2018 Annual Report

Your world. Our domain.

2018

Contents

01

Foreword

Vigorously pursuing our mission

In 2018, we continued to vigorously pursue our mission: connecting people and organisations to promote safe and convenient digital living. The theme that linked all our activities in 2018 was further increasing added value for the Netherlands: our impact on the nation's economy and society. We went about that in three main ways.
First, by reinforcing the position of the .nl domain through activities aimed at positioning, quality, security and innovation. Second, by developing and growing our subsidiary Connectis, realising synergy between the two organisations and developing promising new propositions in the fields of online security and digital identity. And, last but certainly not least, by investing in developments for the internet community. Investment took the form of support for SIDN Fund, research projects undertaken by SIDN Labs, input to international networks such as CENTR, ICANN, IETF and IGF, and involvement in a variety of activities and programmes concerned with digital security and skills in the Netherlands.

At the start of the year, we set ourselves the goal of increasing our impact. And I believe that we achieved that goal. Through our activities, we contribute to the success, quality and security of the internet in the Netherlands. Our contribution took various forms in 2018, which are described in this annual report. In the year ahead, I'm confident that we'll continue to increase our added value for the Netherlands and the wider internet community

Roelof Meijer,
CEO, SIDN

02

.nl

Stable year for the .nl domain

The .nl domain experienced a small amount of additional growth in 2018. Brand preference for the domain increased as well, thanks partly to a successful promotional campaign. Satisfaction amongst registrars and other client groups was higher than ever.

Development of the .nl domain

Following unexpectedly strong growth in 2017, the .nl domain recorded modest growth in 2018. There were 802,739 new registrations and 764,742 cancellations. Growth was strongest in the second half of the year. For the whole year, net growth was 37,997, or 0.66 per cent. We ended the year with 5,832,037 registered .nl domain names. Most new registrations were for business use. Business registrations' share of the total continues to increase.

Market share increases further

The .nl domain's share of the Dutch market rose slightly, to 64 per cent. With various other top-level domains contracting, the local market is increasingly divided between two big players: .nl and .com.

More use of IPv6

The number of IPv6 queries sent by resolvers nevertheless rose gradually during the year. Compared with some other countries, IPv6 adoption has been slow in the Netherlands, according to the IPv6 inventory we carried out in 2018. For example, only 13 per cent of all Dutch visits to Google pages are made from IPv6 addresses. That is mainly because the biggest Dutch access providers don't offer internet users a fully operational IPv6 connection. Reluctance to embrace IPv6 does not bode well for the Dutch internet's future-readiness. Nor, indeed, for the competitiveness of the country's business

Fig. 1 | Development of the .nl-domain

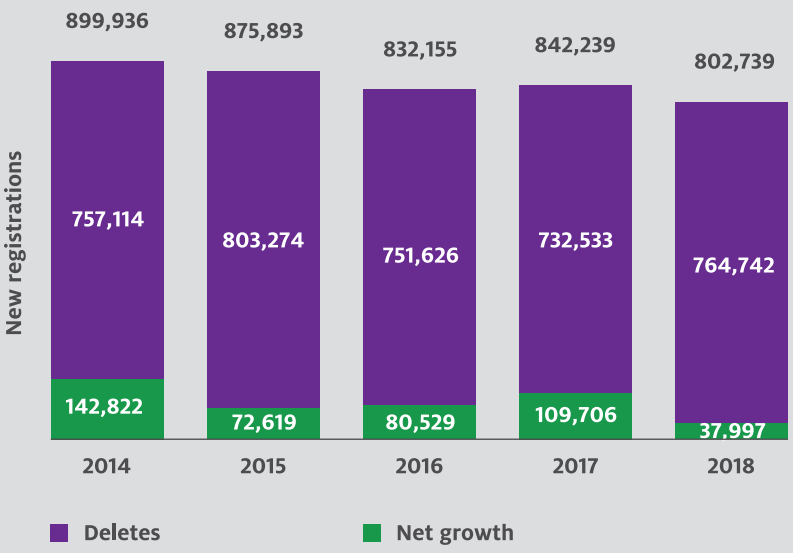
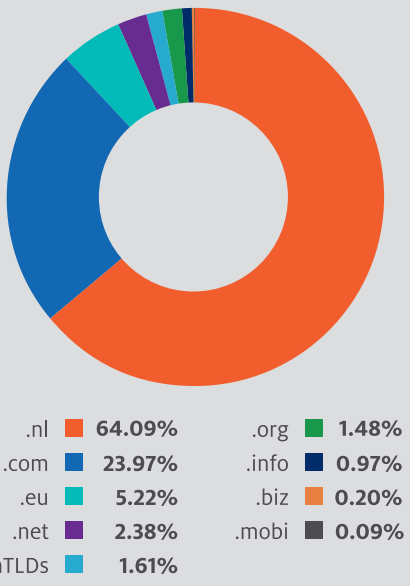


Fig. 2 | Share of Dutch market in 2018



community, since it makes the Netherlands less attractive as a place for innovation and investment in the Internet of Things (IoT).

Compared with some countries, adoption of IPv6 is going slowly in the Netherlands.

Availability high despite major outage

Our DNS systems, which form the bedrock of our services, were again 100 per cent available in 2018. Barely any of the maintenance undertaken on our registration system (DRS) involved perceptible service interruptions, and all the work that did require downtime was completed within the predefined windows. In late January, we were hit by a major outage caused by a fault in a supplier's firmware. Our registration system was unavailable for roughly six hours. In response, we made various improvements to our infrastructure, which should prevent similar issues occurring in the future.

Marketing activities

We work closely with our registrars on commercial matters. Back in 2017, for example, we cooperated on the sales funnel linked to the Whois utility on our website. The funnel directs people who are thinking of registering domain names to suitable registrars. And, if the first domain name they try for is taken, alternatives are suggested. In 2018, we continued refining the funnel, which now generates thousands of leads for our registrars.

A marketing campaign was organised, with the slogan "More click with .nl". The initiative helped increase the brand preference for .nl from 72 per cent to 79. Although the focus was the business community, particularly start-ups, the campaign also led to increased brand preference amongst consumers. The effect underlined the increasing difficulty of distinguishing between the business and retail sectors of the domain name market. Another joint SIDN-RA initiative was a marketing push at the Day of the Domain Name (7 June).

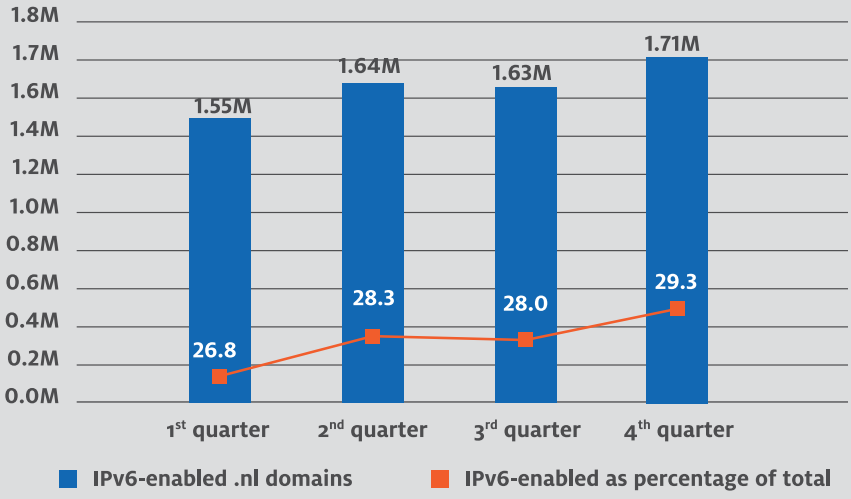
Dispute resolution system for .nl domain names

In 2018, sixty-nine cases were referred to the WIPO Arbitration and Mediation Center under the Dispute Resolution Regulations for .nl Domain Names. Thirty-seven of those cases were resolved by WIPO, and three are still under consideration. The other cases were closed, e.g. because the complaint was withdrawn, or because the two sides reached an amicable agreement. Our mediators handled twenty-two cases. In nine of them, successful mediation led to the dispute being settled early.

Changes to the Whois

We implemented a new Whois backend in preparation for the updated Whois protocol (RDAP), which ICANN is expected to introduce in 2019.

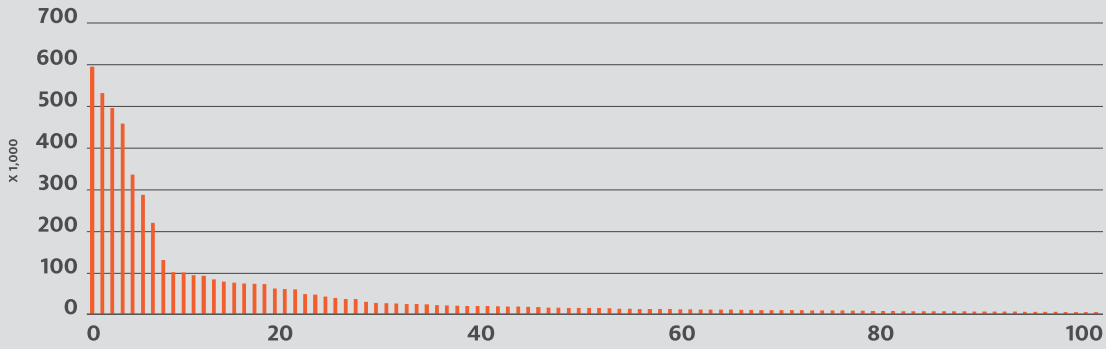
Fig. 3 | Growth in the number of IPv6-enabled domains in 2018



Developments in the registrar community

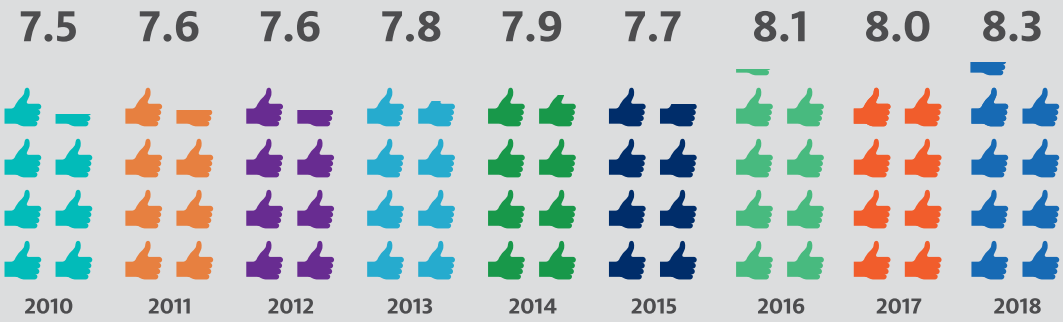
.nl domain names are marketed through a large and diverse community of registrars. For some time, that community has been contracting slightly year on year. The concentration trend continued in 2018, with the number of registrars falling from 1,303 to 1,237. Driving the process were a number of major takeovers and mergers, leading to the creation of several very large players.

