Met de ISOC.nl Innovatie Award wil Internet Society Nederland vernieuwende en belangwekkende initiatieven rondom internet de erkenning geven die ze verdienen. Innovaties, die een stimulans betekenen voor de groei van en kennis over het internet. De prijs wordt uitgereikt aan personen, instellingen of initiatieven en is een teken van grote maatschappelijke waardering voor prestaties ter verbetering van het internet en het gebruik ervan.

Genomineerden

De genomineerden voor 2019 zijn:

Elvis/Map me tender - Tenders Exposed
Settled - IBT Music
IRMA - Privacy by Design foundation
Make Media Great Again - BEMA
My Data Done Right - Bits of Freedom
OpenIntel - Universiteit van Twente
PoliFLW - Open State Foundation
Publicroam - Publicroam BV
SimplyEdit - Muze BV
SPIN - SIDN Labs

Ooit gehoord van openbare aanbestedingen? Tenders? Overheidsuitgaven? Het is wat uw overheid doet met uw hard verdiende belastingcenten. Bedrijven worden gehuurd om van alles voor ons te doen: wegen en gebouwen bouwen, comfortabele bureaustoelen voor de ministeries leveren, of catering voor openbare scholen verzorgen. Veel data over overheidsuitgaven zijn open. Maar de overheid geeft ook heel veel geld uit en de hoeveelheid data is zo (voor niet-dataanalysten) enorm. Om bijvoorbeeld de overheidsuitgaven van Frankrijk te onderzoeken, moet u ongeveer 2 miljoen aanbestedingen induiken. Bovendien kennen aanbestedingen veel technische processen: gunningsprocedures, gunningscriteria, sectorcodes, concurrentie, ... de lijst gaat door. Met ons project willen we aantonen dat het allemaal minder ingewikkeld dan het lijkt.

Tenders Exposed is een project met een missie om kennis en data over openbare aanbestedingen toegankelijk te maken voor iedereen. In overeenstemming met ons motto: “Public spending is fun!” willen we de procedures en data over aanbestedingen transparant en begrijpelijk maken voor journalisten, NGO’s en de geïnteresseerde burger. Want dé manier om iets te verbergen is om het groot en ingewikkeld te maken. Met onze tool Elvis (map me tender) visualiseren we tender data als netwerken van overheden en bedrijven. Deze visualisaties helpen journalisten om met weinig moeite duizenden gegunde opdrachten te filteren en onderzoeken. Daarnaast schrijven we op onze verse Medium blog over mechanismes in openbare aanbestedingen die we met data analyse illustreren. We willen zo aandacht creëren voor trends in de aanbestedingsmarkten van de EU en bijdragen aan de discussie over efficiëntie, competitie en corruptie in de overheidsuitgaven.

Naast ons eigen werk ondersteunen we ook werk van andere professionals. Uit fondsen die we in het geleden hebben geworven konden we drie projecten financieren die aanbestedingsmarkt in de EU onderzoeken. Reeds gepubliceerd is een artikel die de ‘gunningscriteria’ van tenders voor bosbeheer in Tsjechië onder de loep neemt. Het bedrijf die voor Tsjechische bossen zorgt heeft deze opdracht namelijk gewonnen onder de ‘laagste prijs’ criteria. Dit had als gevolg dat deze zorg verwaarloost was. We werken ook samen met andere professionals, bijvoorbeeld met academici rondom het Government Transparency Institute en opentender.eu.

Ons team bestaat uit vijf leden: Adriana Homolova (data journalist in Nederland), Victor Nițu (developer in Roemenie), Georgiana Bere (developer in Roemenie), Ioana Cristea (developer in Roemenie) en Matej Chudada (designer in Slowakije).

In de toekomst blijven we onze koers houden. We willen dat Elvis snel alle EU aanbestedingen in zijn database heeft, want op dit moment bevat die wegens technische beperkingen alleen de Oost-Europese landen. We gaan van Tenders Exposed een stichting maken. We blijven met journalisten en andere professionals samenwerken en samen ervoor zorgen dat het alleen interessanter en leuker wordt om het wereld van openbare aanbestedingen in te duiken.

Transparantie in de muziekindustrie dankzij blockchain-technologie

De muziekindustrie staat bekend als een harde wereld. Het is niet vanzelfsprekend dat je je brood kunt verdienen met muziek maken en helemaal niet voor jonge artiesten. De industrie wordt gekenmerkt door haar ingewikkelde, bureaucratische structuur. Een structuur waarin artiesten maanden moeten wachten op uitbetaling van royalty's, waarin complexe contracten onvermijdelijk lijken en transparantie niet lijkt te bestaan. Dat moet toch anders? Volgens de initiatiefnemers van IBT Music kan dat. Teun van Eil, projectleider van het initiatief, legt uit hoe hun geautomatiseerde blockchain-systeem het verschil kan maken en transparantie brengt in de muziekindustrie.

In het huidige systeem zijn de regelingen rondom muziekrechten niet transparant. Dit werkt vooral in het nadeel van de jonge artiest. Want hoe treed je toe tot die muziekwereld zonder een contract bij een groot platenlabel? Om met muziek je brood te verdienen word je hier haast toe gedwongen. Dit gebeurde ook met Martin Garrix. De jonge dj sloot aan het begin van zijn carrière een contract af zodat hij zich volledig kon richten op muziek. Garrix kreeg een vast maandsalaris van het platenlabel in ruil voor de rechten van zijn nummers. Een aantrekkelijk contract voor een beginnend artiest, maar schijn bedriegt. Ook al krijgt een artiest als Garrix meer bekendheid, het contract blijft staan. Dat betekent dat niet de artiest, maar het label hiervan profiteert. En kom maar eens van dat systeem af.

