten zijn onmisbaar voor ontplooiing, technologische innovatie en de rechtsstaat. Bits of Freedom strijdt voor een open internet voor iedereen, waar privécommunicatie privé blijft.

### **Codeweek**

Tijdens de jaarlijkse Codeweek maken leerlingen en docenten in het basis- en voortgezet onderwijs kennis met programmeren.

### **DINL**

De Stichting Digitale Infrastructuur Nederland wil dat ons land voorop blijft lopen als knooppunt voor digitale infrastructuur. DINL vertegenwoordigt de partijen die de faciliteiten voor de digitale economie leveren, zoals datacenters, hostingpartijen en isp's. Wij waren een van de oprichters.

### **ECP**

ECP is een neutraal platform voor de digitale samenleving, waarin bedrijfsleven, overheid en maatschappelijke organisaties samenwerken. Het doel van het platform is om de digitalisering van de Nederlandse samenleving met de betrokken partijen te faciliteren en in goede banen te leiden. We zijn partner van ECP en we sponsoren sinds jaren het Jaarcongres ECP. Ook nemen we deel in veel van hun activiteiten, zoals de website veiliginternetten.nl.

### **ISOC.nl**

Internet Society is een vereniging met 44.000 leden uit 170 landen. Het is de moederorganisatie achter internationale organisaties als de IETF, IAB en IRTF.



In Nederland heeft ISOC.nl zo'n 1.000 leden uit o.a. de internetsector, het bedrijfsleven en de overheid.

### **Expertisebureau Online Kindermisbruik**

Het Expertisebureau Online Kindermisbruik, voortgekomen uit het Meldpunt Kinderporno op het Internet, heeft als doelstelling het voorkomen en bestrijden van (online) seksueel kindermisbruik en seksuele uitbuiting van kinderen.

### **NLnet Labs**

NLnet Labs is een R&D-instituut met internationale allure. Wij zijn opdrachtgever en financieren het werk van NLnet Labs sinds 2012 voor een belangrijk deel. SIDN Labs werkt nauw met NLnet Labs samen. Cristian Hesselman, directeur van SIDN Labs, is voorzitter van het bestuur van NLnet Labs.

### **Summer School on Internet Governance**

De Summer School on Internet Governance organiseert een uitgebreid introductieprogramma over internet governance voor studenten, academici en mensen uit het bedrijfsleven of de overheid. Wij sponsoren de jaarlijkse European Summer School on Internet Governance.

### **Kinderen leren programmeren**

Samen met Connectis en de TU Delft bieden we

basisscholen in Rotterdam de mogelijkheid om hun leerlingen te leren programmeren. In 2018 maakten circa 100 scholen van dit aanbod gebruik. Maar liefst 2.500 kinderen kregen programmeerles.

## **SIDN fonds**

Na een uitgebreide evaluatie besloten we om het SIDN fonds de komende jaren te continueren. We richtten dit onafhankelijke fonds in 2014 op, met als doel de welvaart en het welzijn in Nederland te verhogen door de waarde van het internet voor Nederland te vergroten. Het SIDN fonds startte in het voorjaar van 2015, ondersteunde bijna 150 innovatieve projecten en behaalde indrukwekkende resultaten.

In 2018 hield het fonds zoals altijd 2 aanvraagrondes voor innovatieve internetprojecten. Aanvragen voor pioniersprojecten en wetenschappelijke onderzoeksprojecten konden alleen worden aangevraagd binnen het jaarthema 'Responsible AI'. Met dit thema wil het fonds artificial intelligence stimuleren die het maatschappelijk belang dient. Na een zorgvuldige weging door de raad van advies werden 39 pioniers- en potentialprojecten en 1 onderzoeksproject gehonoreerd. In november reikte het fonds, samen met Google, Brinkhof Advocaten en Greenhost, de Internet Scriptieprijs uit.

---

## **Enkele projecten van het SIDN fonds**

### **MySensorData**

Elke smartphone bevat sensoren die de hele dag gegevens meten. Met de MySensorData-app zie je welke data worden opgeslagen en kun je zelf bepalen welke data je wilt gebruiken. Via het bijbehorende platform kun je toepassingen kiezen die op een privacyvriendelijke manier je gegevens raadplegen. Dit idee won de SIDN fonds Pioniersprijs tijdens de Dag van de Domeinnaam 2018.

### **Morele Mario**

Hoe test je slimme algoritmes op veiligheid en controleerbaarheid? Dit project ontwikkelt een benchmark op basis van een SuperMario-omgeving. Een zelflerende Mario komt in verschillende levels veiligheidsproblemen tegen, aan de hand waarvan ontwikkelaars kunnen controleren of een algoritme wel moreel is.

### **Touch ID**

Inloggen met een wachtwoord vormt een veiligheidsrisico. Dit kan worden opgelost door in te loggen met Touch ID op je smartphone. Inloggen met biometrie gebeurt nu veelal via een derde partij. Dit project ontwikkelt een open source app die ervoor zorgt dat alles veilig gebeurt, zonder dat een derde partij kan meekijken of login-gegevens kan bewaren.