Fig. 4 | Domain names per registrar



Registrar satisfaction

We run an annual survey of satisfaction amongst our registrars. In 2018, respondents gave our services the highest rating ever: 8.3 out of ten. Approval was highest for personal contact with our Support Department, and for the events we organised. Large registrars actually gave our support nine out of ten. Some registrars criticised the decision to place a stricter limit on the number of Registrar Whois enquiries permitted. However, we were obliged to impose the limit in order to comply with the GDPR.



Webinars

We ran a number of webinars, sharing our expertise with registrars on topics such as the implications of the GDPR for domain registration.

Cooperation with the Registrars' Association

Registrars form one of our primary stakeholder groups. In their relations with us, they are represented by the Registrars' Association (RA). We fund the RA and enjoy a constructive working relationship with the association. The RA continued to provide us with a steady flow of useful ideas, suggestions and advice.

In 2018, we teamed up with the RA to set up a Legal Help Desk for RA-affiliated registrars. So .nl registrars can now get swift, free answers to questions about privacy, terms and conditions and other issues involving ICT and the law. Collaboration with the RA additionally yielded a Privacy Portal: an online resource that supports registrars with GDPR compliance.

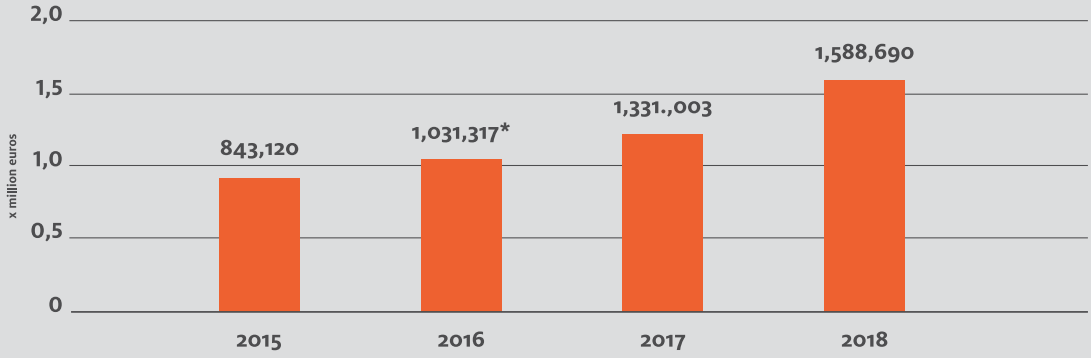
At the RA's request, we also enabled location-independent registration system access via a VPN. We involved the RA and our registrars in the development of new propositions as well. In consultation with the RA Board, we set up a registrar consultation group to discuss two new propositions: eHerkenning and on-line security for SMEs. The valuable feedback received will inform our further development of the two concepts. Finally, we used the SIDN Academy to share knowledge with registrars. The Academy is a new initiative, whose first offering was a free one-day course on e-mail standards.

In 2018, registrars gave our services the highest rating ever: 8.3 out of ten.

Registrar Scorecard

The Registrar Scorecard (RSC) incentivises registrars to invest in the value of the .nl domain. The scheme contributes to the quality of registration data and the active use of .nl, discourages cancellations and promotes investment in security, modern standards and abuse prevention. In 2018, incentive payments totalling € 1.5 million were made. The scheme now has 370 members.

Fig. 5 | Value of incentive payments made



*From 2016, the discount on DNSSEC-enabled domain names was converted into an RSC incentive.

Notice-and-take-down procedure

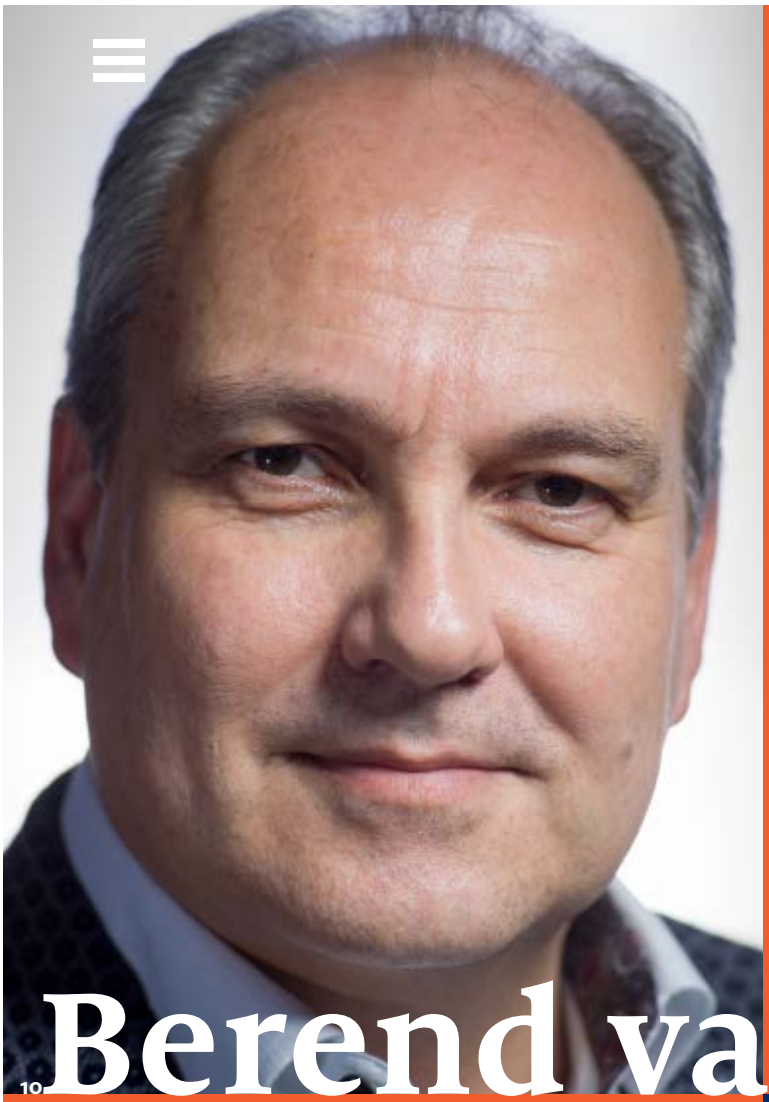
We have a notice-and-take-down procedure, setting out what has to be done if someone contacts us to complain that a website's content is clearly against the law. In the last resort, we can disable a domain name. We received thirty-five notice-and-take-down requests. Seven of those requests led to us disabling the domain name in question. In the other cases, either someone with more control over the offending content intervened or we decided that the content was not clearly criminal or unlawful.
At the end of 2018, in consultation with the On-line Child Abuse Expertise Bureau, an addition was made to the national Notice and Take Down Code, so that child pornography can be removed from the internet more easily.

Complaints and Appeals Board

A .nl registrar or registrant who is unhappy with a decision made by SIDN can appeal to the Complaints and Appeals Board for .nl Domain Names (C&AB) . The C&AB is an independent body that also considers complaints about domain name registrations that are believed to be inconsistent with public order or decency. In 2018, the C&AB received three appeals. However, none of the appeals was actually considered by the C&AB: in each case, either the appeal was withdrawn, or it was not pursued.

Outlook

In collaboration with our registrars, we intend to refine the funnel and suggestion tool on our website, so that it's easier for registrants to find the right domain name and registrar. Through the Registrar Scorecard, we'll also be continuing to invest in the adoption of open standards such as IPV6. In tandem with our registrars, we're going to run a number of data-led .nl marketing campaigns as well. Finally, with the aim of keeping the security of .nl at a very high level, we'll be using the DBS as a basis for helping people in the sector to intervene when domain names are abused.



Berend van Dalfzen

CEO of Realtime Register

"Every month, SIDN's website is visited by thousands of people who want to check whether a domain name they want is still available. However, SIDN doesn't sell domain names; that's the role of the registrars and their resellers. So SIDN has created a funnel on their website. Now, if you look up a domain name and it's available, you're shown the logos of various registrars. You click on a logo, and you're taken to the registrar's website, straight to a page where you can register the name. The logos that appear are selected at random, so that every registrar has the same chance of getting a visitor funnelled through to them.
For some registrars, the system can mean hundreds of new registrations a month. Although the income from those registrations might be modest, each one is the start of a new relationship. A relationship that might involve hosting or VPS services, for example. Services that are the registrant's bread and butter.

Alongside the sales funnel, SIDN has installed a suggestion tool on its website. If the domain name you want has already been taken, the tool suggests alternatives. It's a really useful system. So we've integrated it into our own ADAC suggestion tool, which we offer to resellers. Not all the suggestions made by SIDN's tool are good enough, though. That's partly because it's based on a retro tool: it uses domain names registered in the past as the source of its suggestions. We've given SIDN feedback on that issue, and they're now in the process of upgrading the tool. It's good to see SIDN listening to registrars and helping them out like this."

For some registrars, the system can mean hundreds of new registrations a month.

03 Solutions

Focus on security and identity

We entered into several new partnerships and sharpened the focus of our objectives. We're looking to develop new activities primarily in the growth domains of on-line security and digital identity.

IRMA

During the year, we joined forces with Privacy by Design, the foundation behind the identity platform IRMA. The platform's name is an acronym derived from "I Reveal My Attributes". In ICT, an attribute is any personal characteristic, such as age, address or Public Service Number. With IRMA, you can choose which attributes you reveal, and which you don't. We're working with Privacy by Design to develop propositions and applications for building IRMA's market presence.

PIN lets end users control what smart devices on their home networks can do.

SPIN

SPIN is an open-source system that SIDN Labs developed in 2017 for securing IoT devices in the home. SPIN protects the internet by automatically and temporarily blocking IoT devices in home networks if they send or receive abnormal traffic. It gives end users control over what IoT devices on their home networks are doing. In 2018, the focus was on finding the best way to introduce SPIN on a large scale. The first solid result of our efforts was a partnership with a modem manufacturer, who intends to offer the SPIN software on all their devices. We're now talking to various other suppliers within the industry. Partnering with manufacturers is seen as the business model likely to deliver the biggest impact. The potential of an earnings model based on extra services is being assessed.

On-line security for SMEs

In 2018, internet crooks stole money or data from 52 per cent of Dutch SMEs. Yet many smaller businesses continue to operate without adequate on-line security. They simply lack the time, know-how or financial resources to take action. Against that background, we teamed up with IT infrastructure security specialists Guardian360 at the end of 2018. We've started a cocreation programme with the aim of developing a new proposition to help SMEs stop hacks and data breaches, and reduce their vulnerability to cyber-attacks. The intention is to market the new proposition through our registrar network.

Domain Name Surveillance Service

The Domain Name Surveillance Service (DBS) is a monitoring service that alerts users whenever domain names are registered that closely resemble their own domain names or brand names. It enables companies to act swiftly in the event of typosquatting, phishing or trademark abuse. Such frauds were very much in the news in 2018, due to incidents such as the 'CEO fraud' that cost the Pathé corporation a staggering 19 million euros. The media coverage helped to drive up the number of DBS subscribers. We also used the DBS to perform an analysis of health care insurers' websites. No fewer than 450 scam sites were discovered, which were abusing the insurers' names for phishing. All the detections were reported, and notice-and-take-down procedures were initiated. We also shared advice on spotting phishing sites, both with health care insurers and with the general public.

No fewer than 450 scam sites were discovered, which were abusing health insurers' names for phishing.