Dan hebben we het nog niet gehad over de uitbetaling van het aantal streams (de keren dat een nummer of video online wordt afgespeeld). Door het handmatige administratieve werk duurt het soms wel 9 maanden tot een artiest uitbetaald krijgt. Digital Service Providers (DSP's), zoals Spotify, Apple Music en VEVO, sturen de informatie uit hun systeem naar Buma/Stemra; belangenbehartiger voor componisten, tekstdichters en muziekuitgevers op het gebied van muziekauteursrecht. Buma/Stemra print dit uit en neemt het handmatig over in hun eigen systeem. Een tijdrovend proces, waardoor Buma/Stemra niet kan uitbetalen aan artiesten met minder dan 50.000 streams per nummer. Hierdoor wordt het probleem van deze partijen het probleem van de (beginnende) artiest.

Transparantie is de sleutel
IBT Music is een geautomatiseerd systeem dat hier verandering in brengt. Met het systeem kunnen artiesten zelf *smart contracts* opstellen en deze als basis gebruiken voor uitbetaling door DSP's en platenlabels. Hierdoor kan geld ook sneller uitbetaald worden – binnen 1 dag in plaats van 9 maanden – en hoeven artiesten niet meer te vragen om een basisinkomen."

IBT Music bestaat uit 2 systemen: Rightsshare (http://rightsshare.com/) en Settled (https://www.settled.world/). Rightsshare is het programma waarmee het label of de artiest daadwerkelijk werkt. Settled is het blockchain-systeem daarachter; een open systeem waardoor je ook andere toepassingen aan je blockchain-technologie kunt koppelen zoals het afsluiten van contracten en het uitbetalen van royalty's.

Het systeem is zo gebouwd dat je met Rightsshare niet alleen kunt aansluiten bij Settled, maar ook bij andere blockchains. "Settled is een rails die wij gebouwd hebben en Rightsshare is de eerste locomotief op die rails. Maar er zijn ook andere partijen die rails en locomotieven gebouwd hebben. Wij willen met onze locomotief ook op die rails kunnen rijden en zij mogen met hun locomotieven op onze rails rijden."

Hoe werkt het precies?
Een mooi idee, maar hoe werkt het dan precies? Een artiest produceert een nummer. Het platenlabel registreert dit nummer via Rightsshare (of een concurrent daarvan) en zorgt ervoor dat het muziekstuk gedistribueerd wordt. Via Settled wordt een unieke cijferlettercombinatie aan het nummer gekoppeld. Deze registratie wordt gebruikt om het nummer bij DSP's onder te brengen. DSP's kunnen met die code precies nagaan waar het nummer in de blockchain geregistreerd staat. Alle streams per DSP koppelt het blockchain-systeem automatisch aan het specifieke nummer. Doordat de blockchain transparant en open is, kan de artiest zelf ook zien hoe vaak het nummer bij de verschillende DSP's gestreamd is. Zo kan de artiest zelf uitrekenen wat hij of zij aan royalty's – vergoeding volgens de overeenkomst met het label – hoort te ontvangen. Teun: "In het begin zal het nog zo zijn dat DSP's het geld naar platenmaatschappijen overmaken en dat zij het overmaken naar de artiesten. Later zou dit van de DSP's direct naar de artiesten kunnen."

IRMA two-pager, voor ISOC innovatieprijs 2019.

b.jacobs@privacybydesign.foundation

IRMA is een attribuut-gebaseerd identiteitsplatform voor authenticatie en digitale ondertekening. Gebruikers kunnen de IRMA app vanuit de standaard app stores downloaden en vullen met eigen identiteitsgegevens, en zo een persoonlijk paspoort (eID) samenstellen op hun eigen mobiele telefoon. Deze identeitsgegevens heten *attributen*: korte stukjes persoonsinformatie, over adres, geslacht, email adres, telefoonnummer, bankrekeningnummer, burgerservicenummer (BSN), wel/niet boven 12/16/18/65, medische beroep (en BIG registratienummer), diploma's etc. Deze attributen kunnen op een privacy-vriendelijke manier selectief getoond worden. Bijv. om online een bepaalde game te spelen is het voldoende als je kunt aantonen dat je boven de 16 bent. En bij het online kopen van een boek is het voldoende als je toont wat je adres is (voor bezorging) en wat je bankrekeningnummer is (voor betaling), en verder niks. Aldus is data-minimalisatie een intrinsiek onderdeel van IRMA. Bovendien kun je met IRMA ook digitale handtekeningen zetten op documenten, zodat een bijv. een recept getekend wordt door iemand die aantoonbaar arts is. Dit draagt bij aan vertrouwen in de digitale infrastructuur en samenleving.

IRMA is voortgekomen uit de Digital Security groep olv. Bart Jacobs aan de Radboud Universiteit. Sinds twee jaar werkt de hieruit voortgekomen onafhankelijke stichting *Privacy by Design* (privacybydesign.foundation) aan de uitrol van IRMA, zonder winstoogmerk, met open source software, en zonder kosten voor gebruikers. IRMA is gebaseerd op geavanceerde cryptografie (waaronder *zero-knowledge proofs*) waardoor de herkomst en betrouwbaarheid van attributen gegarandeerd wordt.