### **Project Tigrinya**

Niet iedere taal is gedigitaliseerd, omdat dat voor sommige talen commercieel niet aantrekkelijk is. Het Tigrinya, gesproken in Eritrea, is hier een voorbeeld van. Door de taal te digitaliseren met inzet van AI-algoritmes, is straks tekst-naar-tekst vertaling mogelijk, en in een later stadium ook real-time vertaling via handheld translators. Dit helpt hulpverleners en instanties als politie, ziekenhuizen en vluchtelingenorganisaties zonder tolk te communiceren met de grote groep Eritrese vluchtelingen in ons land.



## Vooruitblik

### **Automatisering**

In 2019 zetten we in op de verdere automatisering van onze IT-omgeving. We verwachten grote stappen te maken in het identity- en access-management van ons domeinnaamregistratiesysteem. We zijn hard op weg om een single sign-on te realiseren voor al onze systemen. In 2019 zullen we op dit gebied ook zoeken naar synergie met Connectis.

### **IDnext**

Op 25 en 26 september 2019 organiseren we samen met IDnext het tweedaagse IDnext-event over veilig internet, privacy, trust, digital identity en online security. Dit event is Europa's toonaangevende conferentie voor experts en sleutelspelers in de wereld van digitale identiteiten.

### **Jamboree in Nederland**

Op 27, 28 en 29 mei 2019 zijn we de host van de Centre Jamboree in Amsterdam.

### **EuroDIG in Den Haag**

Op 19 en 20 juni treden we, samen met het ministerie van Economische Zaken en Klimaat, de Gemeente Den Haag en ECP, op als local host voor EuroDIG, het jaarlijkse Europese Internet Governance Forum.





# Coen van Loon

Systeembeheerder en 100ste medewerker SIDN

“Ik was al een tijdje bij SIDN gedeta-cheerd. En dat beviel goed. Ik houd van COLO-techniek en dan ben je hier aan het juiste adres. SIDN heeft 3 datacenters en veel externe locaties. Het onderhoud daarvan is erg leuk om te doen. Dus heb ik de stoute schoenen aangetrokken en gevraagd of ik niet bij SIDN in dienst kon komen.

Mijn eerste dag als SIDN-medewerker was op 1 mei. De dag daarvoor kreeg ik bericht dat ik niet voor 8.30 uur op kantoor mocht komen. Toen voelde ik al nattigheid. De volgende dag bleek het hele pand versierd te zijn. Alle collega's stonden klaar om me welkom te heten. Er was taart, er werd gezongen, ik liep over een rode loper het pand in, en directeur Roelof Meijer kwam me persoonlijk feliciteren. Wat bleek? Ik was de 100ste medewerker van SIDN!

Zo'n ludieke actie is kenmerkend voor SIDN. Collegialiteit staat hier voorop. Iedereen staat klaar om je te helpen en mensen zijn altijd bereid om even te sparren en met je mee te denken. Het bedrijf is klein genoeg om iedereen te kennen en groot genoeg om leuke, uitdagende projecten te kunnen doen. En er is veel ruimte voor ontwikkeling. Ik ben echt in een topomgeving terechtgekomen!”

*Zo'n ludieke actie is kenmerkend voor SIDN. Collegialiteit staat hier voorop.*

# 08

## Verslag raad van toezicht



# Verbreiding van activiteiten voor meer impact en borging continuïteit

De raad van toezicht houdt toezicht op de bestuurder van SIDN en de algemene gang van zaken betreffende SIDN en staat de bestuurder met raad terzijde. De raad ziet ondermeer toe op de bedrijfsstrategie, de daaruit voortvloeiende ondernemingsrisico's, het behalen van doelstellingen, en op de inrichting en effectiviteit van de interne risicobeheersings- en controlesystemen. In 2018 heeft de raad een externe zelfevaluatie gedaan en de verbeterpunten die hieruit voortkwamen zijn opgepakt.

## Bijeenkomsten

In 2018 kwam de raad van toezicht 5 keer bijeen en voerde daarnaast eenmaal overleg met de Vereniging van Registrars. Tussentijds was er met regelmaat contact met de bestuurder van SIDN. Vooral de ontwikkeling van Connectis en wijzigingen in de organisatie hadden aandacht nodig. Daarnaast kwamen de verschillende commissies meerdere keren bijeen.

- Auditcommissie: 2 bijeenkomsten
- Selectie- en benoemingscommissie: 1 bijeenkomst
- Security- en stabilitycommissie: 1 bijeenkomst

De volgende zaken werden goedgekeurd en/of vastgesteld:

- Jaarrekening en jaarverslag 2017 SIDN
- Jaarverslagen van de raad van toezicht, de selectie- en benoemingscommissie, de auditcommissie en de security- en stabilitycommissie in het kader van corporate governance
- Jaarplan en begroting 2018 SIDN

Daarnaast heeft de raad van toezicht de bestuurder van SIDN goedkeuring verleend om SIDN Deelnemingen B.V. in te laten stemmen met de volgende besluiten in de aandeelhoudersvergadering van Connectis Holding B.V.:

- Jaarplan en begroting 2018
- Jaarrekening 2016
- Jaarrekening 2017
- Jaarplan en begroting 2019



## Samenstelling

De raad van toezicht bestaat uit 7 leden. In 2018 waren er geen wijzigingen in de samenstelling.

