

Connect, reflect and share

SIDN Connect 2017

Een lagerhuis met gelijkgestemden

Van gehackt worden, naar hacker

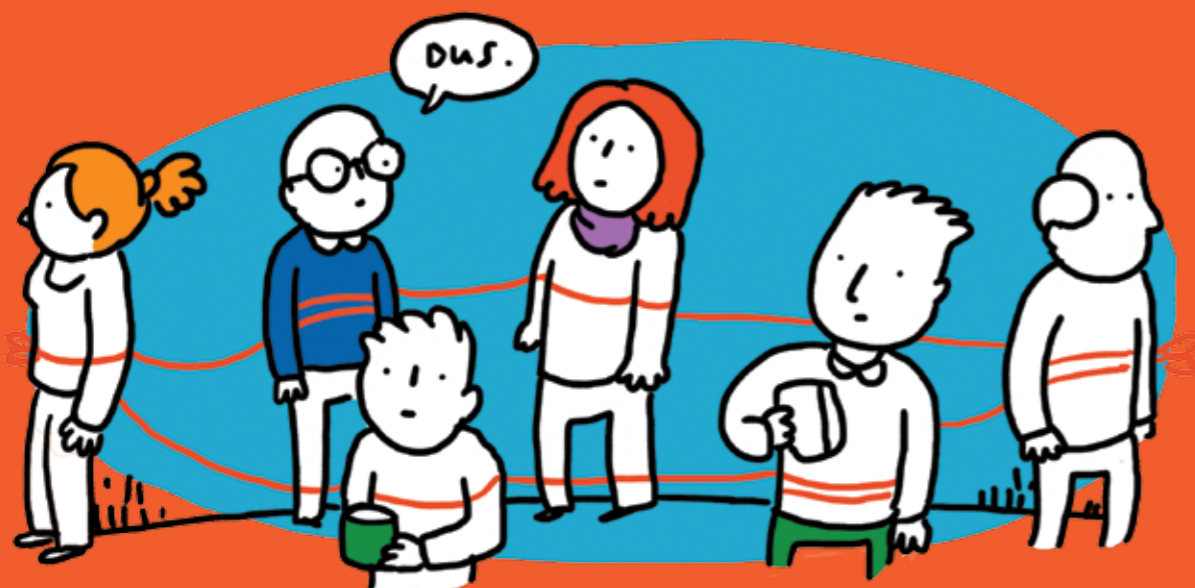
Een sterk internet voor iedereen



Jouw wereld. Ons domein.

SIDN CONNECT

NEEMT PARTNERS VERBINDEN WEL
HEEL LETTERLIJK



Voorwoord van Roelof Meijer



Inhoud **7**

Bezoekersinterviews



5

Jurjen Lengkeek over Moore's law



11

Hattrick van bezoekersinterviews	5
SIDN Connect 2017	7
Ontwikkelingen SIDN	8
Moore's law in actie	11
Bescherming van security en privacy in het internet of things	12
Van gehackt worden, naar hacker	15
Weet wat je verzamelt	17
Een sterk internet voor iedereen	18
Om te groeien moet je alles weten van je klant	21
Hattrick van bezoekersinterviews	23
Een lagerhuis met veel gelijkgestemden	27
Workshops	29
Online advertenties op basis van je simkaart en je WhatsApp-gesprekken	33
Scheidsrechter met passie	35
Colofon	38

SIDN lagerhuis met Chris van het Hof



Keynote van Bas Nijhuis



Diverse 'spelers' aan het woord



Camiel Cornelissen

Hostnet

"Het is de eerste keer dat ik SIDN Connect meemaak. Ik ben vooral benieuwd naar de sessie over GDPR. Dat gaat impact hebben op de bedrijfsvoering. Het is nuttig om eerst van alle kanten informatie te verzamelen voordat we beslissen wat wij daarmee gaan doen." ■



William van Beek

Lukkien BV

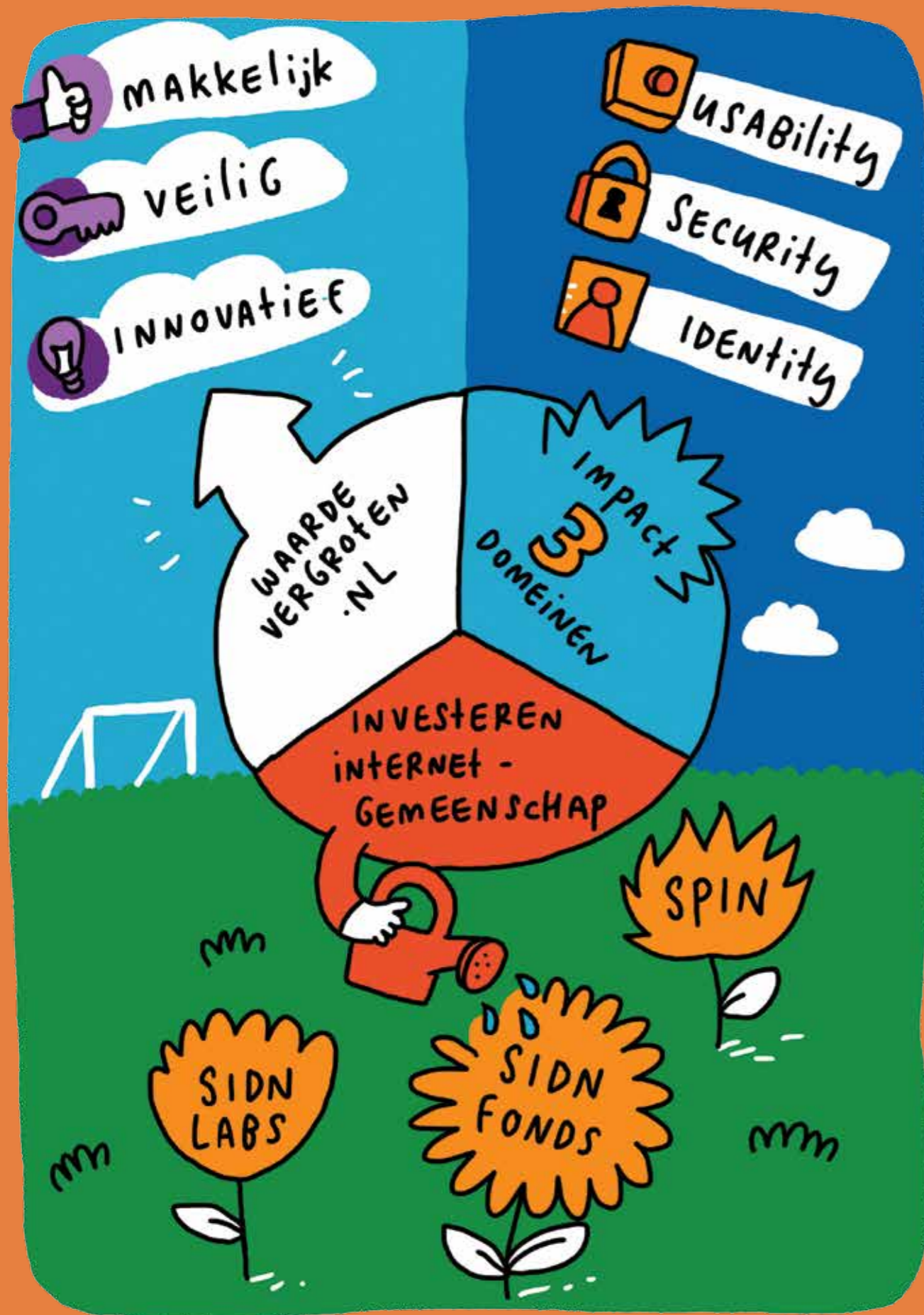
"Ik ben gekomen vanwege de GDPR en wat dat inhoudt op het gebied van hosting. De mogelijkheid van potentiële grote boetes forceert je om stappen te nemen. Wij zijn op zich redelijk laat, deels omdat er weinig voorlichting vanuit de overheid is op dit wetsgebied. Daarom stromen de seminars over dit onderwerp nu vol. De andere sessies laat ik gewoon op me af komen." ■



Cristian Kiesling

Kiesling media

"Dit is de tweede keer dat ik naar een SIDN relatedag kom. Vorig jaar was een succes! Ik heb toen tijdens het event een hele mooie deal weten te sluiten. Vandaag lopen er ook weer veel van mijn leveranciers rond, waarmee ik graag wil connecten. Ik hoop ook veel bruikbare tips uit de sessies mee naar huis te kunnen nemen." ■



SIDN Connect 2017



2017 was best een spannend jaar voor SIDN. Het was het jaar waarin we bekend maakten dat we een meerderheidsbelang namen in Connectis. Connectis is één van de grootste leveranciers van veilige inlogoplossingen in Nederland. Het bedrijf verwerkt miljoenen inlogtransacties per jaar. Met dit meerderheidsbelang gaven we ook invulling aan de ambitie om onze toegevoegde waarde te vergroten door onze dienstverlening te verbreden én zetten we onze eerste stappen op het acquisitiepad.

Een zorgeloos digitaal bestaan voor iedereen

Die ambitie om onze impact te vergroten, hebben we al een aantal jaar. We zijn er namelijk van overtuigd dat we alle ervaring en kennis die we hebben opgedaan met het beheer van het .nl-domein en de positie die we daarmee hebben gekregen optimaal moeten inzetten om het .nl-domein en het internet in Nederland nog stabiel en veiliger te maken. Daarom delen we onze kennis, ondersteunen we via het SIDN fonds projecten die het internet sterker maken en ontwikkelen we nieuwe producten en diensten.