IRMA onderscheidt zich op de volgende drie fronten.

1. Het IRMA platform is gebaseerd op superieure (cryptografische) techniek, voor zowel authenticatie als voor digitale ondertekening, waarin zowel privacy-by-design als ook security-by-design leidend zijn. IRMA gebruikt een decentrale architectuur, waardoor attributen alleen op de telefoon van de gebruiker opgeslagen worden.

2. IRMA is inmiddels aangesloten op belangrijke bronnen van persoonsgegevens, zoals de basisregistratie personen (BRP) van de overheid, iDIN en iDEAL voor gegevens van banken, BIG en AGB gegevens voor de

medische sector, diploma's vanuit DUO, registratie- en email-gegevens van het hoger onderwijs via SURFconext, enz. Vooral de aansluiting IRMA-BRP is van strategisch belang, waarbij burger een twintigtal attributen (waaronder BSN) vanuit overheidsregisters in hun IRMA-app kunnen laden. De beschikbaarheid van het BSN in de IRMA app leidt tot een doorbraak in de zorg, m.n. m.b.t. het inloggen op en vullen van persoonlijke gezondheidsomgevingen (PGOs). Geen enkel ander eID middel kan zoveel attributen leveren als IRMA.

3. IRMA leidt tot geheel nieuwe applicaties, zoals het nieuwe zorgportaal Helder waarop zorgprofessionals exclusief met een medisch IRMA-attribuut inloggen, of de nieuwe manier van machtiging die zorgverzeker VGZ met een IRMA attribuut realiseert. Naar verwachting zal het daadwerkelijke gebruik van IRMA in 2019 sterk groeien.

Alle bestaande elektronische identiteiten zijn gebaseerd op unieke identificatie, via een centrale organisatie waar alle persoonsgegevens staan. Als je bijv. via Facebook Login op de webpagina van een krant in wil loggen, wordt je eerst doorgestuurd naar Facebook en moet je daar inloggen; vervolgens vertelt Facebook aan de krant wie je bent. Facebook heeft dit zo ingericht om bij te kunnen houden wie waar in logt, en om zo nog rijkere profielen op te kunnen bouwen. DigiD van de overheid en iDIN van de banken werken met dezelfde privacy-onvriendelijke centrale architectuur.

IRMA daarentegen heeft een *decentrale* architectuur: attributen staan alleen op de telefoon van de gebruiker, waardoor er bij het inloggen bij een krant alleen communicatie plaats hoeft te vinden tussen de krant en de gebruiker; er is dus geen derde partij — zelfs niet de stichting achter IRMA — die bij kan houden wie waar op welk moment inlogt.

Het decentrale attributen-model van IRMA beschermt niet alleen de privacy maar leidt ook tot innovaties die voorheen onmogelijk waren. Webwinkels hebben jarenlang aan de overheid toegang tot de BRP gevraagd, voor het controleren van adressen bij bezorging. De overheid heeft dat altijd (terecht) geweigerd. De overheid is wel bereid om BRP-gegevens aan de burger zelf te geven — in de IRMA app — voor regie over hun eigen gegevens. Vervolgens kan een webwinkel aan burgers vragen om die (adres)gegevens te mogen zien. Dit decentrale model geeft de gebruiker inzage en controle, leidt tot data-minimalisatie, en past meer in het algemeen uitstekend binnen de kaders van de Algemene Verordening Gegevensbescherming (AVG).

Tekst voor Isoc Award nominatie Make Media Great Again

Wat is het uitgangspunt?

Het internet heeft geweldige vernieuwingen teweeg gebracht in alle geledingen van de samenleving dankzij de kracht van gedistribueerde communicatie. Echter, in de communicatie tussen lezers en media beperkt de feedback zich veelal tot reacties op de inhoud (‘reaguren’). MMGA biedt een transparant systeem en constructieve methode om redactie te verbeteren met inbreng van een panel van lezers, kijkers en/of luisteraars. NU.nl is de eerste test-partner.

Wat is het precies?

MMGA biedt een systeem van annoteren: het maken van kanttekeningen bij teksten – later ook bij video en audio. Met een redactie, zoals bij NU.nl selecteert, instrueert en begeleid MMGA kristische & deskundige lezers die vervolgens met een zelf ontwikkelde browser plug-in commentaar leveren. Ze doen dat in de vorm van gecategoriseerde bondige suggesties voor verbetering van met name brongebruik, maar ook taal en informatievoorziening. Vervolgens reageren (eind)redacteuren via dezelfde tool op de suggesties: ze verwerken de suggesties nu dan wel later, of wijzen die af. Dit kan op de achtergrond draaien, of zichtbaar voor bezoekers, of op een openbare website zoals een forum.

Wat zijn de betekenis en invloed?

Met MMGA is er na 25 jaar publieksinternet voor het eerst een methode beschikbaar waarmee internetters kunnen interacteren met hun eigen media om bij te dragen aan kwaliteitsverbetering. MMGA zal daarmee op termijn een flinke omslag teweeg brengen in de transparantie en betrouwbaarheid van mediaproductie op internet. Ineens krijgen journalisten en andere makers daadwerkelijk en structureel hulp van hun publiek.

Wie zijn de mensen erachter?