Paul Schnabel, voorzitter, selectie- en benoemingscommissie, remuneratiecommissie.

Mark Frequin, selectie- en benoemingscommissie, remuneratiecommissie

Simon Hania, security- en stabilitycommissie

Kees Neggers, security en stabilitycommissie

Jeannine Peek

Peter van Schelven, auditcommissie

Willem van Waveren, auditcommissie

## Conclusie

De raad van toezicht is van mening dat het gevoerde beleid ervoor heeft gezorgd dat de kwaliteit van SIDN's dienstverlening is geborgd en dat SIDN goed voorbereid is op de nabije toekomst.

Het .nl-domein is stabiel en de kwaliteit van SIDN's infrastructuur is hoog. De tevredenheid van de registrars neemt verder toe. Met SIDN fonds, SIDN labs, maatschappelijke investeringen, Connectis en andere diversificatie initiatieven vergroot SIDN haar impact.

Financieel is de organisatie gezond. De afhankelijkheid van het .nl-domein vormt een risico voor de continuïteit op langere termijn. Verbreding van de activiteiten is dan ook van groot belang.

In het geval dat de vraag naar domeinnamen afneemt, is het belangrijk dat de uitgebreide en unieke expertise die SIDN bezit behouden blijft en nog steeds ingezet kan worden op een manier die relevant is voor de (lokale) internetgemeenschap. Bij alles wat SIDN doet, streeft het bedrijf steeds naar maximalisatie van de toegevoegde waarde voor Nederland.

Paul Schnabel,  
voorzitter raad van toezicht

# 09

# Financieel verslag

37



## Financieel

In 2017 hebben we, via onze dochteronderneming SIDN Deelnemingen B.V., een meerderheidsbelang van 65% verworven in Connectis Group B.V., gevestigd te Rotterdam. In de jaarrekening 2018 is het meerderheidsbelang verwerkt als deelneming; het behaalde resultaat over 2018 van Connectis Group B.V. is opgenomen als resultaat deelnemingen.

Het resultaat na belastingen over 2018 kwam uit op een verlies van € 4,0 miljoen, met name door het negatieve bedrijfsresultaat van € 3,5 miljoen. Een negatief bedrijfsresultaat was voorzien in de plannen en begroting voor 2018. Het gerealiseerde resultaat is grotendeels het gevolg van bewust beleid gericht op het effectief inzetten van een deel van de opgebouwde reserves, namelijk de financiering van SIDN fonds en het verhogen van onze uitgaven aan onder meer registrarprojecten en de incentiveregeling voor registrars (Registrar Scorecard). Daarnaast is ook rekening gehouden met een stijging in de personeelskosten in 2018. De helft van deze stijging wordt verklaard door tijdelijke inhuur op vacatures en voor ziektevervangings.

Gecorrigeerd voor de geldverstrekking aan SIDN fonds zou het bedrijfsresultaat over 2018 € 0,8 miljoen negatief zijn (2017: € 1,6 miljoen positief). Het bedrijfsresultaat als percentage van de omzet is uitgekomen op 18% negatief (2017: 0,1% negatief).

**38** Het aandeel in het nettoresultaat over 2018 van Connectis Group B.V. bedraagt € 0,2 miljoen. Connectis realiseerde haar targets en begroting voor 2018, daarnaast werd fors geïnvesteerd in groeipotentie.

De netto omzet in 2018 van € 19,5 miljoen is € 0,2 miljoen (-1%) lager dan voorgaand jaar (2017: € 19,7 miljoen). Dit komt met name door de hogere incentives aan registrars over 2018.

De personeelskosten stegen met € 1,1 miljoen ten opzichte van 2017 en bedragen € 9,9 miljoen (2017: € 8,8 miljoen). De stijging is deels het gevolg van de groei in formatie, de reguliere salarisverhoging (tezamen € 0,5 miljoen) en gestegen pensioenlasten (€ 0,1 miljoen). De formatiegroei bestaat uit de uitbreiding van de onderzoekscapaciteit van SIDN Labs en het oprichten van een Security Operations Centre. De kosten van tijdelijk personeel stegen met € 0,5 miljoen, met name als gevolg van het niet tijdig kunnen vervullen van openstaande vacatures.

De afschrijvingskosten over 2018 van € 2,5 miljoen zijn € 0,5 miljoen hoger dan 2017. De overige bedrijfskosten bedragen € 10,5 miljoen over 2018 (2017: € 8,9 miljoen). Dit is een toename van € 1,6 miljoen ten opzichte van 2017 en is vooral het resultaat van de geldverstrekking aan SIDN fonds.

We genereerden een negatieve kasstroom van € 1,9 miljoen in 2018 (2017: € 10,3 miljoen negatief). In 2017 was dit voornamelijk het gevolg van de verwerving van het meerderheidsbelang in Connectis Group B.V. (€ 8,6 miljoen). In 2018 is de negatieve kasstroom deels het gevolg van een afboeking van de belastinglatentie.