Simplerinvoicing partnership ended

Simplerinvoicing is a trust framework that enables the fully electronic exchange of invoices between different ERP and bookkeeping packages. From 2014, we managed the system for the Simplerinvoicing Foundation. However, the Foundation has since undergone further professionalisation and is no longer in need of our support. Our partnership with Simplerinvoicing therefore came to a scheduled end in 2018.

Outlook

In 2019, we intend to continue development of four market propositions. We'll be seeking to identify practical applications for IRMA. Meanwhile, refinement of the SPIN software will continue; we'll forge multiple new partnerships and define the earnings model more sharply.
Our aim is to achieve success with at least two propositions. In parallel, we'll go on exploring opportunities for bringing further strategically compatible propositions to market in the future.

eHerkenning

eHerkenning is the business equivalent of DigiD, the digital ID system widely used by Dutch consumers. Any business that wants to access government services on line -- to file tax returns, for example -- will soon have to use eHerkenning. The technology is used for accessing a growing number of non-government services as well. As a result, at least 700,000 businesses, associations and foundations will need to acquire eHerkenning tokens. A mechanism has therefore been developed for registrars to buy eHerkenning services from Connectis -- one of the Netherlands' five providers -- for resale to clients. The scheme will enable registrars to benefit from the opportunities created by our acquisition of Connectis.

Bart Jacobs

Professor of Computer Security and Chair of Privacy by Design

""We've recently entered into a partnership with SIDN. They're going to help us with the development of IRMA, the attribute-based identity platform we've set up. IRMA is an acronym derived from 'I Reveal My Attributes'. In ICT, an attribute is any personal characteristic, such as age, address or Public Service Number. Often, an organisation you interact with only really needs to know one or two of your attributes. For example, if you want to play an X-rated computer game, it doesn't matter who you are, just how old you are. And, with a medical statement, the main thing is the doctor's professional registration details. IRMA gives users control over what data is processed. It protects your privacy by disclosing only as much info about you as strictly necessary.

We're strong on the technical side. Less so on the operational side - activities such as marketing. We're also quite a small organisation. And that can sometimes be problematic: potential partners often ask questions about our stability. Will Privacy by Design still be around five years from now? What happens to the foundation if I step away? How can we be sure that your solution will always work? By linking up with SIDN, we're not only gaining access to operational expertise, but also aligning ourselves with a large, stable organisation. And an organisation whose mission matches ours. Another plus is that, like us, SIDN is a non-profit organisation. IRMA is open source and has to stay that way."

By linking up with SIDN, we're not only gaining access to operational expertise, but also aligning ourselves with a large, stable organisation.

04 Internet security

Proactive security policy

We pursued a proactive policy of fake webshop detection, increased the security of our systems and promoted the use of secure internet standards.

Abuse204.nl

Abuse204.nl ('abuse to zero for .nl') is a programme that we run in partnership with registrars and hosting service providers. Its aim is to tackle phishing and malware in the .nl zone. Abuse204.nl alerts registrars and hosting service providers to suspected abuse on their networks, enabling them to intervene. Our Registration and Service Department maintains an overview and provides support where possible. In 2018, we maintained our efforts to drive down the average lifetime of phishing sites and sites with malware. Nevertheless, the figure rose a little, from seventeen hours at the end of 2017 to eighteen hours at the end of 2018. That's still a huge improvement on the situation before the programme started, when problem sites were live for an average of 144 hours. A sudden upturn was apparent in December, when we broadened our scan of the zone to include additional categories of malicious site (shopping site skimmers and cryptojacker sites).

DNSSEC validation rates disappointing

Adoption of the DNSSEC standard is extremely important. DNSSEC makes up for certain vulnerabilities in the DNS by adding an extra layer of security to the basic protocol. People visiting sites with DNSSEC-enabled domain names are better protected against misdirection to fraudulent IP addresses linked to practices such as malware distribution. What's more, DNSSEC forms the basis for new security applications, such as DANE. At the start of 2018, 49.27 per cent of registered .nl domain names were DNSSEC-enabled. By the end of the year, the figure was up to 53.49 per cent. However, there was little improvement in the disappointing rate of validation seen in 2017: the country's two biggest access providers still don't perform DNSSEC validation for their customers. The warning we sounded in 2017 unfortunately remains unheeded. Detailed DNSSEC statistics are available on stats.sidnlabs.nl.

DNSSEC makes up for certain vulnerabilities in the DNS.

Renewal of ISO27001 certificate

ISO27001 is a quality standard for information security. Certification is evidence of a high level of information availability, continuity, confidentiality and integrity. In 2011, we became the first registry in the world to achieve ISO27001 certification. The 2018 audit found no issues of concern, and our certificate was renewed for the eighth time.

E-mail security standards

Our incentive scheme for .nl registrars, the Registrar Scorecard, was extended to promote the use of various e-mail security standards. Financial rewards are available to registrars that use the StartTLS, DKIM, SPF and DMARC standards for the domain names in their portfolios. The standards considerably reduce the risk of abusive practices such as phishing and spamming.

Full migration to anycast

In 2017, SIDN Labs studied the way that resolvers select authoritative name servers in the field. The findings prompted our operations team to decide to phase out the unicast nodes for .nl and switch entirely to anycast. The new set-up boosts DNS traffic speeds and increases redundancy, making the system more robust.

Fake webshops

On the basis of research by SIDN Labs and our Support Desk, we alert registrars to domain names that have fake webshops linked to them. In most cases, the registrars then deal with the situation. The policy has already seen at least twelve thousand fake webshops taken down. Whenever we detect a fake webshop, we also check the registrant's identity, because experience shows the registration data is often false. The checks have enabled our Support Desk and our registrars to close down at least another five thousand fake webshops.

At least seventeen thousand fake web-shops were taken down.

Internet security awareness

We helped to raise internet security awareness in various ways. For example, we frequently highlighted issues through our newsletter and articles on our website. We also started an on-line campaign called Hackman. Videos published on social media showed how actress and presenter Lieke van Lexmond was hacked by an ethical hacker. A campaign website was created as well, where visitors can get advice and check just how good their own security is. The video was viewed almost 1.3 million times, making the campaign a big success. About 30,000 people filled in the hackman test questionnaire as well. Although research shows that Dutch people know how risky using a smartphone on an insecure network can be, lots of them don't take precautions. Only 33 per cent use two-factor authentication to access their social media accounts by mobile, for example. On the plus side, 60 per cent of Dutch smartphone users install software updates immediately.

Liaison with the NCSC

We act as the link between the National Cyber Security Centre (NCSC) and various other partner organisations. We share knowledge and information with the NCSC.

Outlook

In 2019, we'll continue investing in the security of the .nl domain and the wider internet. Our strategy will be based firmly on collaboration. We'll work with government bodies, anti-abuse programmes and partners in the domain name industry. We're also planning to expand the activities of our Security Operations Centre and reinforce its role. A proactive approach to the detection of fake webshops and abusive practices will be maintained.

Fake webshops

We intend to intensify our war on fake webshops. A new tool developed in house will further enhance our detection capabilities. Meanwhile, a procedural change will enable us to take down sites sooner when we find that the registration data has been falsified. All in all, our policies will mean that fake webshops remain active for weeks less than in the past, meaning that fewer consumers fall victim to scams.

Lynn van Herp

Liaison Network Chair, Nationaal Cyber Security Center

"Digital security has implications for the whole of society. So an effective approach to cybersecurity should involve all sectors of society working together. That's why the NCSC has established a network of 'liaisons': links with people within public and private organisations that represent particular sectors or target groups. The liaisons form channels for communication between the NCSC and the sectors or groups in question.

A liaison meeting is held every Thursday. The meetings serve to build mutual trust, reinforce the network and facilitate information exchange. You want all the organisations involved to be able to reach out to one another both in the 'hot' phase -- in an emergency, in other words -- and in the 'cold' phase -- under normal circumstances. Participants talk to each other about current developments, trends, threats and opportunities, and about the best ways to respond. The liaison organisations aren't expected to set up activities themselves, but to get the ball rolling within their sectors or groups.

SIDN is one of our liaison organisations. SIDN has specialist knowledge and expertise concerning the .nl domain and domain name registration; it's the designated organisation for issues in those fields. The NCSC also has close research and development ties with SIDN Labs. The knowledge and research results that they generate are very useful for lots of other organisations, and the liaison network is a great vehicle for wider dissemination."

SIDN has specialist knowledge and expertise concerning the .nl domain and domain name registration.

05 SIDN Labs

Impact continues to grow

In 2018, the research undertaken at SIDN Labs contributed to further enhancement of the security and stability of .nl, the DNS and the wider internet. The impact of our work continues to grow, and we enjoy increasing recognition as an expertise centre. An important feature of the year was a new line of research on internet systems.

Root Canary tool

In 2017, we joined the Root Canary project, bringing the project consortium up to seven partners: SURFnet, the University of Twente, Northeastern University, NLnet Labs, SIDN Labs, RIPE NCC and ICANN. The aim of this international collaborative project was to closely monitor the scheduled DNS root key rollover. The rollover took place on 11 October and involved ICANN replacing the cryptographic key pair that forms the basis of the DNSSEC infrastructure. Using our Root Canary tool, we kept a close eye on how the rollover was proceeding. We published our results in real time via our Twitter account and presented an analysis of the findings at OARC29. We also used the Root Canary tool to monitor the algorithm rollovers performed by our colleagues at .se (Sweden) and .br (Brazil).

DNS measurements

In tandem with the University of Twente, the University of Southern California, the University of Passo Fundo and NLnet Labs, we investigated the effects of DDoS attacks on the behaviour of DNS resolvers. We observed how the caching of DNS queries by DNS resolvers increases the resilience of the DNS. The time to live (TTL) selected for resolver caches plays a critical role in that context: very short TTLs appear to have the potential to amplify the effects of DDoS attacks. An article we produced describing the study was accepted for presentation at the prestigious ACM Internet Measurement Conference 2018. Under the auspices of the IETF, we're now summarising our research in this field to produce a guide to best current practice for authoritative DNS server operators.

SPIN

We implemented a new design for SPIN, our open-source platform for protecting the internet and end users against insecure devices on the Internet of Things (IoT). The new design makes SPIN suitable for use in various ways, including as a basic network device component. We helped our proposition development team to create a SPIN-based product for large-scale installation on modems and routers.
In parallel, we continued developing the SPIN software. That included creating the first version of a module for the automated detection of insecure devices, enabling intervention to stop them being used for DDoS attacks. We presented SPIN at various congresses as well, including the CENTR R&D workshop, the RIOT congress, ICT.Open and the Innovation Congress organised by the Dutch Ministry of Justice and Security.
We also linked up with Delft University of Technology to start the MINIONS project, whose aims include quantifying the concentrations of insecure IoT devices on the internet, mapping IoT botnets and cleaning up infected devices.