MMGA is opgezet door Ruben Brave (sociaal ondernemer inzake internet & media) samen met Adriaan Stoop (commissaris NRC & advocaat) en Kees van Mourik (ICT-ondernemer). Zij doen dat vanuit de door Stoop opgerichte de Stichting Bema in Amsterdam die zich inzet voor een vergroting van de mediabetrouwbaarheid met ondermeer de jaarlijkse uitreiking van European Press Prize, in samenwerking met ondermeer The Guardian. Een internationaal team van jonge technici bouwde de plug-in en een dashboard voor uitgevers en hoofdredacties. Journalist Peter Olsthoorn, onder andere bekend van Leugens.nl, begeleidde het annoteren.

Wat zijn de toekomstplannen?

Tweeledig: MMGA wil na NU.nl meer media gaan bijstaan voor kwaliteitsverbetering van informatievoorziening, maar ook instellingen en overheden zoals bijvoorbeeld gemeenten, musea. Ook zal MMGA in 2019 een openbare website beginnen waarop annotatie van artikelen, en later van video en audio zal plaatsvinden; dit alles gericht op kwalitatief betere journalistiek en informatievoorziening en daarmee meer vertrouwen.

Meer info: zie www.mmga.io

My Data Done Right

Wat is het precies?

My Data Done Right helpt internetgebruikers om meer grip te krijgen op hun data. Het bestaat uit een responsive website die gebruikers helpt bij het uitoefenen van hun rechten uit de Algemene Verordening Gegevensbescherming. In een paar eenvoudige stappen kunnen gebruikers een organisatie selecteren en een inzage-, correctie- of verwijderingsverzoek opstellen.

De tool is ontworpen vanuit het principe van dataminimalisatie: alle persoonlijke gegevens die gebruikers tijdens het genereren van een verzoek verstrekken, worden lokaal en tijdelijk in de browser van de gebruiker zelf opgeslagen. De database van My Data Done Right bevat momenteel de contactinformatie van 1253 organisaties. De website is beschikbaar in het Nederlands en Engels. De website is zodanig opgezet dat we eenvoudig met andere organisaties My Data Done Right kunnen uitrollen in andere landen binnen de Europese Unie.

Wat is de impact?

De lancering van My Data Done Right in Nederland was op 25 oktober 2018 en heeft veel aandacht gekregen in de landelijke media, waaronder: RTL Z, BNR Zakendoen, Een Vandaag, Tweakers, en Radar. Ook andere online persuitingen zoals online bij de NOS of Engadget verwijzen naar My Data Done Right.

De website is in de periode sinds de lancering tot en met 3 januari 2019 door 18.036 bezoekers bezocht. In die periode is er 14.585 keer gekozen om een verzoek of reminder te genereren, waarvan 11.995 keer is gekozen voor een inzageverzoek.

Wie zijn de mensen erachter?

De projectcoördinatie was in handen van David Korteweg (beleidsadviseur en jurist). Daarnaast waren binnen de organisatie Karim Khamis (ontwerper), Evelyn Austin (bewegingbouwer), Imre Jonk (systeembeheerder) en Hans de Zwart (directeur) betrokken bij de realisatie en plannen voor de internationale uitrol van My Data Done Right. Verder waren binnen de organisatie de stagiaire Mary DuBard en Aleksandar Todorović (Mozilla Open Web Fellow) betrokken bij de ontwikkeling van de tool. Bijna 30 vrijwilligers hielpen met het vullen van de database. Het ontwerp van de website is van de externe ontwerper Ruben Doornweerd en de backend en frontend is ontwikkeld door de externe developer Jean Jacques Warmerdam.

Wat zijn de toekomstplannen?

In 2019 richten we ons op de internationale uitrol van My Data Done Right en het onderhoud en de verbetering van de tool. Voor het onderhoud van de Nederlandse database zijn inmiddels vrijwilligers geworven. Voor de internationale uitrol hebben we financiering ontvangen van RIPE NCC en is een plan opgesteld hoe we dit gaan aanpakken. Er is inmiddels ook al contact met enkele buitenlandse organisaties. Voor het (technisch) verbeteren van de website zullen we vrijwilligers werven uit onze achterban.

OpenINTEL bouwt een uniek breedomvattend beeld van de belangrijkste delen van het internet. Dit doen we door dagelijks een snapshot te maken van de toestand van meer dan 60% van het wereldwijde Domain Name System. Op dit moment omvat onze meting zo'n 216 miljoen domeinnamen.

Dit maakt baanbrekend onderzoek mogelijk waarbij de ontwikkeling van het wereldwijde internet wordt blootgelegd, en waarbij de veiligheid van het internet wordt verbeterd, bijvoorbeeld door de effecten van DDoS aanvallen in beeld te brengen en bij de bestrijding van hardnekkige vormen van spam e-mail en andere vormen van fraude. Doordat OpenINTEL actief het internet meet, kunnen we bovendien pro-actief de beveiliging verbeteren, en dus zaken als spam, phishing en DDoS aanpakken voordat ze een probleem worden, en niet - zoals nu gebeurt - reactief, nadat het probleem zich al heeft voorgedaan.

Waar OpenINTEL op de korte termijn direct ingezet kan worden om het internet veiliger te maken, kan het op de lange termijn dienen als het "geweten van het internet". Een belangrijk doel van OpenINTEL is dat onderzoekers in 2025 de vraag kunnen stellen: hoe zag het internet er 10 jaar geleden uit? Wat is er in de tussenliggende tijd gebeurd en veranderd? Wat betekent dat voor ons? Met de gedachte in het achterhoofd hoe radicaal het internet sinds de grootschalige opkomst in de jaren 90 veranderd is, is zo'n langetermijnbeeld van onschatbare waarde voor toekomstig onderzoek.