Ultimo 2018 bedraagt het eigen vermogen € 28,1 miljoen en onze financiële positie is daarmee nog steeds sterk gebleven. Een deel van het eigen vermogen dient als buffer om de continuïteit van de dienstverlening te waarborgen. De ondergrens van deze buffer is gerelateerd aan het structureel kostenniveau van de organisatie. De structurele kosten nemen in de loop der jaren toe door de toegenomen bedrijfsactiviteiten en de hogere kwaliteits-, stabiliteits- en veiligheidseisen. De omvang van de financiële buffer is op dit moment voldoende om de geïnventariseerde risico's en onzekerheden zo nodig en in redelijkheid op te kunnen vangen.

Om liquiditeitsrisico te beperken kochten we in 2017 Nederlandse en Duitse staatsobligaties aan voor € 1,5 miljoen, dit is nagenoeg gelijk aan de huidige waarde. Onze solvabiliteit daalde licht van 76,8% in 2017 naar 73,1% in 2018. In 2018 is € 5,2 miljoen (2017: € 4,9 miljoen) gefactureerd en ontvangen voor dienstverlening die in het kalenderjaar 2019 wordt verricht.

In 2013 zijn we gesprekken gestart over de fiscale behandeling van de geldverstrekking aan SIDN fonds. Wij verschilden met de Belastingdienst van mening over de mate waarin de geldverstrekking fiscaal aftrekbaar is. Bij het bepalen van de aanslag vennootschapsbelasting over 2014 week de Belastingdienst af van onze aangifte. Hiertegen hebben wij bezwaar ingediend. In 2018 heeft er een schikking met de Belastingdienst plaatsgevonden over de feitelijke aftrekbaarheid van kosten vanaf 2013. Dit leidt tot een totaal correctie op de vennootschapsbelasting over voorgaande jaren van per saldo € 0,7 miljoen.

We telden ruim 5,831 miljoen .nl-domeinnamen aan het eind van 2018. De netto domeinnaamgroei in 2018 was met 37.200 lager dan de 109.706 domeinnamen in 2017. Om het beveiligen van domeinnamen met DNSSEC te stimuleren, geven wij sinds juli 2012 een korting per beveiligde domeinnaam per jaar. Eind 2018 zijn zo'n 3,3 miljoen domeinnamen beveiligd met DNSSEC (57% van het totaal aantal domeinnamen). In 2015 startten we een incentive-programma om de kwaliteit van de .nl-zone te verhogen: de Registrar Scorecard. In 2018 keerden we € 1,6 miljoen uit (2017: € 1,3 miljoen) aan de deelnemende registrars. Het totale bedrag van verstrekte kortingen (DNSSEC-korting, Registrar Scorecard, staffelkorting en betalingskorting) in de netto omzet komt uit op € 3,5 miljoen (2017: € 3,2 miljoen). Dit is een stijging van ruim 9% ten opzichte van 2017. Het aantal registrars daalde verder naar 1.258 registrars ultimo 2018 (2017: 1.303).



## Vooruitblik

We verwachten in 2019 een lichte groei van het aantal .nl-domeinnamen en daarmee ook een lichte groei van de omzet uit .nl-abonnementen. Ook verwachten we een lichte stijging van de totale omzet. We voorzien een groei in de formatie en een daarmee samenhangende stijging in de totale kosten. De investeringen liggen naar verwachting op hetzelfde niveau als in 2018 en we verwachten dat het resultaat uit deelnemingen ook in 2019 nihil is. Over het geheel genomen verwachten we een minder negatief bedrijfsresultaat te behalen.

## Risico's en onzekerheden

### Visie en beleid

We werken ons strategisch plan voor de komende 4 jaar jaarlijks bij. Hierbij besteden we ook aandacht aan de (strategische) risico's. Het managementteam en staf maken een omgevingsanalyse; kansen en bedreigingen worden in kaart gebracht. Ook identificeren we sterkten en zwakten van de interne organisatie. Deze analyse vertalen we naar risico's en (eventuele) beheersmaatregelen. De continuïteit van de organisatie, het behoud van de rol van registry van het .nl domein en het beschermen van onze positie en reputatie zijn de speerpunten in de risicobeheersing.

39 Sinds 2011 zijn we ISO27001-gecertificeerd. In het kader van het Information Security Management System (ISMS) voeren we, in een jaarlijkse cyclus en volgens het vastgestelde informatie-beveiligingsbeleid, business impact analyses uit, 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 security overleg (TSO) en voeren eventuele verbeterpunten uit. De opvolging bewaken we aan de hand van halfjaarlijkse management reviews. Hierbij bespreken we onder andere de resultaten van de audits en performance-metingen en de status van audit-actiepunten en eventueel opgetreden securityincidenten.

Voordat we met een project starten, schrijven we een projectplan. Een vast onderdeel is de risicoparagraaf. Risico's van het project worden geïdentificeerd, maatregelen geïnventariseerd en restrisico's beoordeeld. Voordat een project groen licht krijgt, bespreken we de risicoparagraaf, als onderdeel van het projectplan. Tijdens de reguliere projectvoortgangsrapportage komen eventuele wijzigingen in de risico's en beheersmaatregelen aan bod.