Werelden met elkaar verbinden

Met de verbreding van onze dienstverlening gaan er ook nieuwe werelden voor ons open. Er komen andere relaties op ons pad.

Hoe mooi is het om al deze werelden met elkaar te verbinden en relaties met elkaar in contact te brengen. Dat is precies wat we met deze eerste editie van SIDN Connect wilden doen: al onze relaties op 1 dag samenbrengen en inspireren.

Succesvolle 1^e editie

Met elkaar kunnen we terugkijken op een geslaagd event. In dit magazine kun je alle hoogtepunten van de dag nog eens rustig bekijken. De verhalen van Rickey Gevers over zijn leven als hacker en van Bart Schermer over de nieuwe AVG-wet passeren nog eens de revue. Maar ook de discussie tijdens het lagerhuis en de diverse projecten die het SIDN fonds ondersteunt, komen aan bod. En nog veel meer.

Noteer SIDN Connect 2018 alvast in je agenda

Ik hoop dat je tijdens SIDN Connect 2017 een heleboel inspiratie en nieuwe interessante contacten hebt opgedaan. En als je er dit jaar niet bij kon zijn, zorg dan dat je volgend jaar zeker van de partij bent. Ik beloof dat het dan zeker weer een interessant event wordt. Noteer de datum van SIDN Connect 2018 alvast in je agenda: 29 november 2018 bij de KNVB Campus.

Tot volgend jaar!

Roelof Meijer
Algemeen directeur SIDN

Ook in 2018 zetten we onze missie voort: een onbezorgd digitaal bestaan voor iedereen

De meeste mensen kennen SIDN als beheerder van het .nl-domein. Maar in de afgelopen jaren zijn we onze dienstverlening gaan verbreden. We delen onze kennis, doen wetenschappelijk onderzoek, steunen initiatieven voor een beter internet en ontwikkelen nieuwe diensten. Ook namen we een meerderheidsbelang in Connectis om mensen en organisaties te helpen bij het veilig inloggen. Via al deze wegen proberen we de maatschappelijke en economische waarde van het internet te vergroten. Hier lees je wat we afgelopen jaar allemaal hebben gedaan en blikken we vooruit op 2018.

Waarde vergroten van .nl

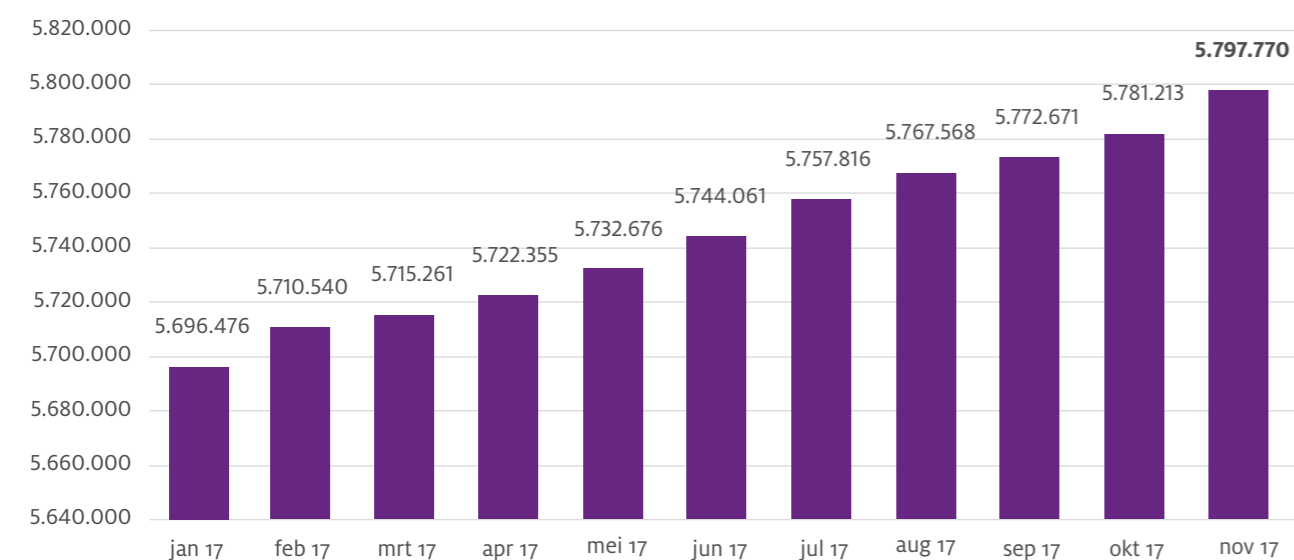
Met bijna 5,8 miljoen domeinnamen groeit .nl, ondanks voorspelde krimp, nog steeds. Onze registrars spelen hierin een belangrijke rol. De opheffingen en registraties zijn in balans omdat er in de afgelopen jaren veel verbeterd is in de kwaliteit van het .nl-houderbestand. Veel registrars hebben de afgelopen jaren flink opgeschoond. In 2018 verwachten we groei door de aantrekkelijke economie. Met onze nieuwe suggestietool is het vinden van een goede beschikbare .nl-domeinnaam makkelijker geworden. Net als het zoeken van een registrar om de domeinnaam te registreren.

Via onze Registrar Scorecard (RSC) stimuleren we onze registrars om het .nl-domein veiliger te maken. Dat doen we door registrars te belonen die bijvoorbeeld al hun

domeinnamen ondertekenen met DNSSEC. Sinds dit jaar belonen we ook op het gebruik van IPv6 en verhoogden we het budget voor de Registrar Scorecard om zo nog betere resultaten te halen. Verder stimuleren we registrars mee te doen aan Abuse204.nl (lees 'abuse to zero for .nl'). Met dit programma bestrijden we phishing en malware in de .nl-zone.

Omdat voorkomen altijd beter is dan genezen, hebben we enkele jaren geleden onze Domeinnaambewakingsservice (DBS) geïntroduceerd. Met onze DBS-monitoringtool waarschuwen we vooraf over de domeinnaamregistraties die lijken op jouw merk of domeinnaam. Sinds dit jaar niet alleen binnen .nl, maar nu ook voor alle extensies. Op die manier kun je in actie komen voordat een aanval start. Inmiddels maken bijna 200 merken gebruik van deze dienst.

Ontwikkelingen .nl 2017



Impact in 3 domeinen: e-identity, security & usability

Binnen onze strategie zetten we in op impact in 3 domeinen, namelijk e-identity, security en usability. Connectis is één van de grootste leveranciers van veilige inlogoplossingen in Nederland. Via Connectis kunnen we onze impact uitbouwen binnen het domein e-identity. We stapten in op het moment dat Connectis een nieuwe fase inging. We hebben de bedrijfsvoering verder geprofessionaliseerd en de commerciële strategie aangepast. De ingezette strategie begint zijn vruchten al af te werpen.

Binnen het domein security werkt SIDN Labs, onze onderzoeksafdeling, aan het SPIN-project. Dit is een prototype voor de beveiliging van smart devices die onderdeel uitmaken van het internet of things. Het systeem is bedoeld voor thuisnetwerken, waarbij we DDoS-aanvallen vanaf slimme apparaten aanpakken. Zo willen we eindgebruikers inzicht geven in en controle geven over de gegevens die gedeeld worden door hun devices. We hebben het systeem dit jaar open source gemaakt en geven regelmatig nieuwe releases uit. Ook in 2018 borduren we voort op dit project.

In het domein usability toetsen we momenteel .nl Garant. De nieuwe standaard in veilig en vertrouwd online shoppen. We werken hiervoor samen met een verzekeraar. Als uit onderzoek blijkt dat er in de markt behoefte is aan dit product, lanceren we deze dienst in 2018.

Investeren in de internetgemeenschap

SIDN Labs zet zich in voor een veilig en stabiel .nl en internet. Afgelopen jaar voerden zij een aantal studies uit in opdracht van ICANN. Ze analyseerden grote hoeveelheden historische data om te onderzoeken wat de impact van het new gTLD-programma is geweest op de stabiliteit van de DNS-root (CDAR) en op domeinnaam-abuse in nieuwe en bestaande gTLDs (SADAG). Dit laat zien dat we mee kunnen met de internationale top. Verder doen we onderzoek naar resolvers 'in the wild'. We onderzoeken hoe DNS-resolvers zich in het veld gedragen. Ook hier weer op basis van analyses van grote hoeveelheden data. Resultaten gebruikten we om onze DNS-strategie aan te passen en unicast nameservers voor .nl uit te faseren.