Wat is de impact?

Op basis van de data die OpenINTEL dagelijks verzamelt zijn inmiddels meer dan 20 wetenschappelijke papers gepubliceerd, de meeste daarvan in toonaangevende journals en conferenties. Deze papers zijn niet alleen geschreven door de mensen achter OpenINTEL, maar in samenwerking met universiteiten van over de hele wereld (o.a. uit de VS, Duitsland, Brazilië en Australië). Een aantal publicaties heeft bijzondere aandacht gekregen, waaronder een best paper award (NOMS 2018) en een Applied Networking Research Prize van de IRTF (https://irtf.org/anrp).

Naast wetenschappelijke impact heeft OpenINTEL ook maatschappelijke impact; zo is data van OpenINTEL in het verleden gebruikt voor het nationale cyberdreigingsbeeld van het NCSC en is OpenINTEL data gebruikt in een recent rapport van het CPB over de bedreiging die DDoS aanvallen vormen voor de samenleving.

Wat zijn de plannen voor de toekomst?

Op dit moment zijn we bezig met het opbouwen van een nieuwe meetomgeving voor OpenINTEL. Zodra die operationeel is gaan we een aantal nieuwe features toevoegen aan onze metingen, waarbij we onder andere ook de performance van het wereldwijde DNS kunnen doormeten en een beter inzicht krijgen in de stabiliteit van het DNS. In december is er een promovendus gestart in onze onderzoeksgroep die zich daar de komende vier jaar op gaat focusen in nauwe samenwerking met CAIDA (https://caida.org/), een onafhankelijke onderzoeksgroep aan de University of California San Diego.

Een ander belangrijk doel dat we in 2019 nastreven is om nog meer van onze gegevens als open data beschikbaar te maken voor andere onderzoekers. Daarnaast doen we op dit moment een project met 5 groepen van de opleiding Media en Communicatie aan de Hogeschool van Amsterdam om mooie visualisaties van OpenINTEL data te maken die de maatschappelijke discussies rondom de centralisering van het internet in de handen van een aantal grote partijen (zoals Google, Facebook, ...) aan moet jagen op basis van hoe het internet zich over de afgelopen 3,5 jaar heeft ontwikkeld.

Voor specifieke voorbeelden van papers op basis van OpenINTEL verwijs ik graag naar onze website, https://openintel.nl/, waar alle papers op basis van OpenINTEL als open access beschikbaar zijn.

Wie zijn de mensen?

Het kernteam van OpenINTEL bestaat uit de volgende onderzoekers in de Design and Analysis of Communication Systems onderzoeksgroep aan de Universiteit Twente:

- Anna Sperotto
- Roland van Rijswijk-Deij
- Mattijs Jonker
- Olivier van der Toorn

Voor een volledig overzicht van de mensen die hebben bijgedragen aan OpenINTEL, zie https://openintel.nl/team/
OpenINTEL is een samenwerking van vier partners: de Universiteit Twente, SURFnet, SIDN Labs en NLnet Labs.

PoliFLW van Open State Foundation

Door: Tom Kunzler, Open State Foundation (2 januari 2019)

Wat is PoliFLW?
Het is voor journalisten, belangenbehartigers en actieve bewoners niet altijd makkelijk om op de hoogte te blijven van politiek nieuws. Om dit makkelijker te maken heeft Open State Foundation PoliFLW gebouwd. Via PoliFLW.nl is nieuws van Nederlandse politieke partijen te volgen: van SP Maastricht tot VVD Groningen. Met behulp van scraping verzameld PoliFLW alle nieuwsberichten die politieke partijen op hun websites en Facebook-pagina's plaatsen.

De nieuwsberichten worden met behulp van machine-learning geordend. Zo worden de nieuwsberichten gekoppeld aan politieke partijen, namen van politici, thema, objectiviteit en polariteit. Gebruikers kunnen daarnaast aangeven of deze door machine-learning toegekende labels kloppen en hiermee wordt het algoritme verbeterd. Dankzij de labeling wordt het eenvoudiger om de bijna 600.000 nieuwsberichten te doorzoeken. Het is sinds kort ook mogelijk om mail-notificaties in te stellen voor bepaalde zoekopdrachten.

De nieuwsberichten die verzameld zijn binnen PoliFLW zijn ook volledig beschikbaar als open data middels een API. Hiermee kan eenieder de data naar eigen inzicht voor nieuwe toepassingen inzetten. PoliFLW is en blijft volledig gratis beschikbaar.

Wat zijn de toekomstplannen voor PoliFLW.nl?
Momenteel zitten in PoliFLW alleen partijen die landelijk opereren. Dit komt omdat de websites van deze partijen er in alle gemeenten hetzelfde uitzien en eenvoudig te scrapen zijn. Lokale politieke partijen hebben allemaal een andere website, wat scrapen complex maakt. Open State werkt momenteel aan een universele scraper die automatisch nieuws van websites van lokale politieke partijen detecteert. Hierdoor zijn binnenkort alle politieke partijen in PoliFLW vertegenwoordigd.

Daarnaast werkt Open State aan een almanak met alle overheden en politici. Almanak.overheid.nl, de officiële overheidsalmanak, is namelijk niet volledig en niet actueel. Door een volledige en actuele All-Manak te bouwen kunnen PoliFLW-berichten binnenkort gekoppeld worden aan een volledige lijst van politici. Daarnaast sturen we de aanvullingen terug naar almanak.overheid.nl.