Onze raad van toezicht houdt toezicht op de strategie, het beleid en de algemene gang van zaken binnen SIDN. Risicobeheersing krijgt hierbij expliciet aandacht. De raad van toezicht heeft daartoe onder andere een auditcommissie en een security & stability-commissie binnen haar geleding.

### Risico's ten aanzien van de strategie

De belangrijkste risico's ten aanzien van de strategie zijn de sterke afhankelijkheid van (omzet uit) het .nl domein en het krimpen van de .nl-markt. We hebben geen direct verkoopkanaal naar de eindmarkt en kunnen deze nauwelijks rechtstreeks

beïnvloeden. We zetten daarom in op samenwerking met onze registrars, bijvoorbeeld in de vorm van de Registrar Scorecard. Met incentives stimuleren we het gebruik van .nl-domeinnamen. Daarnaast kijken we naar mogelijkheden om onze toegevoegde waarde te vergroten, de dienstverlening te verbreden en de afhankelijkheid van .nl te verkleinen. Met het oog daarop hebben we begin 2017 65% van de aandelen verworven in Connectis Group B.V. Om de risico's te scheiden tussen SIDN en Connectis Group B.V. richtten we eind 2016 een dochteronderneming SIDN Deelnemingen B.V. op. Deze dochter houdt 65% van de aandelen in Connectis Group B.V. Connectis Group B.V. bevindt zich in een overgangsfase van start-up naar scale-up. Het is een jong, dynamisch bedrijf met een sterke positie en veel kansen in een groeiende en competitieve markt. In 2018 is net als in 2017 blijvend geïnvesteerd om de (om)slag goed te maken, waaronder in investeringen in verdere professionalisering, het doorvoeren van aanpassingen in de commerciële strategie en het creëren van synergie en meerwaarde. Onze risicobereidheid ten aanzien van strategische risico's is gemiddeld als het gaat om het vergroten van onze toegevoegde waarde.

### Risico's ten aanzien van operationele activiteiten

De 2 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, veroorzaakt door technisch en/of menselijk falen of – al dan niet doelgerichte – menselijke opzet. Dergelijke calamiteiten, wanneer grootschalig en langdurig, kunnen de continuïteit van de organisatie op 2 manieren in gevaar brengen. Enerzijds door ernstige reputatieschade en maatschappelijke en politieke discussie over de legitimiteit van SIDN als registry van het .nl domein. En anderzijds door omvangrijke claims voor vergoeding van schade geleden door onze klanten.

Het belang van sleutelprocessen voor de dienstverlening wordt met Business Impact Analyses, onderdeel van het ISMS, vastgesteld. Onze DNS-diensten, de basis voor het daadwerkelijk doen functioneren van bestaande domeinnamen, zijn daarbij het meest kritisch. Deze worden direct gevolgd door registratie-diensten voor het registreren van nieuwe en het muteren en opheffen van bestaande domeinnamen. Naast DNS en het domeinnaamregistratiesysteem zijn Whois/Is, de energievoorziening, kantoorautomatisering, onze website www.sidn.nl, communicatie en telecommunicatie als kritisch gewaardeerd. Om de beschikbaarheid, integriteit en vertrouwelijkheid te waarborgen hebben we een breed scala aan beheersmaatregelen getroffen. Deze zijn gericht op het verkleinen van de kans op calamiteiten, het mogelijk maken van spoedig herstel en het beperken van de gevolgen van deze calamiteiten. Deze maatregelen variëren van o.a. het elimineren van single points of failure door ver doorgevoerde redundantie in hardware, software, verbindingen, afgenomen diensten en expertise, logische en fysieke toegangsbescherming, audits en penetratietesten, tot eisen aan onze leveranciers, huisregels voor SIDN'ers, inrichting van een uitwijklocatie, uitvoer van



crisis- en uitwijkoefeningen en inrichting van een privacyboard en een Security Operations Centre (SOC).

Onze risicobereidheid 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. Als het gaat om het verbeteren van operational excellence is onze risicobereidheid gemiddeld.