DMAP: functionality enhancement and use for fake webshop detection

In 2017, we developed the DMAP (Domain name ecosystem MAPper), a new tool that automatically looks up and checks all the domain names in a zone. It can establish whether they have security certificates and are IPv6-enabled, for example.
Last year, further improvements were made to the tool. We also used DMAP to automatically scan the 5.8 million domains in the .nl zone for possible fake webshops. Using the findings, SIDN's Support

Department worked with our registrars to take down the fake webshops detected. In addition, we presented our results at various conferences, such as ECP's Annual Congress and the DHPA TechFest. Finally, we wrote a research paper about DMAP, which was accepted for publication at the IFIP/IEEE Network Traffic Measurement and Analysis Conference (TMA 2018).

New internet systems

In the fourth quarter, we started a project investigating the potential of new open inter-networks. These are experimental alternative internet systems that, unlike the current internet, aren't based on the Internet Protocol (IP). New internet-systems could be made more transparent and secure, and could make better use of the opportunities offered by technological innovations such as open and programmable router hardware.

We're aiming to put the Netherlands and Europe at the cutting edge of developments.

Our aim is to contribute to these new systems, with a view to ensuring that the Netherlands and Europe are at the cutting edge of developments and ready for any new systems that emerge. We began by connecting our lab network to the SCION testbed. We also gathered community feedback at three workshops: at a partner's event organised by the registrar OpenProvider, the ECP Annual Congress and our own SIDN Connect event.

Collective anti-DDoS strategy

Along with the University of Twente and SURFnet, we co-authored an open letter proposing a proactive, collective anti-DDoS strategy for the Netherlands' vital infrastructure. Central to the proposal was a 'DDoS clearing house' for the continuous automated exchange of 'DDoS fingerprints' (DDoS attack characteristics) amongst service providers. That would enable proactive infrastructure adaptations to fend off attacks. Against that background, a consortium of about twenty-five partners launched a national initiative to realise the new anti-DDoS strategy. We also introduced the DDoS clearing house concept to the CONCORDIA European research project.

Improvements to stats.sidnlabs.nl

We upgraded our statistics website in 2018. We're now able to share data from our research projects more easily and in a more attractive and accessible form.

Outlook

New internet systems

Along with our partners (University of Twente, University of Amsterdam, SURFnet and NLnet Labs), we'll be experimenting with new types of internet-system.

SPIN

We intend to work with Delft University of Technology to study and evaluate SPIN modules for the automated detection of traffic from insecure IoT devices.

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.

Domain name abuse

We plan to devise new algorithms for the enhanced detection of abusive practices. The aim is to provide the capability to detect activities such as DDoS-for-hire services.

DDoS clearing house

With our Dutch and European partners, we'll be running a pilot with a DDoS clearing house for the continuous automated exchange of DDoS attack characteristics.

New research agenda

At the start of 2019, we published our new research agenda. We're going to focus on three fields: core internet systems, internet evolution and inter-domain trust infrastructures. The third of those fields is a new one for us, aligned with Connectis's activities. That work will start in the second half of 2019.

Aiko Pras

Professor Internet Security, University of Twente

"At a university, we can make all sorts of calculations and develop models, but the real world is never quite the way the theory suggests. So feedback from operational activities is essential. As a university of technology, we therefore need to collaborate with the business community. And, because we focus on DNS security, SIDN is the obvious partner for us. On a personal level too, we get on very well with the people at SIDN Labs. We're on the same wavelength and we interact well.

One great project that we're just starting with SIDN Labs involves research into 'future internets'. It's a topic with enormous significance for society. Europe is increasingly dependent on China and the US. They control the backbone of the internet. However, if we were ever to lose control over our internet, the consequences don't bear thinking about. So we're looking at new internet structures that would enable Europe to regain the control. The work's being done by a European consortium, and I'm really excited about its potential impact."

We're on the same wavelength and we interact well.

06

Expertise

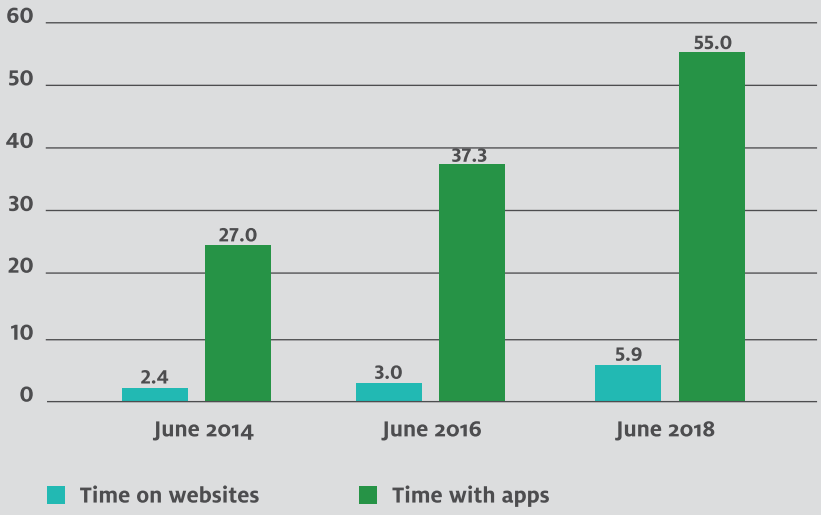
Sharing knowledge at all levels

Within our organisation, we have unique knowledge and expertise, which we're always pleased to share. In 2018, for example, we delivered a series of lectures at the University of Twente and ran courses for our registrars. We also undertook a variety of studies.

Survey of primary pupils' digital skills

We believe in an internet that's accessible to all. And, to access the net, people need certain skills. To find out whether youngsters are being taught the skills they need, we did a survey of digital literacy in primary schoolchildren. The results showed that there's plenty of room for improvement. More than a quarter of primary school teachers rated Dutch pupils' digital skills unsatisfactory. That is despite the fact that the great majority of parents and teachers see digital skills as an important aspect of education.

Fig. 6 | Smartphone users' total internet time (hours)



Trends in Internet Use

Our primary role is operating the .nl zone. The way we perform that role is, of course, influenced by the way that Dutch people use the internet and domain names. We therefore carry out periodic surveys of trends in internet use. We did our fifth such survey in 2018, and it drew some significant conclusions:

- Smartphones are increasingly used for 'serious' purposes. More and more things that we used to do only on our PCs, such as booking hotels, we now do on our mobiles.
- People are spending more time on line. Website visits are getting shorter, but we're using apps for longer.
- In the mobile internet era, apps are the driving force behind commercial success. However, most people have only a small number of apps on their phones. Competition for home screen space is therefore fierce.
- A strong on-line brand is increasingly important. Many firms are therefore merging product-specific sites in favour of a unified corporate brand.
- More and more internet users look at the domain when considering whether to trust an unknown website in a list of search hits. In the Netherlands, .nl domains are seen as the most trustworthy.

SIDN Academy

We've set up the SIDN Academy as a vehicle for sharing our knowledge with our registrars through courses and workshops. Its first offering was a course on using e-mail security standards, which proved so popular that it was repeated later in the year. The aim of the course was to increase knowledge of relevant internet standards and promote their adoption.

Lectures by 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.

In the Netherlands, .nl domains are seen as the most trustworthy.

Research into DDoS attacks

We teamed up with the National Internet Providers Management Organisation (NBIP) to study DDoS attacks in the Netherlands. Attacks on more than 60,000 sites over a twelve-month period were analysed. The study shed light on the backgrounds to DDoS attacks and enabled us to estimate the damage they are capable of causing.

Vooruitblik

Outlook

In 2019, we plan to run a new SIDN Academy course for our registrars, on the subject of IPv6.

Trends in Internet Use - follow-up study

We’ll be building on our annual trends survey by studying trends in e-identities and on-line security. We believe that those fields warrant close attention, which is best achieved by carrying out separate studies.

Kasper Schoonman

Managing Partner HostingU2

"SIDN Academy is a sort of industry-wide investment in knowledge. So I welcome it; it's a true expression of the foundation's purpose. The course was well organised and e-mail security standards was a good choice as the first topic to cover, because it tied in with the introduction of a new Registrar Scorecard incentive. Sharing knowledge at the same time as incentivising use of the standards made it easier for registrars to satisfy the criteria.

The SIDN Academy has now run one course. Personally, I'd like to see SIDN press ahead and start putting on more courses. Preferably covering a wider range of topics. As a Registrars' Association board member, I can confirm that that's the consensus within the RA as well. The RA hasn't always welcomed SIDN's initiatives in the past, but the SIDN Academy is certainly one we're very pleased with. The Academy was created in consultation with the RA, and we'd love to engage in dialogue about what happens next."

SIDN Academy is a sort of industrywide investment in knowledge. So I welcome it; it's a true expression of the foundation's purpose.

07 SIDN

At the heart of the (digital) community

We made increasing use of agile working methods and secured the services of numerous new personnel. We also continued to play an influential role in various international forums.

Operator of essential services

In 2018, the Network and Information Systems Security Act (Wbni) took effect in the Netherlands. The Act is intended to increase the nation's digital resilience and limit the potential impact of cyber-incidents. Under the new law, operators of essential services (OESs) and digital service providers (DSPs) are required to take steps to secure their ICT systems against threats.

As the registry for the .nl domain and a DNS service provider, we are a designated OES.

As the registry for the .nl domain and a DNS service provider, we are a designated OES. As such, we have to report any security incidents to the NCSC and the Radiocommunications Agency.

GDPR

On 25 May, the General Data Protection Regulation (GDPR) came into force in the Netherlands. We took prompt steps to ensure that our organisation is in full compliance. Although we are not strictly required to have a Data Protection Officer, we decided to appoint one, since we believe that, as the national registry, we should satisfy the very highest standards. The appointment reflects the same philosophy that led us to create a privacy board when we began analysing our DNS traffic data.

Internal

Workforce and sickness absence

In 2018, we invested considerable time and energy in raising our profile on the labour market. Our HR and Communications departments worked closely in pursuit of that goal. We also built on our ties with the higher education sector and actively sought to create internships and opportunities for postgraduate students. Our intensified recruitment efforts proved successful: of the twenty-four vacancies that arose in 2018, twenty-two had been filled by the end of the year. That is particularly satisfying, given that most were in professions such as ICT, where well-qualified people are hard to find. As a result, we ended the year with a workforce of 104 (94.09 FTEs). Of those, 28.8 per cent were women and 70.2 per cent men.

Our absence rate was high this year, at 7.2 per cent. However, that was partly due to non-work-related absences.

Agile working

Agile working increases our ability to respond to dynamic situations and reduces time to market. We have made great progress in introducing the philosophy throughout the organisation. Significant decision-making authority has moved to lower levels of the organisation, and increasing use is made of multidisciplinary, self-managing teams. We've also added several agile roles to our organisational model, while agile working methods such as Scrum and Kanban are being used more widely..

Development and training

We aim to provide an inspiring working environment and ample opportunity for personal development. Seven per cent of the wage bill is therefore allocated to training and development. In 2018, a lot of SIDN people did training sessions and courses devoted to Scrum and agile working.

We allocate 7 per cent of the wage bill to training and development.

Personal sponsorship budgets

We encourage personal development, provide an inspiring working environment, devote considerable attention to balancing work and home life, and offer a wide and generous compensation and benefits package. One element of that package is a personal sponsorship budget: a sum is made available to every member of staff each year, to support a good cause of their choice. The scheme is actively used for a variety of purposes.