Wat is de impact?
Er zijn diverse journalisten, dataservices en public-affairs organisaties die gebruik maken van de website of de data achter PoliFLW. Gecombineerd met de data van andere Open State projecten als Open Raadsinformatie en Open Stateninformatie geeft dit een volledig beeld van het handelen van politieke vertegenwoordigers op alle niveaus. Dit maakt het werk van een journalist, die te kampen heeft met krimpende budgetten, eenvoudiger en helpt mee om participatie en belangenbehartiging laagdrempeliger te maken.

Wie zit er achter PoliFLW?
PoliFLW is ontwikkeld door Open State Foundation, een onafhankelijke stichting die zich inzet voor digitale transparantie. Open State richt zich op het bevorderen en ontsluiten van open data over verkiezingen, besluitvorming, geldstromen en prestaties van de publieke sector. PoliFLW wordt in verschillende fases ontwikkeld. De website is gebouwd met steun van het DNI Fund en wordt verder ontwikkeld met budget van het SIDN Fonds.

Poliflw

Home Over API Feedback Contact

Poliflw

Lokaal politiek nieuws inzichtelijk

Zoek PGB

Gebruik bovenstaand zoekveld om door 593062 berichten te zoeken op thema ...

Of zoek naar een locatie:

Amsterdam

Poliflw

Een initiatief van:

DIGITAL NEWS INITIATIVE SIDNfonds

Zoek milieuzone

0 Verificaties vandaag door jou gegeven!

10 Verificaties totaal door jou gegeven!

1645 Verificaties totaal door community gegeven!

GROENLINKS

Er waait een groene wind door de begroting | Arnhem

GroenLinks VVD D66 Partij voor de Dieren PvdA Arnhem

14-11-2018 00:00

Verandering begint écht in Arnhem. De afgelopen weken heeft de gemeenteraad het uitgebreid gehad over hoe we het geld in Arnhem gaan verdelen. Dit leggen we vast in de zogenaamde MJPB, de meerjarenprogrammabegroting. De MJPB is dus erg belangrijk voor de richting van het beleid van de gemeente. We hebben het groenste en sociaalste coalitieakkoord ooit. We zetten ook grote stappen met deze begroting. Fractievoorzitter Mark Coenders voerde woensdag 14 november namens GroenLinks het woord tijdens de algemene beschouwingen.

Wordt Dhr. M.W.K. (Mark) Coenders van GroenLinks, Raadslid in Arnhem hier genoemd?

JA NEE WEET IK NIET

"Voorzitter

Zoek milieuzone

0 Verificaties vandaag door jou gegeven!

10 Verificaties totaal door jou gegeven!

1645 Verificaties totaal door community gegeven!

publicroam
eenmaal aanmelden, overal veilig online

Beschrijving voor ISOC Innovatie Award

PUBLICROAM is een nieuw initiatief om iedereen veilig en makkelijk toegang te geven tot gastwifi. Iemand vraagt één keer, per SMS of via de website, een gratis publicroam-account aan. Hij of zij ontvangt per SMS een username en password, activeert het account en gaat daarna automatisch online, bij alle deelnemende organisaties. Direct, zonder steeds opnieuw aan te melden. Publicroam is een eenvoudige toevoeging aan de bestaande wifi-infrastructuur van organisaties, als extra authenticatievoorziening. Het zorgt voor een veilige verbinding tussen de devices van bezoekers en de wifi-accesspoints van de gastorganisatie op basis van WPA2-Enterprise.

Werking - Als een bezoeker bij een organisatie komt die publicroam aanbiedt, maakt zijn device automatisch contact. Username en password worden naar de publicroam-server verstuurd en daar wordt controleerd of iemand recht heeft op toegang tot het gastwifi. Als het antwoord 'ja' is, dan komt er automatisch een veilige verbinding tot stand tussen het device en het wifinetwerk van de gastorganisatie

Kenmerken

- Publicroam is technisch en conceptueel gebaseerd op de bestaande succesvolle wifi-toegangsdiensten voor de overheid (govroam) en onderwijs (eduroam)
- Publicroam werkt onafhankelijk van aanbieders van apparatuur en netwerken. Aansluiting wordt in eigen beheer gerealiseerd, op basis van open standaarden
- Publicroam is beschikbaar voor zowel publieke als private organisaties, onder gelijke en transparante voorwaarden
- Publicroam gaat misbruik van wifi-gastnetwerken tegen door de eenmalige registratie

Privacy gewaarborgd - Publicroam koppelt inloggegevens aan de mobiele nummers van gebruikers. Deze gegevens worden alleen gebruikt om de dienst te laten functioneren en verder te verbeteren en ze worden zonder nadrukkelijke toestemming van de gebruiker niet gedeeld met derden.

Verdienmodel - Om de technische en organisatorische infrastructuur achter publicroam in stand te houden en verder te ontwikkelen, betalen deelnemende organisaties een jaarbijdrage en een eenmalig aansluitfee, op basis van een toegankelijke prijsstelling. Voor de bezoekers is een account altijd gratis.

Impact - Publicroam wil een beweging op gang brengen naar veilige en makkelijke toegang tot gastwifi. De doelstelling is dat mensen niet meer vragen of er wifi is bij een organisatie maar of publicroam beschikbaar is. Omdat zij veilige toegang eisen en zich niet steeds opnieuw willen aanmelden.
Impact is drieledig: (1) Minder onveilige openbare wifi-netwerken. Hackers hebben minder kans. Verspreiding van illegale content wordt ontmoedigd. (2) Meer gebruiksgemak. Doordat men niet meer steeds opnieuw hoeft aan te melden. (3) Nieuwe diensten worden mogelijk (bv location based services). Doordat technisch gescheiden wifi-netwerken worden verbonden via single sign-on.