#### **Risico's ten aanzien van de financiële positie**

- Schadeclaims en boetes: onderbrekingen in de dienstverlening en verlies van vertrouwelijkheid of integriteit van data kunnen leiden tot claims en/of boetes. Onze algemene voorwaarden beperken een dergelijke aansprakelijkheid c.q. sluiten deze uit.
- Koersrisico/valutarisico: het koers- en valutarisico is beperkt. De prijzen voor onze .nl-dienstverlening luiden in euro's. We kopen maar weinig in bij leveranciers die andere valuta dan de euro hanteren.
- Debiteurenrisico: ca. 75% van de registrars betaalt via automatische incasso. In onze algemene voorwaarden zijn vervolgstappen gedefinieerd, als een registrar niet aan zijn financiële verplichtingen voldoet.
- Liquiditeitsrisico: we hebben onze liquide middelen verspreid over 3 Nederlandse banken. In 2017 kochten we Nederlandse en Duitse staatobligaties aan.
- Marktrisico: de Nederlandse en Duitse staatobligaties hebben we aangekocht met als doel om deze tot het einde van de looptijd aan te houden. Mochten we genoodzaakt zijn om de staatsobligaties eerder te verkopen, dan lopen we het risico dat de waarde van de staatsobligaties is gedaald ten opzichte van het moment van aankopen.
- Solvabiliteitsrisico: wij houden een financiële buffer aan om de continuïteit van de organisatie (voorlopig) te waarborgen wanneer een aanzienlijk deel van onze inkomsten wegvalt of we in een korte tijdspanne zeer hoge uitgaven moeten doen. De ondergrens van deze buffer groeit mee met onze structurele kosten. De huidige omvang van de financiële buffer is ruim boven de vastgestelde ondergrens.
- Onzekerheid in de mogelijkheid om financiering aan te trekken: tot op heden is het niet nodig gebleken om externe financiering aan te trekken.

Onze risicobereidheid ten aanzien van financiële risico's is 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, variërend van wijzigingen in arbeids- en belastingwetgeving tot informatiebeveiliging. Gevolgen brengen we in kaarten vertalen we naar de organisatie en voeren we in. Vanwege het belang van wijzigingen in wet- en regelgeving die onze rol als registry raken, hebben wij hier een legal & policy manager mee belast. Waar nodig en mogelijk oefent hij inhoudelijk invloed uit.

We zijn een uitgebreide inventarisatie gestart om onze persoonsverwerkingen te registreren in het kader van de inwerkingtreding van de Algemene Verordening Gegevensbescherming. We kijken daarbij kritisch of de verwerkingen binnen de grenzen van de wet vallen. Zo nodig passen wij onze werkwijzen aan. Wij hebben vrijwillig een functionaris gegevensbescherming aangesteld.

Onze risicobereidheid ten aanzien van risico's op het gebied van wet- en regelgeving is laag; we willen ruim voldoen aan wet- en regelgeving.





## Geconsolideerde jaarrekening over 2018

Geconsolideerde balans per 31 december 2018 (na resultaatbestemming)

### Vaste activa

#### Immateriële vaste activa

31 december 2018 (in €)

6.992.515

31 december 2017 (in €)

8.393.948

#### Materiële vaste activa

Bedrijfsgebouwen en -terreinen

5.147.068

5.326.488

Machines en installaties

836.742

1.107.138

Andere vaste bedrijfsmiddelen

608.821

789.711

Materiële vaste activa in uitvoering

29.174

0

6.621.805

7.223.337

#### Financiële vaste activa

3.690.854

4.135.007

41

### Vlottende activa

#### Vorderingen

Debiteuren

396.459

303.489

Belastingen en premies sociale verzekeringen

1.208.846

363.548

Overige vorderingen en overlopende activa

1.211.978

1.088.038

2.817.283

1.755.075

#### Liquide middelen

18.384.811

20.326.724

35.507.268

41.834.091

**Groepsvermogen****Langlopende schulden**

Overige schulden

**Kortlopende schulden**

Crediteuren

Belastingen en premies sociale verzekeringen

Overige schulden en overlopende passiva

**31 december 2018 (in €)**

28.149.021

406.250

1.104.879

420.679

8.426.439

---

9.951.997

---

**38.507.268****31 december 2017 (in €)**

32.131.840

406.250

1.113.426

365.941

7.816.634

---

9.296.001

---

**41.834.091**



## Geconsolideerde winst- en verliesrekening over 2018

	2018 (in €)	2017 (in €)
<b>Netto-omzet</b>	19.481.759	19.704.620
<b>Kosten</b>		
Lonen en salarissen	7.345.103	6.351.074
Sociale lasten	709.964	691.554
Pensioenlasten	978.649	858.979
Overige personeelskosten	916.093	892.793
Afschrijvingen	2.518.557	2.000.516
Overige bedrijfskosten	10.518.465	8.929.193
	<u>22.986.831</u>	<u>19.723.927</u>
<b>43 Bedrijfsresultaat</b>	-3.505.072	-19.307
Financiële baten en lasten	48.067	21.950
<b>Resultaat vóór belastingen</b>	<u>-3.457.005</u>	<u>2.643</u>
Belastingen	-726.371	-478.772
	<u>-4.183.376</u>	<u>-476.129</u>
Resultaat deelnemingen	200.557	-169.079
<b>Resultaat na belastingen</b>	<u><b>-3.982.819</b></u>	<u><b>-645.208</b></u>