Via het SIDN fonds dragen we bij aan het vergroten van de waarde van het internet voor economie en maatschappij. Ons fonds is nu 3 jaar actief en er zijn al 121 innovatieve projecten ondersteund. Dit jaar opende het fonds voor het eerst een call binnen een specifiek thema, Blockchain for Good. Maar liefst 14 blockchain-projecten kwamen door de selectie en hebben dit jaar subsidie ontvangen. Ook nieuw dit jaar was de ondersteuning van 3 wetenschappelijke onderzoeken door het fonds. Komend jaar roept het fonds registrars op om mee te denken over belangrijke thema's als: opleiding, security en bewustwording van gebruikers (bv. van encryptie)

Samengevat: 2017 was voor ons in veel opzichten een succesvol jaar. En ook voor 2018 zitten we weer vol plannen. Daar praten we je graag over bij tijdens SIDN Connect 2018! ■

Moore's law in actie

De kracht van computerchips verdubbelt iedere 2 jaar. Deze voorspelling staat bekend als Moore's law en hij geldt tot op de dag van vandaag. Bij RDM Makerspace kijken ze wat al die toegenomen rekenkracht betekent voor de maakindustrie. Jurjen Lengkeek, medeoprichter van RDM Makerspace, vertelt dat ze bij voorkeur aan de slag gaan met technologieën die over de ergste piek aan hooggespannen verwachtingen heen zijn. Mensen zijn geneigd om in eerste instantie te veel te verwachten van nieuwe technologie, maar het effect op de lange termijn juist te onderschatten. Dit proces wordt beschreven in Gartner's Hype Cycle, een grafiek van de vijf stappen die iedere nieuwe technologie doormaakt: een technologie trigger, het hoogtepunt van opgeblazen verwachtingen, een val in desillusie, nieuwe hoop en tenslotte daadwerkelijke productiviteit. Lengkeek: "Na de desillusie gaat de lucht eruit. Dan wordt het interessant om te kijken wat je er echt mee kunt."

Experimenteren met Marvin

Neem het internet of things, dat momenteel hard naar beneden dondert omdat het achterblijft op de voorspellingen. Praktische toepassingen bevinden zich met name op het gebied van predictive maintenance, om stilval van fabrieken tegengaan. Maar je kunt ook zelf met IoT aan de slag. Samen met KPN richtte RDM Makerspace de IoT Academy op, waar iedereen IoT-oplossingen kan bouwen. Bijvoorbeeld met behulp van Marvin, een IoT-development board. Met dit een apparaatje ben je binnen no time verbonden met het internet of things.

Machine learning en metaal 3D printen

RDM Makerspace is gevestigd in een voormalige scheepswerf in Rotterdam. Een zelfvarende watertaxi voor de deur zou dus een mooi visitekaartje zijn. De computer aan boord leert nu nog door

een echte schipper gade te slaan. In de toekomst bestel je de watertaxi met een app en komt hij zelfstandig aanvaren. Meer ontwikkelingen in de scheepvaart: op de dag dat SIDN Connect plaatsvindt, wordt de eerste 3D geprinte scheepsschroef gepresenteerd bij scheepswerf Damen in Gorinchem. Dit is een project van RAMLAB van RDM Makerspace. Het metaal printen nam 256 uur printen in beslag, maar dan heb je ook een schroef van 1.30 meter doorsnede en een gewicht van 200 kilo!

Robots en nieuwe ontwikkelingen

De koepel in het dak van RDM Makerspace is ontworpen door een robot. Hij bestaat uit allerlei verschillende hoeken, die door een robotarm zijn uitgesneden. Daarna hebben mensen heel lang moeten puzzelen om de koepel in elkaar te zetten, maar het resultaat mag er zijn. Ook de in piepschuim uitgefreesde mensen in de hal zijn gemaakt door een robot. Lengkeek zou er nog veel langer over kunnen vertellen, maar hij moet een vliegtuig halen. In Chicago begint binnenkort een hackaton, waar ontwikkelaars uit de hele wereld toepassingen voor Marvin bedenken. Hij straalt ervan. "Met één kleine uitvinding in een klein landje kun je tegenwoordig zo veel bereiken." ■

"Met één kleine uitvinding in een klein landje kun je tegenwoordig zo veel bereiken."

Jurjen Lengkeek, RDM Makerspace



Bescherming van security en privacy in het internet of things

Een veelbesproken onderwerp rond het internet is tegenwoordig de (afwezigheid van) veiligheid en privacy bij internet of things (IoT) apparaten. Naarmate het aantal van dergelijke apparaten in ons dagelijks leven groeit, nemen ook de zorgen rondom de veiligheid en privacy hiervan toe. Jelte Jansen, research engineer, vertelde erover tijdens zijn break-outsessie.

Dit probleem wordt van verschillende kanten aangepakt; organisaties die bezig zijn met IoT kijken naar verbeterde werkwijzen van fabrikanten en beleid en wetgeving over veiligheid en privacy. Dit gebeurt zowel op nationaal als internationaal niveau, maar men richt zich ook op het beter informeren van gebruikers over wat hun apparaten misschien achter hun rug om doen.

Onze aanpak

SIDN Labs is van mening dat er geen 'silver bullet' bestaat om de beveiliging van producten en de privacy van gebruikers van het internet of things (of het internet in het algemeen) te garanderen; er is continue verbetering op al deze fronten nodig.

Jansen: "Met dat in het achterhoofd zijn we gestart met een onderzoekstraject op een van deze gebieden: Security for In-home Networks (SPIN). Het doel van het project is het ontwerpen, prototypen en evalueren van de zogenaamde SPIN controller. Dit is een systeem voor thuisnetwerken dat de gebruiker de controle teruggeeft over de veiligheid en privacy." De SPIN controller moet gebruikers inzicht geven in en controle geven over de veiligheid en het gedrag van hun IoT-producten. In de simpelste vorm lijkt dit op een persoonlijke firewall, maar dan voor een netwerk van IoT-apparaten in plaats van bijvoorbeeld alleen maar een desktopcomputer.

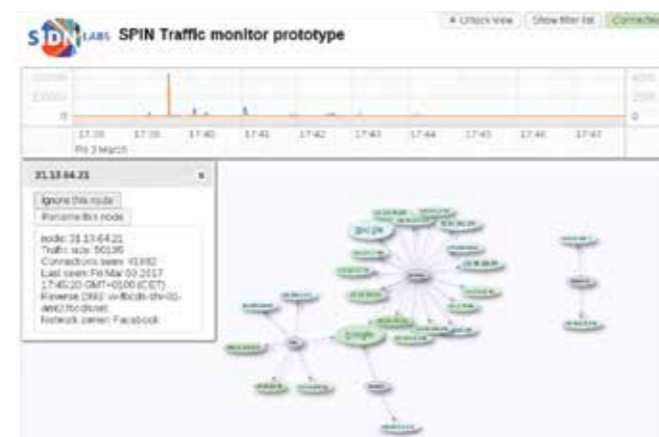
"We hebben ervoor gekozen op thuisnetwerken te focussen omdat we hiermee 2 vliegen in 1 klap slaan: we helpen gebruikers hun netwerken beter te beveiligen en kwaadwillenden hebben minder mogelijkheden om IoT-producten te misbruiken voor aanvallen op de infrastructuur van het internet, zoals die van SIDN als beheerder van het .nl-domein." Natuurlijk zijn er producten waarmee thuisnetwerken bewaakt en bestuurd kunnen worden; er zijn behoorlijk wat 'traffic monitors' en firewall-implementaties beschikbaar. Maar de meeste oplossingen abstraheren te veel details

weg, of juist veel te weinig. Om een voorbeeld te noemen; hulpmiddelen om dataverkeer in te zien geven vaak alleen totalen weer en netwerkfirewalls werken met voorzichtig in te stellen regels die veel details bevatten. Bovendien zijn deze oplossingen vaak niet specifiek gericht op het IoT, en hebben gebruikers veel netwerkkennis nodig om ze effectief in te kunnen zetten.

Jansen: "Het doel van ons onderzoek is hier een middenweg in te vinden, en daarvan open source prototypes te ontwikkelen die door derden kunnen worden opgepakt en ingezet in hun oplossingen."

SPIN-prototype

Het prototype van de SPIN controller richt zich op privacy-awareness en simpele visualisatie, waarbij getoond wordt hoe 'kletsgraag' sommige IoT-producten zijn. De huidige versie van de SPIN-software toont de laatste 10 minuten van netwerkactiviteit (zie Figuur 1). De screenshot laat interne apparaten zien in het grijs, recente verbindingen in het groen, en oudere verbindingen in het blauw.



Figuur 1: Screenshot van de SPIN visualiser prototype



Het scherm links toont extra informatie over de geselecteerde node. Een gebruiker kan voortaan via de interface specifieke data of een heel apparaat blokkeren. Proeft het apparaat vervolgens toch verbinding te maken, dan verschijnt dat op het scherm in het rood.

Open source

"We hebben de SPIN-software beschikbaar gesteld als open-source software op Github. Een werkende versie van het prototype bundelen we met de Valibox software, op OpenWRT gebaseerde firmware voor thuisrouters die DNSSEC-validatie mogelijk maakt op thuisnetwerken. De huidige bèta-versie bevat een prototype van de SPIN visualiser."

Toekomstig werk

Het onderzoek bevindt zich nog in een vroeg stadium. SIDN Labs werkt aan een aantal andere modules voor de SPIN

controller, die het mogelijk moeten maken een veiliger en privacy-vriendelijker thuisnetwerk te hebben, ook als het aantal IoT-producten in dat netwerk toeneemt.

Jansen: "Een van de volgende stappen is bijvoorbeeld om te kijken welk verkeer we voor een apparaat verwachten en welk verkeer niet. Verdere verbeteringen moeten de gebruiker helpen daarbij beter geïnformeerde beslissingen te nemen, door meer inzicht en misschien zelfs adviezen te geven. We willen ook meer intelligente modules toevoegen die het netwerk zelf scannen op kwetsbaarheden zoals standaard wachtwoorden en onbedoeld open toegang van buitenaf."

Nieuwsgierig geworden?