Staff Council

As usual, the Staff Council was informed about SIDN's annual plan and budget for the year ahead. In September, the Council met SIDN's Supervisory Board.

The Council was also asked to approve a Whistle-blowers' Charter, a Standby Roster System for the ICT Department and a scheme to replace a surviving dependants' pension compensation scheme withdrawn by the pension administrator. Finally, the Council responded to a request for advice regarding a change to the organisational structure, and was involved in the transition to more agile working.

Connectis

At the start of 2017, we acquired a 65 per cent majority stake in Connectis, one of the country's biggest suppliers of secure log-in solutions. In 2018, Connectis made great progress with its product development and increased its turnover by nearly 50 per cent. The company implemented a new commercial strategy and realised operational improvements. Further efforts were also made to promote synergy with SIDN. In April, for example, SIDN enabled a private cloud service for Connectis. Connectis is therefore assured of a robust technical infrastructure, leaving it free to focus on its core activities. In November, Remco Coenen took over the reins as Connectis's Chief Executive. SIDN's CEO Roelof Meijer previously performed the role on an interim basis. Alongside Remco Coenen, Jeroen de Bruijn was appointed Commercial Director.

Contributions to organisations and conferences

We play an active role in various important international forums. In 2018, we again participated in numerous national and international meetings, helping to organise several of them.

ICANN

ICANN meetings were held in San Juan (10-15 March), Panama City (25-28 June) and Barcelona (20-25 October). Stakeholders from all around the world gathered to address policy issues, particularly concerning the Domain Name System. Ahead of two ICANN meetings, we worked with the Ministry of Economic Affairs and Climate Policy to organise the pre-ICANN meetings for the Dutch delegation..

IETF/IRTF

We attended the IETF meetings in London (17-23 March), Montreal (14-20 July) and Bangkok (3-9 November). We contributed actively to various IETF/IRTF working groups by making presentations and preparing an Internet Draft.

RIPE

We have been working with RIPE for many years. In 2018, we took part in both RIPE meetings, in Marseille (14-18 May) and Amsterdam (15-19 October). SIDN Labs spoke about the findings of our research into the impact of DDoS attacks on the DNS.

CENTR

We are active members of CENTR, the organisation for European ccTLDs. In addition, our Security Officer chairs CENTR's Security Workgroup, while our Legal and Policy Manager chairs the Legal and Regulatory Workgroup. CENTR organises various meetings for members to exchange experiences and discuss developments, including a Registrar Day, which we invite .nl registrars to attend with us. At the CENTR Jamboree in Moscow on 1 June, we organised

various successful sessions devoted to topics such as IoT security and tackling fake webshops. We also hosted the CENTR Marketing workshop in February and the R&D workshop in November.

ECP Annual Congress

We were once again pleased to support the ECP Annual Congress, held on 15 November. The event explored a variety of topics, including artificial intelligence. For the first time, we had our own track in the programme, with people from SIDN, SIDN Labs and SIDN Fund all sharing knowledge. The event gave some of the project teams assisted by SIDN Fund the opportunity to showcase their work as well.

One Conference 2018

Enterprises, governments and academics from all over the world met in The Hague on 2 and 3 October to share cybersecurity knowledge and experiences. We made a number of presentations, including a joint SIDN-NBIP session on defending against DDoS attacks.

Internet Security Platform

The Internet Security Platform is a joint public-private initiative intended to promote internet security. In 2018, we were again active participants, with representation on the steering committee for Internet.nl, for example.

Notice and Take Down Working Group

Under the umbrella of the Internet Security Platform, the NTD Working Group oversees the National Notice and Take Down Code of Conduct, introduced in 2008. Our Legal and Policy Manager chairs the group. Following a request from the Dutch government, the working group amended the Code at the end of 2018 to enable child pornography to be taken down more quickly.

RIOT Summit 2018

RIOT is an operating system for the Internet of Things. SIDN Labs made a SPIN presentation at the Summit in Amsterdam on 13 and 14 September.

DHPA TechFest 2018

The DHPA is a foundation that speaks for Dutch cloud and hosting service providers. At the DHPA Techfest 2018, held in Naarden on 24 May, we spoke to the audience about the detection of fake webshops.

ICT.Open 2018

ICT.Open is an event for ICT research in the Netherlands. SIDN Labs was in Amersfoort for the sixth edition on 19 March, giving a talk about SPIN.

Innovatiecongres

At the Innovation Congress hosted in Rotterdam on 20 November by the Ministry of Justice and Security, SIDN Labs made a presentation on SPIN.

SIDN Connect

On 29 November, we held the second edition of our SIDN Connect event, bringing together partners of SIDN, Connectis, SIDN Fund and SIDN Labs for a day on the KNVB Campus in Zeist. Having enjoyed a range of inspiring talks and thought-provoking sessions, participants gave the event a rating of 8.1 out of ten.

Partnerships and sponsorship

We work with and/or contribute to organisations, projects and campaigns that promote digital skills, mitigate the internet's negative side-effects or drive internet-related innovation.

Alert Online

Alert Online is an annual campaign run by the government, together with the business and academic communities. Its aim is to boost cybersecurity awareness amongst internet users of all ages and from all walks of life.

Bendoo Box

The Bendoo Box is a complete teaching package designed to get youngsters interested in learning to program. In 2018, no fewer than 2,700 schools were given free Bendoo boxes.

Bits of Freedom

Bits of Freedom defends freedom and privacy on the internet. Freedom and privacy are fundamental rights, and essential for development, technological innovation and the rule of law. Bits of Freedom fights for an internet that is open for everyone, where private communication remains private.

Codeweek

During the annual Code Week, we introduce primary and secondary teachers and pupils to the world of programming.

DINL

Digital Infrastructure Netherlands is a foundation dedicated to helping the Netherlands remain a leading digital infrastructure hub. DINL represents the companies and organisations that supply the facilities on which the digital economy is based – data centres, hosting service providers, internet service providers and others. We were one of the organisation's founders.

ECP
ECP is a neutral platform for the digital society, where the business community, the government and community organisations work together. Its aim is to facilitate and guide the digitisation of Dutch society through cooperation amongst its participants. We are one of ECP's partners and a long-time sponsor of ECP's annual congress. We also participate in many ECP activities, including the website veiliginternetten.nl.

ISOC.nl
The Internet Society has 44,000 members in 170 different countries. It is the parent organisation for various international bodies, including the IETF, IAB and IRTF. In the Netherlands, ISOC.nl has about a thousand members from the internet industry, business and government.

On-line Child Abuse Expertise Bureau
The On-line Child Abuse Expertise Bureau developed from the Reporting Hotline for Internet Child Pornography. It exists to prevent and tackle the on-line and off-line sexual abuse and exploitation of children.

NLnet Labs
NLnet Labs is an R&D institute with a strong international reputation. We have commissioned and funded a substantial portion of NLnet Labs' work since 2012. SIDN Labs works closely with NLnet Labs, and Cristian Hesselman, Director of SIDN Labs, chairs the NLnet Labs Board.

Summer School on Internet Governance
The Summer School on Internet Governance organises an extensive introductory programme on internet governance for students, academics, officials and businesspeople. We sponsor the annual European Summer School on Internet Governance.

Teaching children to program
In partnership with Connectis and Delft University of Technology, we offer programming lessons to primary schools in Rotterdam. In 2018, about a hundred schools took up the offer, enabling 2,500 children to receive tuition.

SIDN Fund

Following detailed evaluation, we decided that SIDN Fund should continue its work in the coming years. SIDN Fund is an independent foundation that we set up in 2014 to promote prosperity and wellbeing in the Netherlands by supporting initiatives that boost the internet's value to the nation. Having started work in spring 2015, SIDN Fund has made grants to nearly 150 innovative projects and achieved some striking results.
In 2018, the Fund again held two grant application rounds for innovative internet projects. Applications for Pioneer Project grants and academic research grants had to be linked to the theme for the year, Responsible AI, the idea being to promote artificial intelligence with a social conscience. Following careful consideration by the Advisory Panel, grants were awarded to thirty-nine Pioneer and Rich-potential Projects, plus one academic research project. In November, the Fund linked up with Google, Brinkhof Advocaten and Greenhost to organise the Internet Thesis Awards.

Some of the projects supported by SIDN Fund

MySensorData
Every smartphone has sensors, which collect data throughout the day. The MySensorData app lets you see what data is stored and decide for yourself what data you want used. On the MySensorData platform, you can choose applications to consult your data in a privacy-friendly manner. The idea won the SIDN Fund Pioneers Award at the Day of the Domain Name 2018.

Moral Mario
How can you test the safety and controllability of smart algorithms? In this project, a benchmark is being developed for a Super Mario environment. A self-learning Mario comes across safety problems at various levels, providing a basis for developers to test how 'moral' an algorithm is.

Touch ID
Logging in with a password represents a security risk. However, the problem can be solved by using your Touch ID on your smartphone. Biometric log-ins usually involve going through a third party. But this project is developing an open-source app, which ensures security and lets you log in without anyone else watching or saving your data.

Tigrinya project

Not all the world's languages have been digitised, because there's no commercial incentive in some cases. Tigrinya (spoken in Eritrea) is a good example. By digitising the language using AI algorithms, text-to-text translation will soon be possible. At a later stage, real-time translation using handheld translators is envisaged. That will help social workers and support agencies to communicate with the many Eritrean refugees arriving in the Netherlands, even if no interpreter is available.

Outlook

Automation

In 2019, we'll continue the automation of our IT environment. We expect to make major identity and access management enhancements to our Domain Registration System. We're well on course to realise a single sign-on for all our systems. In the year ahead, we'll also look to benefit from synergy with Connectis in this field.

IDnext

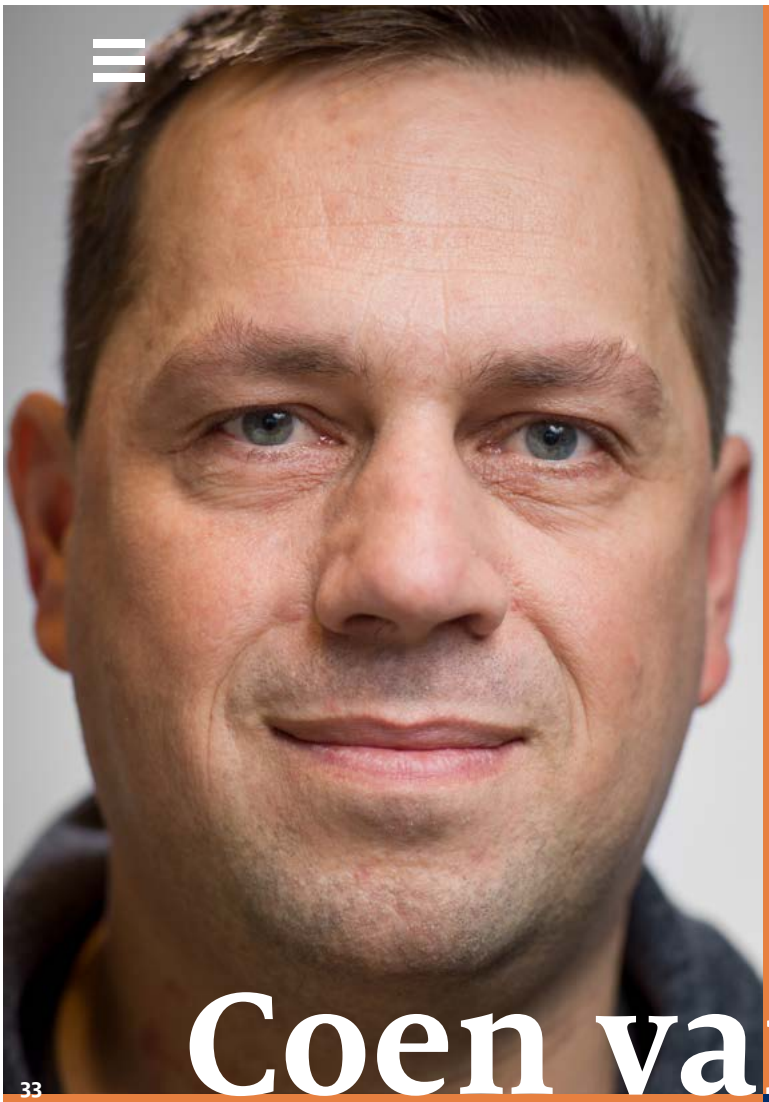
On 25 and 26 September 2019, SIDN and IDnext will co-host the two-day IDnext event devoted to internet security, privacy, trust and digital identities. IDnext is Europe's leading conference for experts and key players in the world of digital identification.