## Geconsolideerd kasstroomoverzicht over 2018

	2018 (in €)	2017 (in €)
<b>Kasstroom uit operationele activiteiten</b>		
Bedrijfsresultaat	-3.505.072	-19.306
Aanpassing voor afschrijvingen	2.518.557	2.000.513
<i>Veranderingen in werkkapitaal:</i>		
Mutatie vorderingen	-253.002	-96.250
Mutatie kortlopende schulden	665.339	876.965
Kasstroom uit bedrijfsoperaties	<u>-574.178</u>	<u>2.761.922</u>
Ontvangen interest	1.145	30.356
Vennootschapsbelasting	-587.155	-709.653
	<u>-586.010</u>	<u>-679.297</u>
<b>44</b> Kasstroom uit operationele activiteiten	<b>-1.160.188</b>	<b>2.082.625</b>
<b>Kasstroom uit investeringsactiviteiten</b>		
Investerings in immateriële vaste activa	-268.099	-8.424.855
Investerings in materiële vaste activa	-247.493	-775.767
Verwervingen deelneming	0	-243.956
Mutatie overige financiële vaste activa	-266.133	0
Verstrekke langlopende leningen	0	-1.487.260
Verwerving van effecten	0	-1.489.643
Kasstroom uit investeringsactiviteiten	<u>-781.725</u>	<u>-12.421.481</u>
<b>Toename/(afname) geldmiddelen</b>	<b><u>-1.941.913</u></b>	<b><u>-10.338.856</u></b>



## Geconsolideerd kasstroomoverzicht over 2018

	2018 (in €)	2017 (in €)
<b>Samenstelling geldmiddelen</b>		
Geldmiddelen per 1 januari	20.326.724	30.665.580
Mutatie liquidemiddelen	<u>-1.941.913</u>	<u>-10.338.856</u>
<b>Gemiddelden per 31 december</b>	<u>18.384.811</u>	<u>20.326.724</u>

# IO

## Personalia



Personalia zoals op 31 december 2018

### **Directeur/bestuurder**

Roelof Meijer

### **Managementteam**

Cristian Hesselman, SIDN Labs

Arjan Middelkoop, New business, Marketing & Sales

Lilian van Mierlo, Registratie & Service

Cees Toet, ICT

[vacature], financieel directeur

### **Ondernemingsraad**

Sebastiaan Assink (voorzitter)

47 Remko van den Berg

Barry Peters (vicevoorzitter)

Martin Sluijter (secretaris)

Ruben Wubbels

### **College voor Klachten en Beroep**

Peter Blok

Huib Gardeniers (secretaris)

Hendrik Struik

Judith de Vreese-Rood (voorzitter)

Thomas de Weerd

Dennis Wijnberg

### **Raad van toezicht**

Mark Frequin

Simon Hania

Kees Neggers

Jeannine Peek

Peter van Schelven

Paul Schnabel (voorzitter)

Willem van Waveren

# II

# Woordenlijst





### **Abuse**

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

### **Access provider**

Een (internet) access provider biedt faciliteiten om verbinding te maken met het Internet.

### **Agile**

Een manier van werken die het organisaties mogelijk maakt om wendbaarder en flexibeler te zijn. In een agile-organisatie worden projecten vaak opgedeeld in kleine, overzichtelijke perioden en is er continu afstemming met de klant. De agile-filosofie is afkomstig uit de ICT-wereld en kent veel verschillende methoden, waarvan scrum een van de bekendste is.

### **Anycast**

Globale anycast is een bewezen en effectieve technologie die de netwerkbelasting 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.

### **Algemene Verordening Gegevensbescherming (AVG)**

Per 25 mei 2018 geldt in de hele EU dezelfde privacywetgeving. In het Engels heet de AVG General Data Protection Regulation (GDPR).

### **Big data**

Het analyseren van grote hoeveelheden digitale data, vaak uit verschillende bronnen.

### **Blockchain**

De techniek achter veel cryptomunten, zoals Bitcoin. De techniek is te vergelijken met een grootboek. Maar dan een grootboek dat niet wordt bijgehouden door een centrale instantie, maar door alle gebruikers. Als één gebruiker een transactie doet, wordt dat direct bij alle gebruikers vastgelegd. De decentrale structuur maakt het onmogelijk om een blockchain te hacken.

### **Caching**

Het opslaan van data in tijdelijke bestanden. Door veel opgevraagde webpagina's op te slaan in een cache wordt voorkomen dat dezelfde informatie steeds opnieuw moet worden opgehaald.

### **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](http://centr.org).*

### **Cloud computing**

Het leveren van diensten als opslag, databases, netwerkfuncties, en software via het internet ('de cloud'). Bekende voorbeelden zijn streaming video en online gaming.

### **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](http://cvkb.nl).*

### **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.

### **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.

### **Downtime**

De tijd dat een website niet bereikbaar of een applicatie niet actief is.

### **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 secondleveldomein, 'sidn'.

### **Domeinnaambewakingservice (DBS)**

Een monitoringservice van SIDN om onder meer typosquats op te sporen. DBS waarschuwt bedrijven als er een domeinnaam wordt geregistreerd die lijkt op hun bedrijfs- of merknaam.

### **Domeinnaamhouder**

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



### **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.

### **General Data Protection Regulation (GDPR)**

Per 25 mei 2018 geldt in de hele EU dezelfde privacywetgeving. In Nederland spreken we over de Algemene Verordening Gegevensbescherming (AVG).

### **ECP**

Binnen ECP, Platform voor de InformatieSamenleving, werken bedrijfsleven, overheid en maatschappelijke organisaties samen om het gebruik van ICT in de Nederlandse samenleving te versterken.  
*Zie ook [ecp.nl](#).*

### **E-facturatie**

Het digitaal versturen van facturen.