Bekijk op sidnlabs.nl/SPIN de screencast van een vroeg prototype van de SPIN-software die draait in een netwerk met een aantal apparaten, waaronder een smart televisie en een RIPE Atlas probe. ■

Van gehackt worden, naar hacker

Het begon voor Rickey Gevers allemaal toen zijn website Waarneming.nl gehackt werd. Hij wist niet wat hem overkwam en voelde zich machteloos. Aan die machteloosheid wou Rickey iets doen. Hij zocht uit hoe zijn website te hacken was en hoe hij zich in de toekomst kon wapenen tegen een hackaanval. Al snel ontdekte Rickey dat hij goed was in hacken en werd het een spelletje voor hem om lekken in systemen te ontdekken. Inmiddels is Rickey al zes jaar professioneel actief in de cybersecuritywereld en gebruikt hij zijn hack skills om bedrijven te weren tegen cybercrime.

Door het zelf te doen, ontdekte Rickey dat hacken helemaal niet zo moeilijk is. "Mensen denken altijd dat hacken heel ingewikkeld is. Dat daar de meest technische en vernuftige trucjes bij komen kijken. Maar dingen als een wachtwoord verzinnen doen mensen meestal op zo'n eenvoudige manier, dat je vaak al te moeilijk denkt als je het probeert te raden", vertelt Rickey. Hij probeert mensen daarom altijd een spiegel voor te houden en benadrukt dan ook hoe eenvoudig hacken is. Zo legt hij uit dat iedereen met tools als Ransomware achter zijn of haar eigen bureau van cybercrimineel kan uithangen. "Ransomware heeft cybercrime heel toegankelijk gemaakt. Met een paar muisklikken kun je een hacktool downloaden. Daarnaast is de Bitcoin erbij gekomen waardoor je zelf ook heel goed de betalingen kunt regelen."

Toename

Zo ziet Rickey cybercrime de laatste jaren toenemen. "Ik denk dat dat vooral komt omdat we steeds meer met technologie opgroeien. Je ziet dat jongeren die met een iPad worden opgevoed, vaak technisch gezien veel meer ervaring hebben dan oudere mensen. Daarom zijn juist oudere mensen eerder slachtoffer van criminele hackers."

Goed vs. slecht

Er zijn gelukkig niet alleen hackers die hun hack skills voor criminele doeleinden inzetten, Rickey is hier een voorbeeld van. Rickey: "Als cybercrimespecialist bij Red Socks Security houd ik mij bezig met het in de gaten houden van cybercriminelen. Ik kijk vooral naar welke tools ze gebruiken om hun aanvallen uit te voeren. Zo krijg ik een beeld van wat er gaande is. Met die kennis wapenen we bedrijven en organisaties

tegen cyberaanvallen." Waar organisaties eerst huiverig waren, ziet Rickey steeds meer bedrijven die open staan voor de diensten van een cybercrimespecialist.

"Het wordt steeds meer maatschappelijk geaccepteerd. Je ziet een toename in het aantal bedrijven dat een Responsible Disclosure beleid toepast. Men begrijpt nu beter dat wij niet meer bekijken dan nodig is, om te kunnen bevestigen waar een lek zich bevindt."

Een gewaarschuwd mens

Naast de uitgebreide rapporten die Rickey schrijft voor organisaties, heeft hij ook voor particulieren een paar simpele tips, waarmee iedereen de meeste hackers buiten de deur kan houden. Het is belangrijk dat je ervoor zorgt dat de software op je apparaten up-to-date is. Daarnaast is Two Factor Authentication een goede manier om persoonlijke informatie extra te beveiligen. Dat is een methode waarmee je ervoor zorgt dat je pas in kunt loggen als je ook de code invult die je door middel van een SMS ontvangt. "Hackers kunnen vaak heel makkelijk je wachtwoord achterhalen, maar jij hebt jouw telefoon in je bezit. Een ander kan dan niet makkelijk achterhalen wat de code is. Stel je loopt ergens buiten en je krijgt een SMS met het wachtwoord, terwijl je niet zelf probeert in te loggen, dan weet je dat iemand anders onder jouw naam probeert in te loggen. Dan kun je direct maatregelen nemen."

Juist omdat je met dit soort kleine maatregelen je gegevens net iets beter kunt beveiligen, vindt Rickey het belangrijk om mensen hiervan bewust te maken. "Ik wil zoveel mogelijk mensen informeren, want een gewaarschuwd mens telt voor twee." ■

*"Met boeven
vang je
boeven.
Dat klopt."*

Rickey Gevers, Red Socks Security

Weet wat je verzamelt

Vanaf 25 mei 2018 gaat de nieuwe Algemene Verordening Gegevensbescherming wet van kracht. Deze Europese privacyverordening regelt de legitieme en zorgvuldige omgang van (persoons)gegevens door overheden en bedrijven. De focus ligt hierin onder andere op het versterken en uitbreiden van privacyrechten, strengere eisen en meer verantwoordelijkheden voor organisaties en gelijke bevoegdheden voor alle privacytoezichthouders in Europa. Sinds 25 mei 2016 krijgen organisaties de ruimte om hun bedrijfsvoering met de nieuwe AVG-wet in overeenstemming te brengen. Bart Schermer, partner bij Considerati, helpt bedrijven hiermee en legt uit hoe je in je eigen bedrijfsvoering de eerste stappen zet ter voorbereiding op de nieuwe wet.

Gelijke rechten, gelijke kansen

“Deze nieuwe wetgeving is zo belangrijk omdat het over de gegevens van mensen gaat en een zorgvuldige omgang daarmee. Er kan heel veel misgaan met die gegevens, zeker als je ze niet netjes beveiligd of beschermt. Mensen kunnen op allerlei manieren op een negatieve manier geconfronteerd worden met de verwerking van gegevens”, zegt Bart. Daarnaast creëert deze nieuwe wetgeving een gelijk speelveld voor organisaties, hosters, registrars en andere belanghebbenden in Europa. Bart: “Of je nu een hoster bent in Frankrijk of een hoster in Nederland, in heel Europa gelden straks exact dezelfde regels.”

Beginnen bij het begin

“De verordening zegt dat je twintig dingen moet regelen. Dat lijken in eerste instantie op zichzelf staande regels, maar er zit een samenhang in. Door er een geïntegreerd programma van te maken en duidelijk in kaart te brengen wie er binnen je organisatie verantwoordelijk is voor de verschillende onderdelen, maak je het zoveel mogelijk relevant voor de afdelingen die belast worden met de nieuwe wetgeving”, zegt Bart.

Zoals in elk proces moet je eerst weten waar je nu staat. Bart: “Dat betekent in termen van de AVG dat je twee dingen moet weten: ‘wat doe ik allemaal met gegevens’ en ‘hoe bescherm ik die gegevens’. Dat is waar wij onze projecten altijd mee beginnen. Heel vaak weten bedrijven dat niet eens. Maar je moet eerst weten wat je hebt, dat bepaalt het risico en de urgentie van het verwerken van bepaalde maatregelen.”

Beveiligen

Een andere belangrijke randvoorwaarde is beveiliging en het aanpassen van je toegangsbeleid. Bart: “Beveiligen kan op tal van manieren, zoals het toepassen van wachtwoorden en toegangsbeleid. Wie mag er bij welke gegevens, onder welke omstandigheden? Maar denk ook aan encryptie – het versleuteld opslaan van gegevens – of firewalls en antivirusbescherming. Eigenlijk moet je alles wat je normaliter bij informatiebeveiliging in zijn algemeenheid gebruikt, hierbij ook doen.”

“Vanuit informatiebeveiligingsperspectief is het met name relevant dat je een goede risicoclassificatie maakt. Je wilt niet een dubbeltje met een kwartje beveiligen. Of je nou een dubbeltje in huis hebt of een euro, dat kun je alleen beoordelen door eerst een overzicht te maken van wat je nou eigenlijk met gegevens aan het doen bent binnen je bedrijf”, vertelt Bart.

Serieuze zaak

“Deze nieuwe privacywet is een stuk strenger dan de oude wet. Tot op heden maakte de privacywetgeving weinig mensen iets uit. Maar met deze wet gaan bedrijven het steeds belangrijker vinden, omdat de risico's, met name in de vorm van hoge boetes, groter worden. Ook voor hosters heeft dit consequenties. Verantwoordelijken die een hoster gaan inhuren hebben met de nieuwe wet de verplichting om alleen met hosters te werken die zich netjes aan de regels houden. Als resultaat laten zij hosters contracten ondertekenen om het risico op hoge boetes te verkleinen. De nieuwe AVG-wet zorgt dus voor bewustwording bij deze doelgroep, maar ook bij individuele burgers. Er gaat een andere discussie komen.” ■

“Select
before you
collect.”

Bart Schermer, Considerati

Een sterk internet voor iedereen



In 2014 besloot SIDN een deel van haar vermogen te investeren in het vergroten van de waarde van het internet voor de maatschappij en de economie en richtte zij SIDN fonds op. Een onafhankelijk fonds met als missie 'een sterk internet voor iedereen'. Volgens Valerie Frissen, directeur van SIDN fonds, betekent een sterk internet niet alleen een robuust internet, maar ook een internet dat open is, dat je vertrouwt, waar je vrij kan zijn en waar je veilig voelt.