Jamboree in the Netherlands

On 27, 28 and 29 May 2019, we'll be hosting the CENTR Jamboree in Amsterdam.

EuroDIG in The Hague

In partnership with the Ministry of Economic Affairs and Climate Policy, the Municipality of The Hague and ECP, we're acting as local hosts for this year's EuroDIG: the annual European Internet Governance Forum, scheduled for 19 and 20 June.



Coen van Loon

ICT Operations

"I'd already been seconded to SIDN for a while, and really enjoyed it. I'm really into colo systems, and SIDN does a lot of colocation. The organisation has three data centres and uses numerous external sites. The maintenance of an operation like that is the sort of thing that appeals to me. So I took the plunge and asked whether they would give me a job.

My first day as an SIDN staffer was 1 May. The day before, I got a message saying that I shouldn't report for work before 8:30am. So I suspected that something was going on. When I turned up, they had decorated the whole place! Everyone was there to welcome me. There was cake... singing... they literally rolled out the red carpet for me. The CEO Roelof Meijer was even there to congratulate me personally. Because it turned out that I was SIDN's hundredth employee!

Crazy things like that are typical of SIDN. There's a really good team spirit. Everyone's willing to help, and we're always bouncing ideas around, thinking things through together. The organisation's small enough for everyone to know each other, but big enough to tackle exciting and challenging projects. There's plenty of opportunity for development as well. I couldn't wish for a better place to work!"

Crazy things like that are typical of SIDN. There's a really good team spirit.

08

Report of the Supervisory Board

Diversifying to maximise impact and assure continuity

The Supervisory Board supervises SIDN's Chief Executive and supports him with advice. The Supervisory Board considers matters such as SIDN's business strategy and the associated risks, realisation of the organisation's objectives and the design and effectiveness of the internal risk management and control systems. In 2018, the Board commissioned an external performance evaluation and implemented the recommendations.

Meetings

The Supervisory Board met five times in 2018, and also had one discussion with the Registrars' Association. There was regular contact with SIDN's CEO between meetings. Particular attention was given to the development of Connectis and to organisational changes. The Supervisory Board's various committees additionally met a number of times.

- Audit Committee: two meetings
- Selection and Appointments Committee: one meeting
- Security and Stability Committee: one meeting

The following were approved and/or adopted:

- Annual Report and Annual Financial Statement of SIDN for 2017
- Annual reports of the Supervisory Board, the Selection and Appointments Committee, the Audit Committee and the Security and Stability Committee in the context of corporate governance
- Annual plan and budget of SIDN for 2019

The Supervisory Board additionally authorised SIDN's CEO to vote on behalf of SIDN Deelnemingen B.V. in favour of the following motions at the Shareholders' General Meeting of Connectis Holding B.V.:

- Adoption of annual plan and budget for 2018
- Adoption of annual financial statement for 2016
- Adoption of annual financial statement for 2017
- Adoption of annual plan and budget for 2019

Membership

The Supervisory Board has seven members. Its membership did not change in 2018.

Paul Schnabel - Chair, Selection and Appointments Committee, Remuneration Committee
Mark Frequin, Selection and Appointments Committee, Remuneration Committee
Simon Hania, Security and Stability Committee
Kees Neggers, Security and Stability Committee
Jeannine Peek
Peter van Schelven, Audit Committee
Willem van Waveren, Audit Committee

Conclusions

The Supervisory Board believes that the policies pursued by SIDN have been such that the quality of SIDN's services is assured and that the company is ready for the immediate future. The .nl domain is stable and the quality of SIDN's infrastructure is high. Satisfaction amongst registrars continues to grow. Through SIDN Fund, SIDN Labs, community investments, Connectis and other diversification initiatives, SIDN is increasing its impact.
Financially speaking, the organisation is in robust health. Nevertheless, dependency on the .nl domain represents a long-term continuity risk. Diversification is therefore crucial. If the demand for domain names declines, it's important that SIDN's extensive and unique expertise are retained and used for the benefit of the local and/or wider internet community. In everything it does, SIDN strives to maximise the added value for the Netherlands.

Paul Schnabel,
Chair of the Supervisory Board

09 Financial statement

Finance

In 2017, through our subsidiary SIDN Deelnemingen B.V., we acquired a 65 per cent majority interest in Connectis Group B.V. of Rotterdam. In the Annual Financial Statement for 2018, the majority interest is accounted for as a participating interest; hence Connectis Group B.V.'s result for 2018 is included under 'Result from participating interests'.

The net result for the year was a loss of € 4.0 million, attributable mainly to the negative operating result of € 3.5 million. A negative operating result was foreseen in the plans and budget for 2018. The actual result is largely attributable to the deliberate policy of putting a portion of our accrued reserves to effective use: supporting SIDN Fund and increasing spending on, for example, 'registrar projects' and the Registrar Scorecard (our incentive programme for registrars). Allowance was also made for increased personnel costs in 2018. Half of the recorded rise in personnel costs was caused by the need to hire temporary staff to cover vacancies and absences due to sickness.

Corrected for the donation to SIDN Fund, the operating result for 2018 would be minus € 0.8 million, compared with a surplus of € 1.6 million in 2017. As a percentage of turnover, the operating result was minus 18 per cent (2017: minus 0.1 per cent).

Our share in Connectis Group B.V.'s net result for 2018 was € 0.2 million. Connectis realised its targets and budget for 2018, and substantial capital was invested in growth potential.

The net turnover in 2018 was € 19.5 million, or € 0.2 million down (-1%) on the previous year (2017: € 19.7 million). The reduction in turnover is attributable mainly to higher incentive payments to registrars in 2018.

Personnel costs were € 1.1 higher than in 2017, at € 9.9 million (2017: € 8.8 million). The rise is attributable partly to growth of the workforce and general pay rises (together € 0.5 million) and partly to higher pension contributions (€ 0.1 million). The increase in the size of the workforce was due to the expansion of SIDN Labs' research capacity and the establishment of a Security Operations Centre. Expenditure on temporary personnel increased by € 0.5 million, mainly as a result of delays filling certain vacancies.

Depreciation changes for 2018 were € 2.5 million, i.e. € 0.5 million higher than for 2017. The other operating expenses in 2018 were € 10.5 million (2017: € 8.9 million). The increase of € 1.6 million relative to 2017 was due mainly to the donation made to SIDN Fund.
We generated a negative cash flow of € 1.9 million (2017: negative flow of € 10.3 million). The negative cash flow in 2017 was mainly a consequence of acquiring a majority interest in Connectis Group B.V. (€ 8.6 million). The negative cash flow in 2018 is attributable partly to a tax deferral being charged to the accounts.

At the close of 2018, our equity capital was € 28.1 million. Our financial position therefore remains strong. The equity capital serves partly as a financial buffer, helping to assure service continuity. The minimum financial buffer required is related to the organisation's structural cost base. The cost base rises over time, as the organisation's activities expand and the quality, stability and security requirements increase. The financial buffer is currently ample to provide necessary and reasonable cover against the identified risks and uncertainties.

In order to manage our liquidity risk, we spent € 1.5 million on the acquisition of Dutch and German government bonds in 2017. The current value of the bonds is very similar. Our solvency fell slightly from 76.8 per cent in 2017 to 73.1 per cent in 2018. In 2018, € 5.2 million was invoiced and received for services to be delivered in the following calendar year; that is up from € 4.9 million in 2017.

In 2013, we began talks regarding the tax implications of the donation to SIDN Fund. SIDN and the tax authorities differed in their view of the extent to which the donation is tax-deductible. Hence, the corporation tax assessment received in respect of 2014 was not in line with the amount that SIDN reported as due on its tax return for that year. We accordingly appealed against the assessment. In 2018 we reached a settlement with the tax authorities regarding the actual deductibility of expenditure since 2013. That led to a net overall adjustment of € 0.7 million to the corporation tax liability for the preceding years.

The .nl domain contained more than 5.831 million domain names at the end of the year. In 2018, the net growth in the number of registered domain names was 37,200 down on the 109,706 seen in 2017. In order to promote the use of DNSSEC to secure domain names, we have been paying an annual rebate per secure domain name since July 2012. By the close of 2018, approximately 3.3 million domain names were secured with DNSSEC (57 per cent of all .nl domain names). In 2015, we started the Registrar Scorecard: an incentive programme designed to further increase the quality of the .nl zone. Through the programme, we returned € 1.6 million to participating registrars in 2018 (2017: € 1.3 million). The total value of all the incentives set off against the turnover (DNSSEC discount, Registrar Scorecard rewards, volume discount and direct debit discount) was € 3.5 million: a 9 per cent increase on the 2017 total of € 3.2 million. The number of registrars fell again, to stand at 1,258 at the close of 2018 (2017 1,303).

Outlook

We anticipate a slight increase in the number of registered .nl domain names in 2019 and a modest corresponding growth in earnings from .nl registrations. Total earnings are likely to increase a little as well. Our workforce is expected to grow, thus pushing up overall expenditure. Capital expenditure is likely to be broadly similar to 2018 and we anticipate that the result from participating interests will again be nil in 2019. Taking all factors into account, we envisage a smaller negative operating result.

Risks and uncertainties

Vision and policy

Our strategic plan for the next four years is reviewed and updated annually. As part of that process, we consider the company's (strategic) risk exposure. The management team and staff carry out a context analysis, in which opportunities and threats are surveyed. We also identify the strengths and weaknesses of the internal organisation. The conclusions of the analysis are then translated into a statement of risks and (where appropriate) countermeasures. The primary objectives of risk management are to assure the continuity of the organisation and our role as registry for the .nl domain, and to protect our position and reputation.