De mensen erachter - De initiatiefnemers van publicroam zijn Ted Dinklo (48) en Paul Francissen (50). Beide zijn ervaren zelfstandige adviseurs en al jaren werkzaam in de publieke sector. Ted op het gebied van international public finance. Paul op gebied van online dienstverlening. Paul was tevens de drijvende kracht achter govroam.

Toekomstplannen - In november 2018 is de dienst gelanceerd op de Haagse Markt door de gemeente Den Haag. De andere launching customers zijn ECP, Wigo4it en gemeenten Valkenswaard, Heeze-Leende en Cranendonck. In 2019 ligt de focus op de uitrol van publicroam in Nederland. Doelstelling is om een snelle groei te realiseren. Ook richt publicroam zijn focus op het buitenland. De lange termijndoelstelling is dat publicroam internationaal breed beschikbaar komt.

Een introductie van SimplyEdit

Het web is stuk. Hyperlinks lijden aan “reference rot”[1], het web heeft geen werkend geheugen[2]. Daarnaast wordt het web overheerst door een klein aantal grote bedrijven die gebruikers eerder zien als graag als internet consument zien en niet als gelijkwaardig. Verder worden delen van het web geblokkeerd en gecensureerd door verschillende overheden. Dit is niet zoals het web bedoeld is. Om deze en andere problemen op te lossen wordt aan een nieuw, decentraal web gewerkt. Deze maakt gebruik van peer-to-peer en andere decentrale technologie. IPFS[3] en DAT[4] zijn twee protocollen die in ontwikkeling zijn. Beide lossen een aantal problemen van het huidige web op, maar maken het web wel technisch complexer.

Om het decentrale web echt te laten groeien moet het minstens net zo makkelijk in gebruik en begrijpelijk worden als het huidige web. Omdat er geen centrale servers meer zijn, werken traditionele web applicaties zoals o.a. content management systemen (CMS) niet op het decentrale web. Brewster Kahle van archive.org riep in 2015 in zijn talk ‘locking the web open’[5] dan ook op tot het maken van een ‘Wordpress voor het decentrale web’. SimplyEdit is dit, een CMS voor het decentrale web. Het draait zonder centrale servers maar bied alle mogelijkheden van een traditioneel CMS.

Een SimplyEdit website is direct in de browser te bewerken, zonder enige kennis van HTML of lange gebruikerscursus. Het werkt in iedere browser, op elk device, ook met touch. Dus ook met het gewone, huidige web. Maar als je het combineert met bijv. de Beaker browser, gemaakt voor het DAT protocol, dan zie je de kracht pas echt. Met de Beaker browser kun je een website die gemaakt is voor het decentrale web, in dit geval voor DAT, met één druk op de knop kopiëren. Je hebt dan een eigen kopie, die vanuit je eigen Beaker browser geserveerd wordt. Je browser is dan ook een server. Met een SimplyEdit website kun je vervolgens direct de editor opstarten, de website aanpassen en opslaan. Er is geen server nodig, geen installatie procedures, geen technische kennis, geen accounts bij externe partijen. Iedereen kan dit. Hiermee wordt het web weer echt een lees en schrijf medium.

SimplyEdit wordt gemaakt door Muze, een club van idealistische web ontwikkelaars die al sinds 1998 bezig zijn om het web beter te maken. Auke van Slooten (oprichter) en Yvo Brevoort zijn de ontwikkelaars en architecten van SimplyEdit. Beiden hebben informatica gestudeerd aan de Universiteit Twente en meegeholpen aan het tot stand komen van het CampusNet vanuit Studenten Net Twente. Beide besloten vroegtijdig uit de academische wereld te stappen en ondernemer te worden om zich volledig op het web te kunnen richten. In 2019 is Muze een bedrijf met 9 werknemers.

Muze heeft als missie om het web eenvoudiger te maken voor iedereen. Voor ontwikkelaars, designers, redacteuren en eindgebruikers. En niet als consument of klant, maar als mede ‘burger’ met gelijke mogelijkheden en rechten als grote organisaties. SimplyEdit is daar een onderdeel van.

Op dit moment is SimplyEdit vooral gericht op eindgebruikers en op frontend ontwikkelaars met kennis van HTML en CSS. In 2019 willen we een plugin en theme systeem bouwen, zoveel mogelijk op basis van al bekende web standaarden. Een volgende stap is om design tools te maken die met een Design System aanpak visuele designers in staat stellen om zelfstandig nieuwe originele websites te ontwerpen en publiceren.

We zijn daarnaast bezig met een uitbreiding, genaamd SimplyView, waarmee we ook web applicatie ontwikkeling, inclusief Progressive Web Apps (PWA), eenvoudiger willen maken en beter laten aansluiten bij de ‘view source’ filosofie van het vroege web. Met deze aanpak wordt het ook makkelijker om designers en developers te laten samenwerken aan hetzelfde project.

Zie ook https://simplyedit.io/, en https://reference.simplyedit.io/ (ook via dat://reference.simplyedit.io/). Voor een voorbeeld PWA met SimplyView zie https://hnpwa.simplyedit.io/, en bekijk daar ook de source met ‘view source’ in uw browser.