SIDN fonds

SIDN fonds biedt ondersteuning aan projecten die een bijdrage kunnen leveren aan een sterker internet en daarmee ook een maatschappelijke focus hebben. Enerzijds zijn dit projecten die te maken hebben met het internet zelf. Dit zijn projecten die een veilig, open en vrij internet realiseren en versterken. Anderzijds gaat het om projecten die het internet als middel gebruiken om maatschappelijke impact te creëren, bijvoorbeeld in het onderwijs of in de zorg.

Uniek in haar soort

"Er zijn niet zoveel private fondsen die in internet- of technologieprojecten investeren. In die zin hebben wij een unieke plek", vertelt Valerie. "In de internetwereld zie je heel snel dat startups naar het private geld toegaan om ietste kunnen realiseren, die maatschappelijke impact verdwijnt dan al snel naar de achtergrond." Daarom biedt SIDN fonds naast financiële ondersteuning, ook bijeenkomsten aan waarin ze experts aan de projecten koppelen. Denk bijvoorbeeld aan juridisch advies ter voorbereiding op de nieuwe privacywetgeving in 2018. "We bieden zo veel mogelijk ondersteuning, zodat het geld dat we verstrekken niet 'down the drain' gaat, maar zodat de projecten het zo effectief mogelijk inzetten", vertelt Valerie.

Aanmelden

Twee keer per jaar kunnen projecten zich aanmelden. Daarin maakt SIDN fonds onderscheid tussen pioniers (projecten gericht op de uitwerking van goede ideeën) en potentials (projecten die al bewezen hebben dat ze een maatschappelijke meerwaarde brengen en doorontwikkeling of opschaling nodig hebben). Beide groepen gaan door een zorgvuldige selectie en worden grondig getoetst door het bureau van het SIDN fonds en de Raad van Advies van het fonds, bestaande uit experts in de internetwereld. De beste potentials projecten mogen langskomen om hun project bij de Raad van Advies te pitchen.

Cases

De eerste stappen in e-banking

Otly! is een voorbeeld van een project dat SIDN fonds ondersteunt. Otly! is een e-banking app, waarmee kinderen hun zakgeld ontvangen, sparen en online aankopen doen, binnen een veilige digitale omgeving en onder toezicht van ouders. De app helpt kinderen bij het omgaan met geld en besteedt aandacht aan belangrijke elementen als beveiliging en de risico's van online betalen. Als ouder bepaal jij de content die jouw kind ziet. Je kunt Otly! koppelen aan je bank of je kiest ervoor zelf via iDeal of PayPal te betalen.

Lior Bornshtain: "Met Otly! vullen wij een missende laag in veilig bankieren voor kinderen. Wij begeleiden hen tijdens hun eerste stappen in de e-banking wereld en ondersteunen ouders bij het geven van financiële educatie. SIDN fonds heeft ons een landingsbaan gegeven om onze start-up verder te ontwikkelen."

Otly! wordt momenteel door 16.000 kinderen in Nederland gebruikt, mede dankzij de hulp van SIDN fonds.

Een open source alternatief

De opkomst van wearable health devices is enorm. Door middel van smartapparaten meet je je beweging en vitale functie, waardoor ziektes soms eerder gevonden of voorkomen worden. Een knappe ontwikkeling die tegelijkertijd ook zorgt voor onduidelijkheid, want van wie zijn deze data? **Totem Open Health** biedt een open source alternatief, waarbij gebruikers zelf bepalen wat er met data gebeurt. De wearable die met behulp van SIDN fonds financiering ontwikkeld is, meet ECG en beweging.

Wouter Heijnen: "Door de bijdrage van SIDN fonds hebben wij een technologie ontwikkeld die een open source alternatief biedt. De zorg is een commerciële markt en in een commerciële markt kijk je hoe je een zo'n groot mogelijk project kunt maken. Grote techbedrijven houden gegevens bij van geboorte tot dood. Die data is van hen en niet van ziekenhuizen. Ook blijven de niche vragen liggen, terwijl deze juist interessant zijn. Er zijn al zoveel wearables, maar juist omdat wij vraagstukken oppakken die een ander laat liggen creëren we impact."

Goudmijn aan informatie

Gemiddeld krijgt één op de drie Nederlanders kanker. Lotgenoten zoeken steun bij elkaar op het internet. Internetplatforms en patiëntenfora zijn een goudmijn aan informatie, waar eigenlijk niks mee gedaan wordt. Het onderzoeksproject **Patiëntenplatform Miner** doet iets met deze waardevolle informatie door middel van kunstmatige intelligentie. Met behulp van zelf gegenereerde informatie van patiënten leveren ze zo een bijdrage aan de kwaliteit van leven van kankerpatiënten.

Gerard van Oortmerssen: "Het project is voortgekomen uit een concrete behoefte van patiënten, met name patiënten met een zeldzame vorm van kanker. Als zij de diagnose krijgen is er niemand in hun omgeving die iets soortgelijks heeft ervaren. Met kunstmatige intelligentie halen we waardevolle informatie uit al die fora en delen deze met patiënten, onderzoekers en specialisten. Ik ben SIDN fonds heel erg dankbaar. Zonder SIDN fonds hadden we het project niet op gang gekregen."

Feedback

"We vinden het bij SIDN fonds uitdagend om met zulke vernieuwende projecten te werken en zijn continu bezig met het verbeteren van onze service. Ik nodig stakeholders dan ook van harte uit om met ons in gesprek te gaan, alle feedback is welkom", aldus Valerie. ■



Om te groeien moet je alles weten van je klant

Dataprovider specialiseert zich in het indexeren en structureren van het internet. Daardoor weet Christian Branbergen, mede-oprichter van het bedrijf, precies hoeveel webwinkels actief zijn in een bepaalde regio, of welke domeinnamen in gebruik zijn. Dat is kennis waar klanten veel aan kunnen hebben.

Een burgemeester van een middelgrote stad hoeft maar een dagje rond te fietsen om een globaal beeld te krijgen van hoe de stad er voor staat. Welke wijken zijn toe aan een opknapbeurt? Waar is er leegstand? Waar gaan de kinderen huppelend naar school? Een registrar, een bedrijf dat domeinnamen registreert, heeft het lang zo makkelijk niet. Het internet is namelijk grotendeels onzichtbaar. Hoe hou je overzicht over alle domeinen? Dat doet Dataprovider, het bedrijf van Christian Branbergen en zijn compagnons. Elke website is een mini-databron op zich en Dataprovider houdt al die data bij. Kun je bij een webwinkel met creditcard betalen? Dan weet Dataprovider daarvan. Het bedrijf maakt samenvattingen van het internet. "Telefoonnummers zijn online een drama: iedereen schrijft ze op zijn eigen manier. Wij standaardiseren dat."

Klanten adviseren

Elk kwartaal analyseert Dataprovider voor SIDN de .nl-zonefile: waarvoor worden de .nl-domeinen eigenlijk gebruikt? Door wie? Waar worden ze gehost? Zijn ze überhaupt actief? Zo onderzoekt het bedrijf maandelijks zo'n 150 variabelen. SIDN kan de samenvattingen van Dataprovider gebruiken om klanten te adviseren. Christian: "Veel websites die persoonsgegevens opslaan passen bijvoorbeeld geen SSL-certificaat toe. Als ze daarnaast ook nog op oude besturings-software draaien, is de data onveilig. SIDN kan registrars daarop attenderen."

Crawler

Eigenlijk is het toeval dat Christian in deze branche is beland. Al op jonge leeftijd schreef hij software. Toen het internet groeide en SEO steeds belangrijker werd, maakte hij een crawler om te rapporteren of websites goed in elkaar zaten. Totdat een klant hem vroeg of hij niet kon uitzoeken welke webwinkels nog niet over een betalingsmechanisme beschikten. "Google

is een super zoekmachine", zegt Christian. "Maar Google kan niet alle webwinkels met één bepaalde betaalmethode voor je opzoeken. Wij wel."

Internetland

Meer dan tachtig procent van de klanten van Dataprovider bevindt zich in het buitenland. "Nederland is een echt internetland. Registrars zijn gewend dat de klanten vanzelf komen, maar het verzadigingspunt komt in zicht. Hoe meer je weet van je bestaande klant, hoe beter je hem kunt helpen. Grote Amerikaanse bedrijven sturen al heel exacte mailings. Een aanbieding voor shared hosting is bijvoorbeeld interessant voor websitebouwers, maar dan moet je wel weten wie van je klanten websites maken."

Toenemende internetcriminaliteit

Dataprovider verschuivingen op het internet bijhoudt, geeft inzicht in toekomstige trends. "Internetcriminaliteit neemt toe. Het gaat allang niet meer om spammails uit Nigeria. Criminelen zetten een eigen CMS op een verlopen domeinnaam, verkopen er zogenaamd Nike schoenen en proberen zo creditcardgegevens of e-mailadressen en wachtwoorden te bemachtigen. Op het eerste gezicht zie je niets gekks aan zo'n site, maar ik kan je wijzen op details die verraden dat je er beter niet kunt bestellen. Daar gaan we nog veel over horen."

Wachten op Amazon

Een ander inzicht: in Nederland zijn er zo'n 103.000 webwinkels. In Frankrijk, een land met een veel grotere economie, maar 79.000. Hoe komt dat? Waarschijnlijk omdat we in Nederland nog geen Amazon hebben. Een kwestie van tijd. Christian: "Als jij nu uitsluitend webwinkels maakt, zou je kunnen overwegen om ook iets anders te gaan doen." ■

"Er zijn 40.000 phishing sites in Nederland en 4.000 Nederlandse websites waarvan de titel begint met 'Hacked by'. Oeps!"

