Internet: een kwestie van vertrouwen

SIDN labs –
Een veilig en betrouwbaar internet voor iedereen

Cristian Hesselman | ECP Jaarcongres 2016

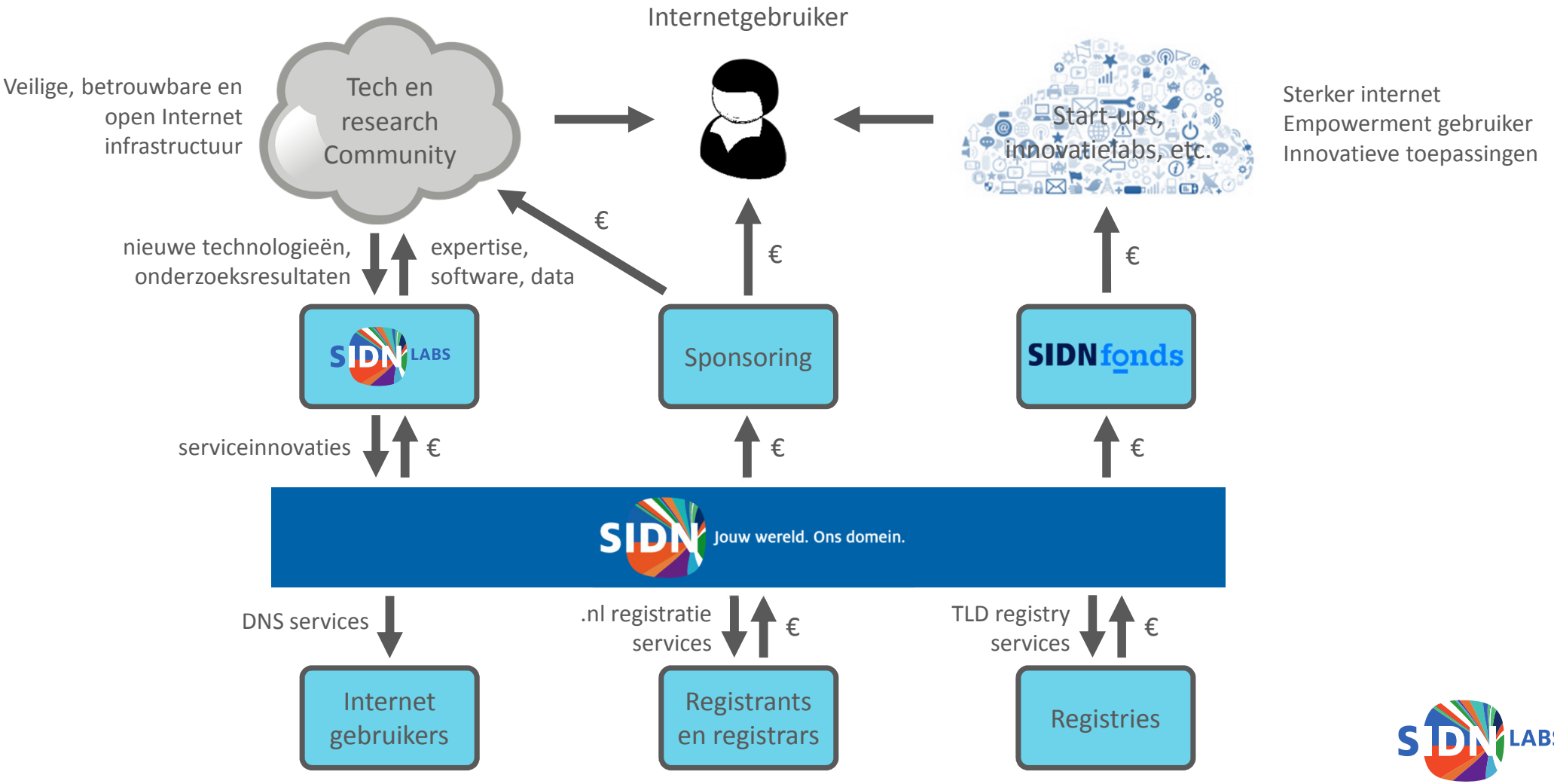
17 november 2016

SIDN: een zorgeloos digitaal bestaan voor iedereen

- Het bedrijf achter 4e grootste en een van veiligste landendomeinen: .nl
- 5.6 miljoen .nl-domeinnamen, waarvan 2,5 miljoen met een digitale handtekening.
- Verantwoordelijk voor de .nl-zone sinds 1996.
- We delen onze kennis, steunen initiatieven en ontwikkelen diensten die bijdragen aan een waardevoller, veiliger en makkelijker internet.