Since 2011, we have been ISO27001-certified. That status involves operating an Information Security Management System (ISMS), featuring an annual cycle of business impact analysis, risk identification, risk management and residual risk appraisal, all in accordance with a defined information security policy. The findings, reports and internal and external audits are regularly discussed, e.g. in our Tactical Security Meetings (TSMs), after which any necessary improvements are implemented. The outcomes are monitored by means of biannual management reviews. In that context, consideration is given to the results of the audits and performance assessments, as well as to the status of audit action points and any security incidents that may have occurred.

Before starting a project, we produce a project plan, which always includes a section covering the risks associated with the project, the risk management measures to be taken and residual risks. Before the project is given the go-ahead, consideration is given to the risk section of the project plan. Any changes to the risk situation and the risk management measures are addressed in the regular project progress reports.

Our Supervisory Board oversees our organisation's strategy, policy and general operational position. The Supervisory Board pays explicit attention to risk management, which is scrutinised by the Board's Audit Committee and Security & Stability Committee.

Strategic risk analysis and reporting

The main risks associated with SIDN's strategy stem from the strong dependence on (earnings from) the .nl domain and from the contraction of the .nl market. We do not have a direct sales channel to the end market and therefore have very little scope for influencing that market ourselves. The focus is consequently on collaboration with our registrars, e.g. through the Registrar Scorecard, which offers incentives to promote the use of .nl domain names. At the same time, we are seeking to increase our added value, extend the range of services we offer and reduce our dependence on .nl. It was with those aims in mind that we acquired a 65 per cent holding in Connectis Group B.V. at the start of 2017. In order to maintain risk separation between SIDN and Connectis Group B.V., we established a subsidiary, SIDN Deelnemingen B.V. at the end of 2016. It is the new subsidiary that holds 65 per cent of the shares in Connectis Group B.V. Connectis Group B.V. is currently transitioning from start-up to scale-up. It is a young, dynamic enterprise with a strong position and abundant opportunities in a growing and competitive market. In 2018, as in 2017, we continued to invest to facilitate the process of transition, with the emphasis on further professionalisation, realignment of the company's commercial strategy and the creation of synergy and added value.
Our strategic risk appetite is moderate in relation to activities with the potential to increase our added value.

Operating risks

The two main risks associated with our operating activities are interruptions to the availability of our services and breaches of the confidentiality or integrity of important data. Such problems could arise from technical and/or human error, or from deliberate (targeted or indiscriminate) human action. A prolonged, large-scale problem in one of those fields has the potential to threaten the continuity of the organisation in two ways. First, by seriously damaging our reputation, giving rise to doubts in political circles and the community at large as to SIDN's legitimacy as the registry for the .nl domain. Second, by leaving us vulnerable to large compensation claims from clients.

The significance of each key process for service continuity is assessed by means of Business Impact Analysis, which is part of the ISMS. Our DNS services – the basis of the functionality of registered domain names – are the most critical, closely followed by our registration services, which enable users to register new domain names and to update and cancel existing registrations. Also rated as critical are the Whois/Is, the power supply, our office IT systems, our website www.sidn.nl, and our communication and telecommunication systems. With a view to assuring availability, integrity and confidentiality, we have put a wide variety of risk management measures in place, designed to minimise the likelihood of problems, and to enable swift corrective action and minimise impact if problems do arise. The measures in question range from the elimination of single points of failure by extensive redundancy in hardware, software, connections, third-party services and expertise, logical and physical access control, audits and penetration testing, contractual arrangements with suppliers, codes of conduct for SIDN personnel, an emergency backup location, crisis and relocation drills, a privacy board and a Security Operations Centre (SOC).

Our operating risk appetite is low in relation to interruptions to the availability of our services and breaches of the confidentiality or integrity of important data. Our risk appetite in relation to activities with the potential to increase operational excellence is moderate.

Financial risks

- Damage claims and penalties: service interruptions and data confidentiality or integrity breaches have the potential to generate claims and/or penalties. Our General Terms and Conditions limit or exclude our liability for such problems.
- Currency/exchange rate risk: our exposure to currency and exchange rate risks is modest. Our .nl services are priced in euros and we make little use of suppliers that charge us in other currencies.
- Bad debt risk: about 75 per cent of registrars pay by direct debit. Our General Terms and Conditions make provision for action to be taken if a registrar does not fulfil its financial obligations.
- Liquidity risk: our liquid assets are divided across three Dutch banks. In 2017, we acquired a portfolio of Dutch and German government bonds.
- Market risk: our portfolio of Dutch and German government bonds was acquired with a view to holding the bonds until maturity. If circumstance should require us to dispose of the bonds prior to maturity, we would face the risk of the bonds having diminished in value relative to the date of purchase.
- Solvency risk: we maintain a financial buffer to assure the continuity of the organisation (for a period) in the event of a significant loss of our earnings and/or the need for high expenditure at short notice. The minimum size of the buffer increases in step with our structural cost base. The financial buffer is currently well above the defined minimum.
- Uncertainty about our ability to attract finance: to date, we have not needed to seek external finance.

Our financial risk appetite is low.

Legislative and regulatory risks

Changes to national or international legislation and regulations have the potential to affect our organisation and operating processes. We take stock of potentially significant proposed or impending legislative and regulatory changes – e.g. changes in employment law, tax law or data protection law – at an early stage. The impact of any such change is assessed and translated into organisational adaptations, which are then implemented. In view of the potential impact of legislative or regulatory changes relating to our registry role, we have a Legal & Policy Manager with responsibility for that domain. Where necessary and possible, the Legal & Policy Manager seeks to influence the nature of any proposed changes.

We initiated a comprehensive inventory of our personal data processing activities in connection with the General Data Protection Regulation, which came into effect in 2018. Each processing activity is being critically examined to determine whether it is consistent with the new legislation. Where necessary, we will modify our procedures to ensure compliance with the law. We have voluntarily appointed a Data Protection Officer.

Our legislative and regulatory risk appetite is low; we endeavour to operate well within the parameters of all applicable legislation and regulations.

Consolidated financial statements for 2018

Consolidated balance sheet as at 31 December 2018 (after appropriation of profit)

	31 December 2018 (in €)		31 December 2017 (in €)	
Fixed assets				
Intangible fixed assets		6,992,515		8,393,948
Tangible fixed assets				
Land and buildings	5,147,068		5,326,488	
Machinery and equipment	836,742		1,107,138	
Other fixed business assets	608,821		789,711	
Tangible fixed assets under development	29,174		0	
		6,621,805		7,223,337
Financial fixed assets		3,690,854		4,135,007
Current assets				
Receivables				
Trade receivables	396,459		303,489	
Tax and social security contributions	1,208,846		363,548	
Other receivables and accrued and deferred assets	1,211,978		1,088,038	
		2,817,283		1,755,075
Liquid assets		18,384,811		20,326,724
		35,507,268		**41,834,091**

	31 December 2018 (in €)		31 December 2017 (in €)	
Group equity		28,149,021		32,131,840
Long-term liabilities				
Other liabilities		406,250		406,250
Short-term liabilities				
Accounts payable	1.104,879		1,113,426	
Tax and social security contributions	420,679		365,941	
Other liabilities and accrued and deferred liabilities	8,426,439		7,816,634	
		9,951,997		9,296,001
		38,507,268		**41,834,091**

Consolidated profit and loss account for 2018

	2018 (in €)	2017 (in €)
Net turnov	19,481,759	19,704,620
Expenditure		
Wages and salaries	7,345,103	6,351,074
Social liabilities	709,964	691,554
Pension costs	978,649	858,979
Other personnel costs	916,093	892,793
Depreciation	2,518,557	2,000,516
Other operating expenses	10,518,465	8,929,193
	22,986,831	19,723,927
Operating result	-3,505,072	-19,307
Financial income and expenditure	48,067	21,950
Result before taxation	-3,457,005	2,643
Taxes	-726,371	-478,772
	-4,183,376	-476,129
Result from participating interests	200,557	-169,079
Result after taxation	**-3,982,819**	**-645,208**

Consolidated cash flow statement for 2018

	2018 (in €)	2017 (in €)
Cash flow from operating activities		
Operating result	-3,505,072	-19,306
Adjustment for depreciation	2,518,557	2,000,513
Movement in working capital		
Movement in receivables	-253,002	-96,250
Movement in short-term liabilities	665,339	876,965
Cash flow from operating activities	-574,178	2,761,922
Interest received	1,145	30,356
Corporation tax	-587,155	-709,653
	-586,010	-679,297
Cash flow from operating activities	**-1,160,188**	**2,082,625**
Cash flow from investment activities		
Investments in intangible fixed assets	-268,099	-8,424,855
Investments in tangible fixed assets	-247,493	-775,767
Acquisition of participating interests	0	-243,956
Mutatie overige financiële vaste activa	-266,133	0
Long-term lending	0	- 1,487,260
Acquisition of securities	0	-1,489,643
Cash flow from investment activities	-781,725	-12,421,481
Increase/(decrease) in funds	**-1,941,913**	**-10,338,856**

Consolidated cash flow statement for 2018

	2018 (in €)	2017 (in €)
Analysis of funds		
Funds as at 1 January	20,326,724	30,665,580
Movement in liquid funds	-1,941,913	-10,338,856
Funds as at 31 December	**18,384,811**	**20,326,724**

10 Directors and officers

Directors and officers on 31 december 2018

Chief Executive Officer

Roelof Meijer

Management team

Cristian Hesselman, SIDN Labs
Arjan Middelkoop, New business, Marketing & Sales
Lilian van Mierlo, Registration & Services
Cees Toet, ICT
[vacancy], Chief Financial Officer

Staff Council

Sebastiaan Assink (Chair)
Remko van den Berg
Barry Peters (Vice-Chair)
Martin Sluijter (Secretary)
Ruben Wubbels

Complaints and Appeals Board

Peter Blok
Huib Gardeniers (Secretary)
Hendrik Struik
Judith de Vreese-Rood (Chair)
Thomas de Weerd
Dennis Wijnberg

Supervisory Board

Mark Frequin
Simon Hania
Kees Neggers
Jeannine Peek
Peter van Schelven
Paul Schnabel (Chair)
Willem van Waveren

11 Glossary

Abuse
Use of the internet for an inappropriate purpose. Common forms of abuse include sending spam, phishing and creating botnets.

Access provider
A service provider that enables customers to access the internet.

Agile working
Working in a responsive and adaptive way. In an agile organisation, projects are often divided into small, surveyable periods and there is continuous consultation with the client. The agile working philosophy originates from the ICT industry and makes use of various techniques, most notably the scrum.

Anycast
Global anycast is a proven and effective technology for spreading network load across multiple instances of seemingly the same server. The way it works is as simple as it is effective: a number of servers share a single IP address, making routers 'think' that they are all the same server. IP packages are forwarded to the 'nearest' point.
Local anycast differs from global anycast insofar as a number of local nodes are created. A node is a computer or another device connected to a given network, which can only be approached locally. As a result, worldwide DDoS traffic cannot ever reach a local node. The only DDoS traffic that can reach the node is locally generated traffic, which is much easier to control. Local anycast is therefore an effective response to the risk of major DDoS attacks.

General Data Protection Regulation (GDPR)
From 25 May 2018, uniform privacy legislation will apply throughout the EU: the General Data Protection Regulation (GDPR).