Christian Branbergen, Dataprovider

Diverse 'spelers' aan het woord



Erik Wellner

Realtime Register BV

"Ik ben gekomen om te netwerken, mede-registrars te ontmoeten en om geïnformeerd te worden door middel van de sessies. Dat is op alle punten geslaagd. Ethisch hacken was erg interessant, net als de sessie over het SIDN fonds. De medische projecten die zij ondersteunen spraken me erg aan. Daar zie ik heel veel toepassingen voor. Ik denk dat het een goede investering van het fonds is geweest." ■



Nique Sanders

Webtics

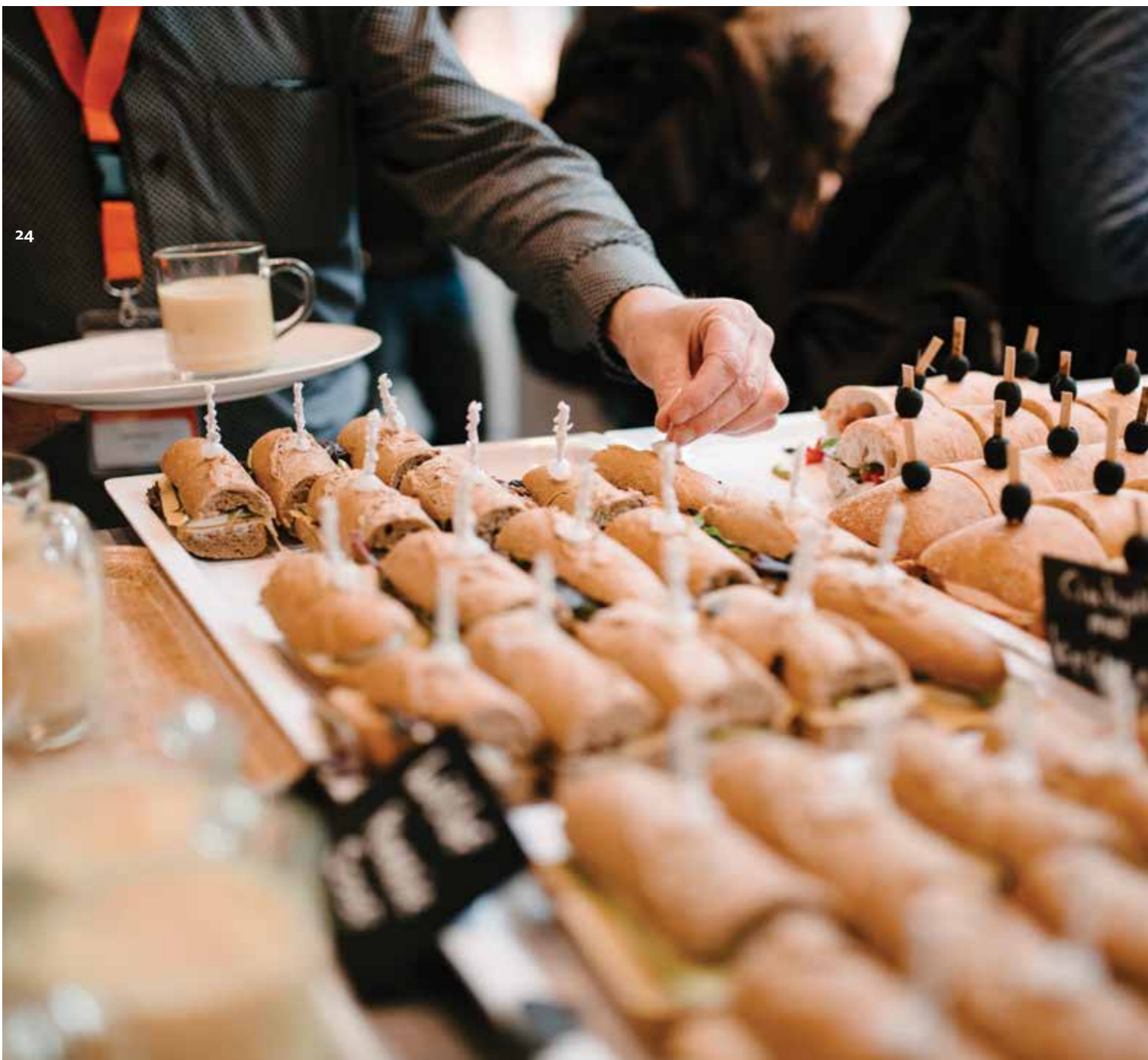
"Wij zijn registrar bij SIDN sinds 1995, maar dit is de eerste keer dat we zijn gekomen. We hadden interesse in een paar specifieke onderwerpen in het programma: big data, Moore's law en Future NL. Het was boven verwachting: leuke sprekers die heel veel kennis overbrachten. Ik ben ook te spreken over de interactie met andere bezoekers en de mensen van SIDN. We werken al heel lang met internet, maar nu treedt er een versnelling op: meer partijen, meer mogelijkheden, meer toepassingen, waardoor er maatschappelijke en economische veranderingen ontstaan. Dat merkte ik vandaag ook weer." ■



Teun van Eil

RB-media

"Dit is mijn eerste bezoek aan SIDN Connect. Ik ben betrokken bij IBT music, een blockchain-project voor de muziekindustrie dat subsidie heeft gekregen van het SIDN fonds. De presentatie van de hacker vond ik interessant, over hoe makkelijk je kunt inbreken op een computer, onder andere bij die van mezelf. Ik heb geleerd hoe je moeilijkere wachtwoorden maakt en dat je ze niet moet opslaan in een e-mail-map. Je denkt altijd dat je geen doelwit bent, totdat je het een keer wel bent." ■



SIDN LAGERHUIS

- ① SIDN MAG VOOR ABUSE BESTRIJDING
NOOIT OPSPOREN, BEORDELEN EN
 HANDHAVEN TEGELIJK UITVOEREN



- ② SIDN MOET DE .NL-ZONE
 BESCHIKBAAR MAKEN ALS
 OPEN DATA



Een lagerhuis met veel gelijkgestemden

Speciaal voor de registrars leidt dagvoorzitter Chris van het Hof het SIDN lagerhuis, waar zij pittige stellingen krijgen voorgelegd. De eerste is van Martijn Kamphuis, aantredend voorzitter van de Vereniging van Registrars (VvR): SIDN mag voor de bestrijding van abuse nooit en te nimmer alle drie de taken opsporing, beoordeling en handhaving tegelijk uitvoeren. Een meerderheid van de lagerhuisdeelnemers is het ermee eens. In principe zijn het onverenigbare taken. Degenen die kiezen voor 'oneens', beargumenteren dat de stelling te sterk is aangezet. "Op het moment dat politie weinig doet met een melding, is het te makkelijk om de verantwoordelijkheid bij een ander te blijven leggen. SIDN is eindverantwoordelijk voor het .nl-domein. Als het niet anders kan, moet SIDN in actie komen." Daar kan ook het eens-kamp zich in vinden.

Zonefile als open data

Stelling twee is afkomstig van Roland van Rijswijk, onderzoeker bij de Universiteit Twente. SIDN moet de .nl-zonefile beschikbaar maken als open data. Van Rijswijk licht toe dat hij werkt aan een groot onderzoeksproject, waarvoor hij voor heel veel domeinen dagelijks informatie moet opvragen. Dat komt onder andere ten gunste aan de veiligheid. Met een openbare zonefile kan iedereen diezelfde informatie opvragen. Op één na blijven alle registrars in het 'eens'-vak zitten. De ene tegenstemmer meent dat het voor onderzoek niet nodig is om de zonefile open te maken. De onderzoekers kunnen ook gewoon een lijst bij SIDN opvragen. Van Rijswijk werpt tegen: "Onderzoekers moeten reproduceerbaar onderzoek doen. Dat kunnen wij niet, omdat de data niet open zijn." Algemeen directeur Roelof Meijer laat weten dat SIDN van plan is om de zonefile beschikbaar te maken als open data. "De kracht van open maken is achteraf ontdekken wat mensen ermee doen. Maar ook voor misbruik van de zonefile geldt dat je niet alles van te voren kunt verzinnen. Daarom moeten we eerst goed onderzoeken wat er moet gebeuren."

Alle policies gelijktrekken?

Arjan Middelkoop, manager New business, Marketing & Sales bij SIDN, komt met de stelling: Om als hostingprovider te overleven in deze markt volstaat het niet meer om te focussen op een traditioneel portfolio van webhosting en domeinnamen, maar moet je waarde toevoegen vanuit een bredere propositie. Een meerderheid van de registrars kan zich daarin vinden. De drie tegenstanders geloven dat er een markt zal blijven bestaan voor hostingproviders.

Stelling vier: Er is behoefte aan standaardisatie in de policies en SIDN moet hierin het voortouw nemen, levert meer discussie op. Tegenstanders noemen het onhaalbaar om alle policies wereldwijd gelijk te trekken. Een voorstander noemt het "niet uit te leggen aan een registrant dat er overal andere policies gelden. Het zou het werk veel makkelijker maken." Een andere voorstander is er minder zeker van dat er een behoefte is aan standaardisatie, maar meent wel dat als gelijk getrokken moet worden, deze taak bij SIDN ligt. Roelof Meijer gelooft er niet erg in: "SIDN is bij wijze van spreken een kleine fabrikant van mobiele telefoons en nu moeten wij ervoor zorgen dat alle mobiele telefoons ter wereld hetzelfde snoertje hebben?"