---

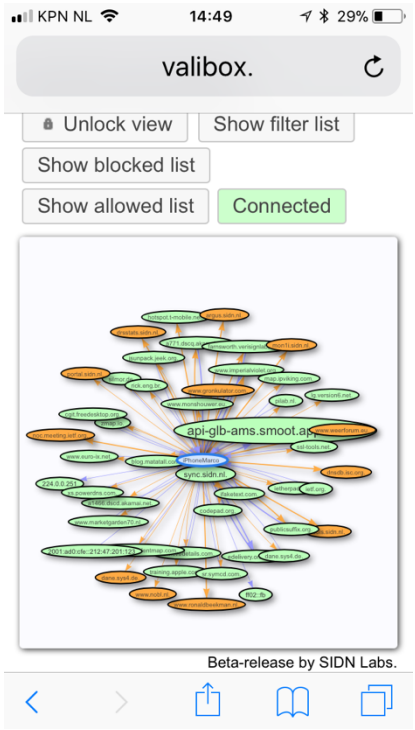
1 https://www.newyorker.com/magazine/2015/01/26/cobweb
2 https://www.itnews.com.au/news/internet-is-losing-its-memory-cerf-495854
3 https://motherboard.vice.com/en_us/article/78xgaq/the-interplanetary-file-system-wants-to-create-a-permanent-web
4 https://datproject.org/
5 https://media.ccc.de/v/camp2015-6938-locking_the_web_open_call_for_a_distributed_web

SPIN: Security and Privacy for In-home Networks

SPIN is een open source onderzoeksplatform en heeft als doel het Internet veiliger te maken met de komst van het Internet of Things. SPIN analyseert (lokaal) het netwerkverkeer op een thuisnetwerk, en biedt gebruikers inzicht in het gedrag van de apparaten in hun netwerk. Daarnaast kunnen gebruikers hun netwerk controleren door de netwerktoegang van specifieke apparaten uit te zetten. De basis van SPIN maakt het mogelijk om onderzoek te doen naar het tijdelijk geheel of gedeeltelijk beperken van apparaten die abnormaal netwerkgedrag vertonen. Een voorbeeld van afwijkend gedrag is een lamp met een wifi-verbinding die beperkt communiceert, maar plots grote aantallen pakketten het internet op gaat sturen omdat deze onderdeel is geworden van een botnet.

Met het SPIN-platform als basis richten we ons op twee pijlers:

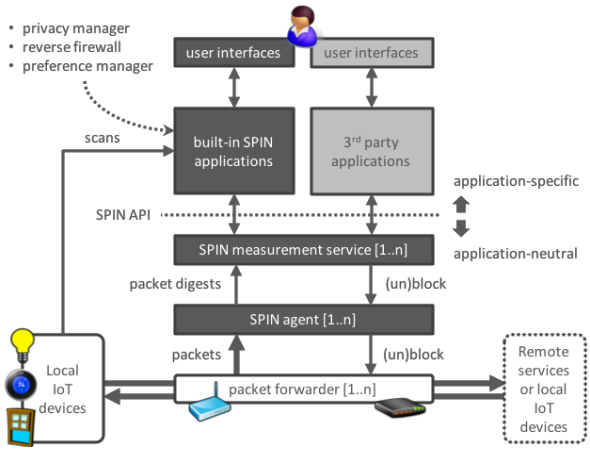
1. Nieuw onderzoek doen op het gebied van beveiliging van IoT; denk daarbij aan onderzoek naar anomaly detection (afwijkend gedrag dat duidt op een infectie), incident handling (plaatselijk, en tijdelijk blokkeren van besmette apparaten, in plaats van het hele netwerk), of nieuwe manieren om het Internet-verkeer van apparaten te visualiseren.
2. Impact maken bij eindgebruikers van thuisnetwerken door samenwerking met modemleveranciers en Internet serviceproviders, zodat SPIN-technologie daadwerkelijk zijn weg kan vinden naar de praktijk en eindgebruikers de controle krijgen over de veiligheid en het gedrag van hun slimme apparaten.



Met SPIN willen wij een bijdrage leveren aan de digitale veiligheid van het Internet of Things. Door onze kennis in papers en blogs te publiceren en op diverse conferenties te presenteren en de broncode open-source beschikbaar te maken, hopen we ontwikkelaars, leveranciers en andere partijen te stimuleren om meer aan IoT-beveiliging te doen. SPIN verwerkt data lokaal en communiceert niet met externe (cloud-)servers, omwille van privacy. Daarmee onderscheidt SPIN zich van andere oplossingen.

Onze toekomstplannen voor SPIN bestaan uit drie hoofdonderwerpen: (1) het eenvoudig en veilig configureren van nieuwe IoT-apparaten in een thuisnetwerk door automatisch toegangsbeperkingen op de router actief te maken; (2) het onderzoeken van bestaande IoT-apparaten en het in kaart brengen van hun onlinegedrag; en (3) ontwikkelen en testen van algoritmen om afwijkend gedrag van IoT-apparaten in thuisnetwerken te detecteren.

SPIN wordt ontwikkeld door SIDN Labs, de onderzoeksafdeling van .nl-registry SIDN. Specifiek werken Jelte Jansen, Marco Davids, Caspar Schutijser, Elmer Lastdrager en Cristian Hesselman aan het SPIN-project.



https://spin.sidnlabs.nl
https://github.com/sidn/spin
https://www.sidnlabs.nl/a/weblog/jaar-2-van-spin
https://www.sidnlabs.nl/downloads/papers-reports/sidn-tr-2017-002.pdf