### **eID**

Een elektronisch identiteitsbewijs waarmee je veilig en betrouwbaar toegang kunt krijgen tot online dienstverlening van overheden en bedrijven.

### **ENTRADA**

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

### **Fake webshop**

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

### **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.

### **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](#).*

### **Identity- en access-management (IAM)**

De overkoepelende term voor alle processen in een organisatie die zich richten op het administreren en beheren van gebruikers in het netwerk. Hieronder valt bijvoorbeeld de toegangscontrole voor applicaties en systemen.

### **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 governance**

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

### **Internet Governance Forum**

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-of-things**

Ook wel het Internet der Dingen genoemd. Een ontwikkeling van het internet, waarbij alledaagse voorwerpen, zoals thermostaten en babyphones, zijn verbonden met het internet en gegevens kunnen uitwisselen.

### **ISP**

Een internet service provider (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.

### **IP-adres**

Een Internet Protocol-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.

### **ISOC (Internet Society)**

Een internationale organisatie voor wereldwijde samenwerking en coördinatie op het gebied van het internet en daaraan gerelateerde technologieën en toepassingen. De vereniging brengt in 180 landen zestienduizend internetprofessionals samen. Velen van hen stonden aan de basis van het internet.  
*Zie ook [internetsociety.org](#).*

### **Internet Society Nederland (ISOC.nl)**

Brengt zo'n 800 individuele leden samen uit onder meer de internetsector, het bedrijfsleven, de overheid, consumentenorganisaties, de non-profitsector, de techniek en het financiële, juridische en academische veld.  
*Zie ook [isoc.nl](#).*

### **Java**

Een programmeertaal die veel wordt gebruikt op internet.

### **Malware**

Een verzamelnaam voor kwaadaardige software, zoals computervirussen of wormen.



### **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.

### **New gTLD program**

Dit initiatief van ICANN is de grootste uitbreiding van het domeinnaamsysteem ooit. In 2013 werd het aantal generieke domeinnamen uitgebreid van 22 naar meer dan 1000.

### **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 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.

### **Open source**

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.

### **Realtime**

De werkelijke tijd die nodig is om iets uit te voeren. Realtime interactie vindt plaats zonder vertragingen of wachttijden als gevolg van gegevensverwerking.

### **Registrar**

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

### **Registry**

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

### **Resolving**

Antwoord geven op een DNS-vraag.

### **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.*

### **Server**

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

### **TLD**

Afkorting voor Top Level Domain. Dit is het meest rechtse deel van een domeinadres na de punt.

### **Topleveldomein**

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

### **Service provider**

Een internet service provider (ISP) biedt internetdiensten aan, zoals digitale televisie en internettelefonie. Ook leveren ISP's netwerkapparatuur 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).

### **Single sign-on**

Met single sign-on-software geeft je, na één keer inloggen, automatisch toegang tot meerdere applicaties of resources in een netwerk. Zo hoeft je niet elke keer opnieuw je wachtwoord in te vullen.

### **Spam**

Verzamelnaam voor ongewenste e-mailberichten.

### **SSL**

Een techniek waarmee de verbinding tussen de bezoeker van een website en de server waar de website is ondergebracht, met encryptie wordt beveiligd.

### **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.

**Unicast**

Een manier van data verzenden binnen computernetwerken. Bij unicast stuurt één bronapparaat data naar één enkele bestemming.

**Uptime**

De periode waarin een computersysteem of netwerk beschikbaar is.

**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.

**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 Whois-gegevens voor alle .nl-domeinnamen.  
*Zie [sidn.nl/whois](http://sidn.nl/whois).*

52

**WIPO Arbitration and Mediation Center**

Een onafhankelijke, internationale non-profit organisatie die zich bezighoudt met de arbitrage in onder meer conflicten rondom domeinnamen.  
*Zie ook [wipo.int](http://wipo.int).*

**Zonefile**

Een tekstbestand waarin domeinnamen en de bijbehorende ip-adressen van webservers staan.

# Colofon

## **Redactie**

SIDN, Arnhem

## **Tekst**

ARA, Rotterdam

## **Ontwerp & realisatie**

Lumen Ontwerpersnetwerk, Breda

## **53 Vertalingen**

G & J Barker Translations, Worcester, Verenigd Koninkrijk

## **Contact**

SIDN

Meander 501

6825 MD Arnhem

Postbus 5022

6802 EA Arnhem

T +31 (0)26 352 55 00

[communicatie@sidn.nl](mailto:communicatie@sidn.nl)

[www.sidn.nl](http://www.sidn.nl)

## **© SIDN**

Teksten en cijfers uit dit jaarverslag mag je overnemen, maar wij willen dan wel graag als bron vermeld worden. Ook worden wij graag vooraf geïnformeerd via [communicatie@sidn.nl](mailto:communicatie@sidn.nl).

## **Meld je aan voor onze nieuwsbrief**

[www.sidn.nl/nieuwsbrief](http://www.sidn.nl/nieuwsbrief)