Big data
A very large volume of digital information gathered for analysis, often from various sources.

Blockchain
The technology underpinning many cryptocurrencies, including Bitcoin. In principle, it works like a general accounting ledger.
However, it isn't maintained by a central administrator, but by all its users. When one user performs a transaction, it is immediately recorded by all users. Its decentralised structure makes a blockchain unhackable.

Caching
Storing data in temporary files. Retaining frequently visited web pages in a cache means that the same information doesn't have to be fetched repeatedly.

ccTLD
In full: country-code top-level domain. A top-level domain linked to a country, e.g. .nl (the Netherlands), .de (Germany) and .fr (France).

CENTR
An association for the registries that run ccTLDs, including SIDN. It is a forum for discussion about policies that affect ccTLDs and a conduit for communication between the ccTLDs and other parties involved in the internet's (further) development, such as ICANN.
See also centr.org.

Cloud computing
Computer services, such as storage, database management, networking and software, which are delivered via the internet ('the cloud'). Examples include video streaming and on-line gaming.
Complaints and Appeals Board (C&AB)
An independent body to which .nl registrars and registrants can appeal against certain types of decision made by SIDN. The C&AB also considers complaints asserting that a domain name's registration is inconsistent with public order or decency.
See also cvkb.nl.

DDoS
A distributed denial-of-service attack is a concerted effort to make a computer, network or service unavailable to its intended user(s). DDoS attacks can be carried out in several different ways.

DNS
Abbreviation of Domain Name System or Domain Name Server. The global DNS is the system and protocol used on the internet to translate domain names into IP addresses and vice versa.

Downtime
The time that a website is unreachable or an application is inactive.

DNSSEC
Domain Name System Security Extensions (DNSSEC) is a suite of extensions to the DNS protocol. It involves the use of cryptographic techniques to prevent cybercriminals diverting internet traffic to fraudulent websites without the users realising. The basic DNS protocol does not provide optimum protection against such threats.

Domain name
A name within the Domain Name System (DNS), the internet's naming system. A domain name such as sidn.nl is made up of several parts: the top-level domain, '.nl', and the second-level domain, 'sidn'.

Domain Name Surveillance Service (DBS)
A monitoring service provided by SIDN to assist with the identification of typosquats and other issues. Users are alerted if a domain name is registered that is similar to their company name or brand name.

Registrant
The person or organisation in whose name a domain name is registered. Only the registrant is entitled to receive SIDN's services.

Dispute Resolution System for .nl Domain Names
Anyone who registers a .nl domain name is responsible for making sure that the registration doesn't infringe anyone else's rights. That can happen if, for example, the domain name makes use of someone else's brand name, trading name, personal name or organisation name. If a registration appears to infringe someone's rights, a dispute can arise. SIDN's Dispute Resolution System has been set up as a quick and affordable alternative to using the law courts to settle a dispute.

General Data Protection Regulation (GDPR)
From 25 May 2018, uniform privacy legislation will apply throughout the EU. The Dutch regulation implementing the GDPR is the Algemene Verordening Gegevensbescherming (AVG).

ECP
ECP, the Platform for the Information Society, is a vehicle for the business community, the government and social organisations to work together to support the use of ICT in Dutch society.
See also ecp.nl.

E-invoicing
The electronic exchange of invoices.

eID
Electronic evidence of identity, which can be used for gaining secure and reliable access to on-line public and commercial services.

ENTRADA
An open-source big data platform developed by SIDN Labs for the analysis of large volumes of DNS data. The database that ENTRADA uses contains more than a hundred million DNS queries.

Fake webshop
An internet site that looks like a normal webshop, but actually exists only to defraud visitors.

gTLD
Generic top-level domain: one of the main types of internet domain. Well-known gTLDs include .com, .org and .edu. The introduction of numerous new gTLDs, including .amsterdam, began in 2014.

ICANN
The Internet Corporation for Assigned Names and Numbers is a non-profit organisation that performs a number of important tasks, such as assigning and specifying top-level domains, assigning domain names and allocating IP addresses. ICANN does not manage any domain names itself. That job is delegated to registries such as SIDN (.nl) and VeriSign (.com and .net).
See also icann.org.

Identity and access management (IAM)
The collective processes by which an organisation administers and manages network users, including for example processes for managing access to applications and systems.

IETF
The Internet Engineering Task Force is an international community of network designers, operators, suppliers and researchers, which develops internet standards.
See also ietf.org.

Internet governance
The development and application of shared principles, standards, rules, decision-making procedures and programmes that shape the way the internet is used.

Internet Governance Forum
The Internet Governance Forum (IGF) is an annual gathering of governments, market players and non-governmental organisations, under the auspices of the United Nations. At the IGF, public policy issues are discussed with the aim of ensuring that the internet remains manageable, robust, secure and stable. The IGF does not define policy.
See also intgovforum.org.

Internet of Things
A development of the internet, where everyday devices, such as thermostats and baby monitors, are connected to the internet and able to exchange data.

Internet service provider (ISP)
A business that provides internet access services to other businesses or private individuals. Many ISPs also provide other services, such as e-mail, web hosting and spam filtering.

Internet Protocol (IP) address
A unique combination of numbers and/or letters. Every computer or server on the internet has an IP address, at which it can be contacted. If you visit www.whatismyip.com you can check the IP address of the device you are currently using.

IPv6
Every computer or server on the internet has an IP address, at which it can be contacted. Addresses are created in accordance with the Internet Protocol. IPv6 is that latest version of that protocol, which supports an almost infinite number of IP addresses. It has been developed to succeed IPv4 (version 4), because IPv4 addresses are running out.

ISOC (Internet Society)
An international organisation for worldwide collaboration and coordination on matters relating to the internet and the associated technologies and applications. ISOC brings together sixteen thousand internet professionals in 180 countries, many of whom helped to create the internet.
See also internetsociety.org.

Internet Society of the Netherlands (ISOC.nl)
A society of about eight hundred members from backgrounds including the internet industry, the business community, government, consumers' organisations, the non-profit sector, the technology industry and the financial, legal and academic domains.
See also isoc.nl.

Java
A programming language that is widely used on the internet.

Malware
Any kind of malicious software, including computer viruses and worms.

Name server
A computer on the internet, which 'translates' a domain name into an IP address (a unique numeric internet address). The name server is part of the DNS.

New gTLD Programme
An ICANN initiative: the largest extension to the domain name system ever. In 2013, the number of generic domain names was increased from twenty-two to more than a thousand.

NL IGF
A joint initiative by the Ministry of Economic Affairs, SIDN and ECP. Its purposes are, first, to embed the conclusions of the international Internet Governance Forum (IGF) in national policy and, second, to ensure that the Netherlands has a voice and that Dutch issues are aired within the international IGF.

Notice-and-Take-Down Procedure
A voluntary internet industry code of conduct on dealing with reports of unlawful or illegal website content, such as child pornography, plagiarism, discrimination and selling illegal goods. The code describes the procedure for complaining about the content of a website. A complaint should be addressed first to the provider of the offending content. If the provider cannot be contacted or refuses to take the content down, the matter may be taken up with the next party in the chain. The chain is as follows:
- Content provider
- Website provider (registrant)
- Website hoster
- Internet access provider
- SIDN (registry)

If all the other parties in the chain have been asked to take down the offending content but have not done so, SIDN can, in the last resort, disable the associated domain name.

Open source
A development philosophy based on making source material freely available to all. Open-source software is software whose source code is freely available, so that anyone may copy it, modify it or distribute it without having to pay for the privilege.

Phishing
A form of internet crime. It involves sending e-mails and setting up websites that look as though they come from or belong to well-known and trusted organisations, when in fact they are forgeries. The forged messages and sites encourage people to part with information, such as log-in details and credit card details, which the criminals then use for their own purposes.

Real time
The actual amount of time required to do something. Real-time interaction is interaction without delays or data processing waiting periods.

Registrar
An intermediary who acts for a registrant or prospective registrant in interaction with a registry. (The registry for .nl is SIDN.) Most registrars are hosting service providers, internet service providers or access providers.

Registry
In full: domain name registry. The register of all the internet domain names under a given top-level domain, or the organisation that manages that register.

Resolving
Responding to DNS queries.

RIPE NCC
The Réseaux IP Européens Network Coordination Centre is the Regional Internet Registry (RIR) with responsibility for issuing IP addresses in Europe and the Middle East. RIPE NCC is one of the world's five RIRs, the other four being APNIC (for Asia and Australia), AfriNIC (for Africa), LACNIC (Latin America) and ARIN (for North America).
See also ripe.net.

Server
A powerful computer with a fast connection, which is set up to provide information. A web server is directly connected to the internet.

TLD
Abbreviation of top-level domain.
The domain whose name forms the last part of an internet address, after the dot.

Top-level domain
The domain whose name forms the last part of an internet address, after the dot, e.g. '.nl' in 'sidn.nl'.

Internet service provider (ISP)
A business that provides internet services, e.g. on-line TV and internet telephony. ISPs typically also provide network equipment for home networks.

Signing
DNSSEC works with digital signatures, known as 'private keys'. For effective security, DNS data needs to be signed with a digital signature and the signature needs to be checked ('validated') by the data user.

Single sign-on
Single sign-on-software enables a network user to gain automatic access to multiple applications or resources by signing on once. It therefore removes the need to enter a password repeatedly.

Spam
Unsolicited e-mail.

SSL
A data encryption technology for securing the connection between a website visitor and the website's server.

Typosquatting
A form of internet abuse that takes advantage of the fact that people sometimes make slips when typing web and e-mail addresses. A user who mistypes an address lands on the typosquatter's site. Typosquatting is often associated with malicious activities such as phishing.

Unicast
A way of exchanging data on a computer network, where data packages go from a single source to a single destination (host).

Uptime
The period that a computer system or network is available.

Validation
DNSSEC works with digital signatures, known as 'private keys'. For effective security, DNS data needs to be signed with a digital signature and the signature needs to be checked ('validated') by the data user.

Registrars' Association (RA)
Association that speaks for the .nl registrars in their relations with SIDN and regularly discusses the main features of registry policy with SIDN.

Whois
A protocol for retrieving the details of a domain name, e.g. the name and address of the registrant and registrar, from a database. SIDN manages the Whois data for all .nl domain names.
See sidn.nl/Whois.

WIPO Arbitration and Mediation Center
An independent, international non-profit organisation that arbitrates in domain name disputes and other cases.
See also wipo.int.

Zone file
A text file listing all the domain names in a zone, plus the associated webserver IP addresses.

Colophon

Editorial
Stichting Internet Domeinregistratie Nederland, Arnhem

Text
ARA, Rotterdam

Design & realisation
Lumen Ontwerpersnetwerk, Breda

Translations
G & J Barker Translations, Worcester, United Kingdom

Contact
SIDN
Meander 501
6825 MD Arnhem
Postbus 5022
6802 EA Arnhem
The Netherlands
T +31 (0)26 352 55 00
communicatie@sidn.nl
www.sidn.nl

© SIDN
Text and figures from this report may be reproduced, but we ask that you let us know of your intentions in advance by mailing communicatie@sidn.nl and that you credit us as the source.

Subscribe to our newsletter
www.sidn.nl/newsletter