Stellingen uit het publiek

Omdat er tijd over is, mag het publiek stellingen opperen. Met de stelling: Er moet een meldplicht komen voor registrars voor abuse op internet, is iedereen het eens. Op de vraag wie van de registrars alle meldingen doorgeeft aan eindgebruikers, zegt ongeveer de helft dit te doen. De rest kijkt liever eerst zelf. Stelling zes: Booters, websites die DDoS-aanvallen uitvoeren, moeten worden geblokkeerd. Ook hiermee is iedereen het eens. De laatste stelling uit het publiek luidt: Als een gebruiker zijn CMS niet updatet na een melding dat hij moet updaten en je ziet dat het wordt misbruikt, moet je als registrar de site uit de lucht kunnen halen. Tegenstemmers vinden dat er andere manieren zijn om misbruik te stoppen, en dat één melding te weinig is om tot actie over te gaan. Een meer commerciële oplossing is bijvoorbeeld om als webhoster de updates voor de klant voor je rekening te nemen. En dan is het tijd voor koffie. ■

Digital identities

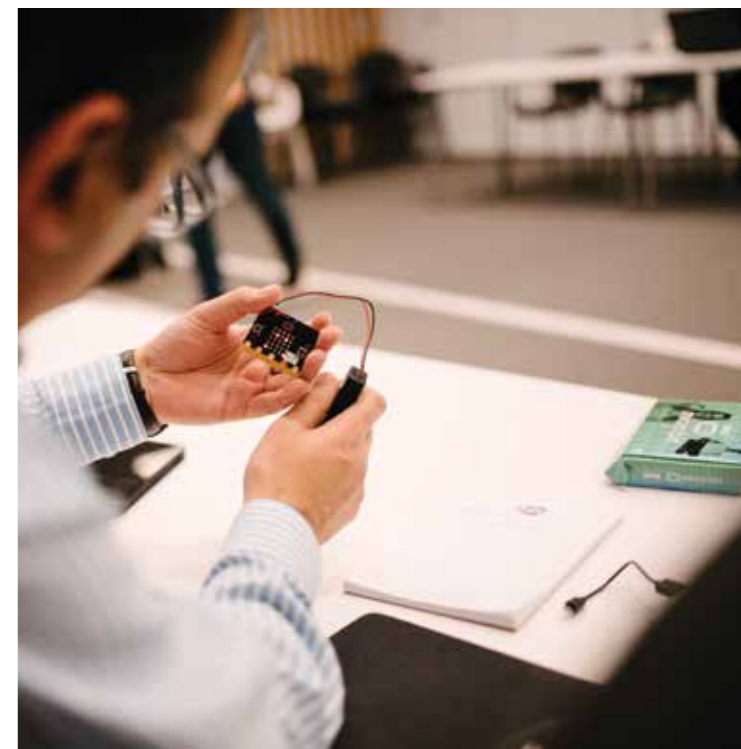
Esther Makaay, SIDN

Wat is een identiteit? Hoe kun je controleren of iemand ook echt is wie hij zegt dat hij is? Welke digitale identiteiten zijn er? Belangrijke vragen waar niet iedereen zich van bewust is en die niet enkel aan het domein digital identity gekoppeld zijn.

“Op een dag als vandaag is het belangrijk dat we van elkaar zien waar we mee bezig zijn. Je kunt onderwerpen als privacy, security en identity niet los van elkaar zien. Je kunt privacy niet goed regelen zonder over security na te denken. Digital identity gaat over de waarde van jouw data, maar ook alles wat je online doet. Dan heb je het eigenlijk over het internet.”

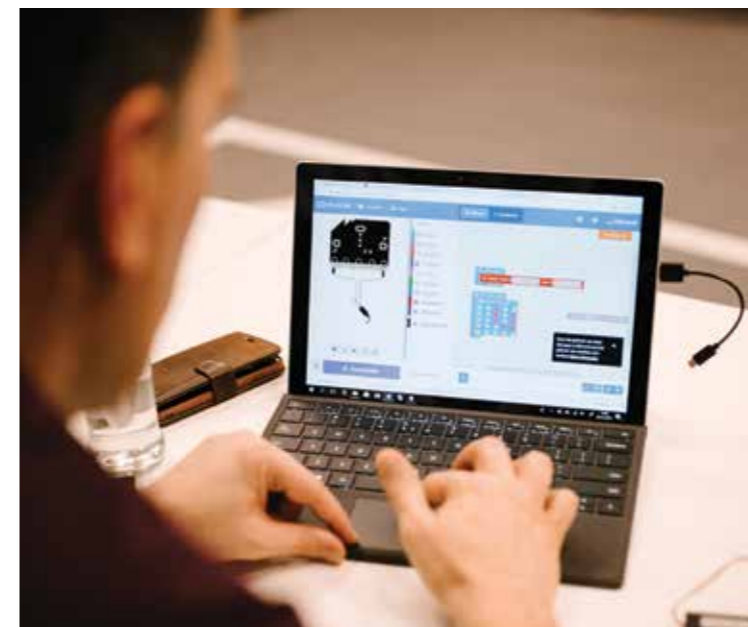


Workshops



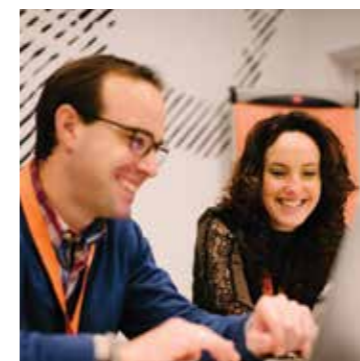
28

“Een identiteit kan heel sterk zijn, maar het hangt af van de context.”



29

“We hebben ook allemaal een identiteit vanuit onze werkgever, waarmee je toegang hebt tot ruimtes of systemen.”



Ga mee op Expeditie Micro:bit

Ronilla Snellen, Iris Muis & Jenya Krul, Future NL

De Micro:bit is een mini-computer ontwikkeld door BBC Education, waarmee basisschoolkinderen leren programmeren. Met hulp van het SIDN fonds heeft Stichting Future NL Nederlands lesmateriaal ontwikkeld, waardoor kinderen op Nederlandse basisscholen kennis kunnen maken met programmeren.

“Op de computer kunnen kinderen de Micro:bit programmeren door middel van het plaatsen van blokken of een echte code. Dat downloaden ze op hun Micro:bit, waardoor de code direct werkelijkheid wordt. Druk je op knopje A dan maakt de Micro:bit bijvoorbeeld een geluidje. Zo komen kinderen erachter hoe technologie werkt en ze leren op een laagdrempelige manier programmeren. Dat is allemaal onderdeel van computational thinking.”

Next Generation Internet

Marco Davids en Moritz Müller, *SIDN Labs*

IPv6 is essentieel voor het Next Generation Internet; een smarthome vol IoT heeft meer voordelen dan nadelen; centralisatie van het internet is een vanzelfsprekende ontwikkeling. Een kleine greep uit enkele stellingen waarover deelnemers van de interactieve Next Generation Internet workshop discussieerden.

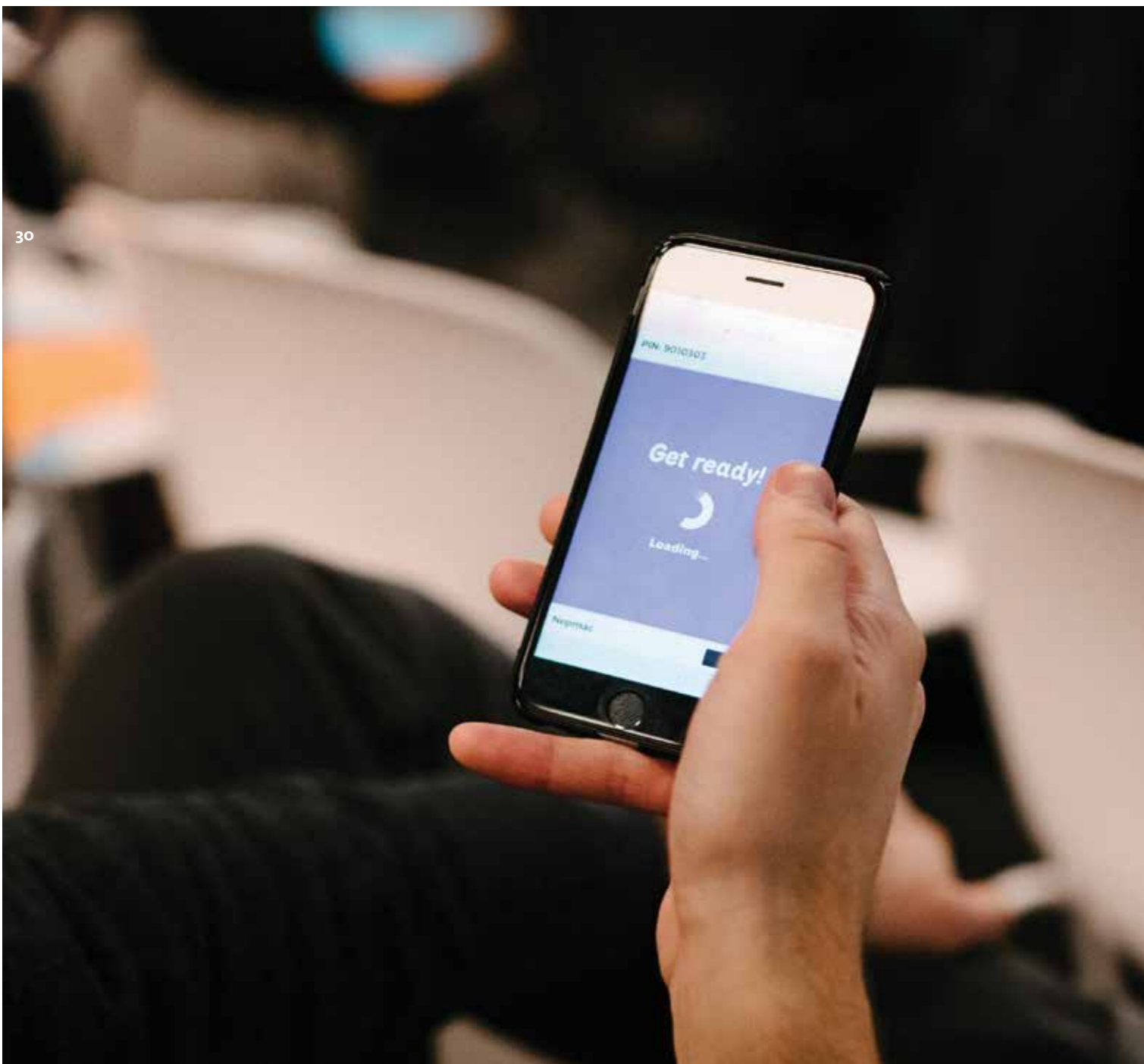
Moritz: "We hebben gezien dat mensen veel over de toekomst van internet nadenken. Het is iets wat leeft binnen alle domeinen en wordt bekeken vanuit diverse perspectieven zoals het business-, privacy- en securityperspectief. We hebben dingen voorbij horen komen, waar wij zelf van tevoren nog niet over nagedacht hadden."



Workshops



"Er zijn vier superbedrijven die alles wat wij doen overnemen. Ik denk dat dit de grootste bedreiging is van het internet in Europa."



30

"Een smarthome of smartcity gaan helpen bij het slimmer inzetten van energie."



31



"Moeten we wel vasthouden aan het huidige internet of moeten we het helemaal redesignen?"

Online advertenties op basis van je simkaart en je WhatsApp-gesprekken

Eduard Nandelall weet als geen ander hoe een boodschap de juiste mensen bereikt. Zijn bedrijf OptimusAd ontwerpt en beheert online reclamecampagnes. Hij bepaalt niet alleen wie wat te zien krijgt, maar vooral ook wie niet. Met die macht komt verantwoordelijkheid.

Drie zetels kreeg DENK als nieuwe partij bij de Tweede Kamerverkiezingen van 2017. Volgens Eduard Nandelall is dit succes voor een aanzienlijk deel op het conto van zijn bedrijf OptimusAd te schrijven. "Het grootste gedeelte van hun bescheiden budget ging naar ons", zegt hij. De Haagse ondernemer investeerde het in het gericht targetten van potentiële DENK-stemmers. "We adverteerden bijvoorbeeld alleen onder mensen die zich op WhatsApp positief uitlieten over DENK." Als je nu denkt: mag dat zomaar? Dat mag. Gebruikers van WhatsApp geven hiervoor toestemming door akkoord te gaan met de gebruikersovereenkomst en de data zijn geanonimiseerd.

Big data-analyse

"Together we change the world of advertising" is het motto van OptimusAd. Kijk je op televisie naar The Dog Whisperer, dan is de kans groot dat je op je tweede scherm een advertentie voor diergeneesmiddelen ziet langskomen. Daar zitten wij achter. Het is best mogelijk dat je die advertenties vaker ziet dan anderen, omdat je toevallig een Duitse herder in huis hebt. Dat komt dan omdat wij door middel van big data-analyse hebben vastgesteld dat eigenaren van Duitse herders hogere aankopen doen dan eigenaren van Afghaanse windhonden.

Kennisdeling

Eduard ontdekte de kracht van strategische marketing toen hij als entertainer op een cruiseschip werkte. "Passagiers in een dure suite kregen andere advertenties te zien op hun televisie dan mensen in een goedkopere suite. Dat zette me aan het denken. De online advertentiesector stond nog in de kinderschoenen, maar ik wist toen al dat de toekomst lag in big data." Zonder relevante opleiding of zelfs maar een middelbare-schooldiploma bouwde hij zijn eigen bedrijf uit tot een koploper in de branche. Hij is daarmee een uithangbord van zijn visie: met het internet zijn de mogelijkheden van kennisdeling ongekend groot geworden. Je kunt jezelf alles bijbrengen wat je wilt weten.

Ethische grenzen

Maar with great power comes great responsibility. Daar is hij zich terdege van bewust. Neem een ander voorbeeld uit de DENK-campagne: de doelgroep van de nieuwe partij bestaat voor een groot deel uit moslims. Moslims bellen relatief vaak met een simkaart van Lebara. Voor OptimusAd is het een fluitje van een cent om alleen Lebara-gebruikers te targetten. Dat betekent ook dat andere doelgroepen de online advertenties waarschijnlijk niet te zien krijgen. Je hoeft maar te denken aan de Russische inmenging in de Amerikaanse verkiezingen van 2016, om te weten hoe groot de invloed van online advertenties kan zijn. Eduard: "Hoe ver wil ik daar in gaan? Bijvoorbeeld wel adverteren op basis van woonplaats, maar niet op basis van etniciteit? Ik ben dan wel ondernemer, maar ik voel wel verantwoordelijkheid voor onze invloed op de politiek."

Naar een andere planeet

Liever helpt Eduard het internet naar een hoger plan te tillen. "Er is vanaf 1 januari 2017 tot nu toe meer data verzameld dan in de 100 jaar ervoor. Als de technologie zich exponentieel blijft ontwikkelen, maken we binnen nu en tien jaar zulke grote sprongen in kennisdeling. Allemaal dankzij big data. Dáár wil ik mijn bijdrage aan leveren." ■

"Ik ben van mening dat de beste tijden van het internet nog moeten komen."

Eduard Nandelall, OptimusAd



Scheidsrechter met passie

Waarom wordt iemand voetbalscheidsrechter? Je moet wel een hele dikke huid hebben om week na week de grofste scheldpartijen aan te horen. Ook na jaren ervaring vindt scheidsrechter Bas Nijhuis het niet leuk om beledigingen aan het adres van zijn moeder te ontvangen, of om in de Telegraaf te lezen dat hij er weer helemaal niks van heeft gebakken. Gelukkig staat er heel wat tegenover, zo maakt hij duidelijk in de afsluitende keynote. Passie, dat is het belangrijkste. Niks magischer dan een goed gevuld stadion binnenstappen voor de warm-up met je team. Samen fouten delen om er sterker van te worden. Blindelings op elkaar kunnen en moeten vertrouwen. Blijven innoveren: een scheidsrechter wordt steeds meer behangen met apparaten. Nijhuis draagt tijdens zijn werk een headset, een klokje dat gaat trillen als de bal over de lijn is, een sensor voor als de grensrechter vlagt, een spray om lijntjes te trekken en de mogelijkheid om via video een mogelijke overtreding direct terug te zien. "Iedereen vindt het prachtig, totdat de technologie spelers benadeelt. Dan komen ze protesteren."

Aan sociale media doet hij niet, sinds hij van 400 nieuwe vrienden tegelijk doodsb bedreigingen ontving. Met de traditionele media heeft hij een dubbele relatie. De ene week is hij een 'hangjas' (aldus Sjaak Swart), de week erop prijzen ze hem de hemel in. Nijhuis heeft er ondertussen handigheid in gekregen om de media te bespelen, vertelt hij met zichtbaar plezier. Zit hij bij Voetbal Inside, dan neemt hij oliebollen mee van zijn eigen bakkerij in Haaksbergen. "Betere reclame is er niet."

Uren kan hij doorgaan met het vertellen van anekdotes. Bijvoorbeeld over de keer dat een voetballer kwam klagen dat hij een penalty had moeten krijgen. "Voetballers worden chagrijnig als ze te lang niet scoren. Dan komen ze verhaal halen. Ik zeg: ik kan je wel een penalty geven, maar je schiet hem er toch niet in."

Mocht hij de scheidsrechtersfluit aan de wilgen hangen, dan kan Nijhuis zo de theaters in. Succes gegarandeerd. ■

"Iedereen vindt het prachtig, totdat de technologie spelers benadeelt."

Bas Nijhuis, Voetbalscheidsrechter



*De volgende
SIDN Connect is op
29 november 2018.
Zien we je dan
weer?*



Colofon

Met een team van creatieve professionals heeft Visuele Notulen voor de verslaglegging van dit evenement gezorgd.

Ontwerp

Lumen ontwerpersnetwerk, Breda

Tekst

Marjolein van Trigt & Yara Drissen

Fotografie

Michèle Giebing

Illustraties

Rob van Barneveld

Opmaak en lay out

Visuele Notulen

Drukwerk

NPN drukkers, Breda

38



visuele notulen

Lumen ontwerpersnetwerk



NPN
DRUKKERS



SIDN

Postbus 5022

6802 EA Arnhem

Meander 501

6825 MD Arnhem

T +31 (0)26 352 55 00

support@sidn.nl

www.sidn.nl