SIDN LABS

Een zorgeloos digitaal bestaan voor iedereen



SIDN Labs: veilig en betrouwbaar internet voor iedereen

- Het researchteam van SIDN.
- SIDN Labs ontwikkelt nieuwe technieken en systemen die de stabiliteit en veiligheid van .nl, het DNS en de internetinfrastructuur in de breedte verder verhogen.
- We werken graag samen met onderzoeksinstellingen en andere bedrijven.
- We richten ons op 2 onderwerpen:
  - DNS-protocollen en systemen.
  - Privacy-vriendelijk network analytics.

SIDN fonds: een sterker internet voor iedereen

- Opgericht door SIDN om de toegevoegde waarde van het internet voor de Nederlandse economie en maatschappij te vergroten. April 2015 1e call!
- Steunen internetprojecten met lef:
  - Versterking van het internet
  - Empowerment van de gebruiker
  - Tech for good
- 2 calls per jaar. Medio december opent de eerstvolgende aanvraagronde (deadline 7-3-17)
- 67 projecten ondersteund: 31 pioniers, 35 potentials, 1 samenwerkingsprojecten (28 Tech for good, 21 sterker internet, 18 empowerment)

SIDN fonds

SIDN LABS

Agenda

1. Ervaringen met privacybeheer voor DNS-‘big data’-toepassingen
   - *Jelte Jansen, Senior Research Engineer SIDN Labs*

2. Internetfraude bestrijden door samenwerking Fraudehelpdesk en SIDN
   - *Elmer Lastdrager, specialist Cybersecurity Fraudehelpdesk*
   - *Maarten Wullink, Senior Research Engineer SIDN labs*

Ervaringen met privacybeheer voor DNS-'Big Data'-toepassingen

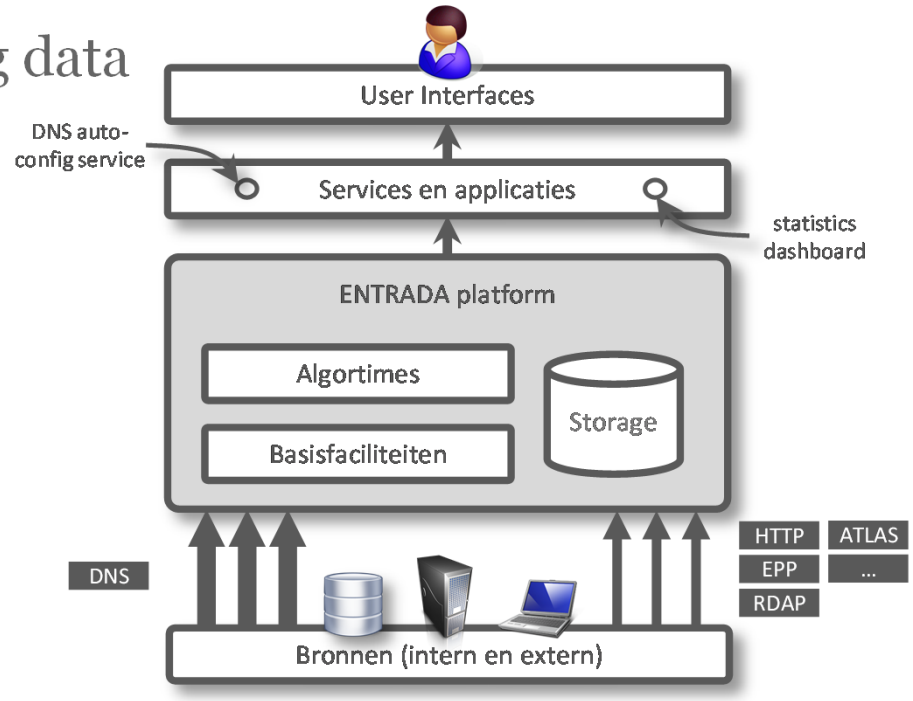
SIDN labs –
Een veilig en betrouwbaar internet voor iedereen

Jelte Jansen | ECP Jaarcongres 2016

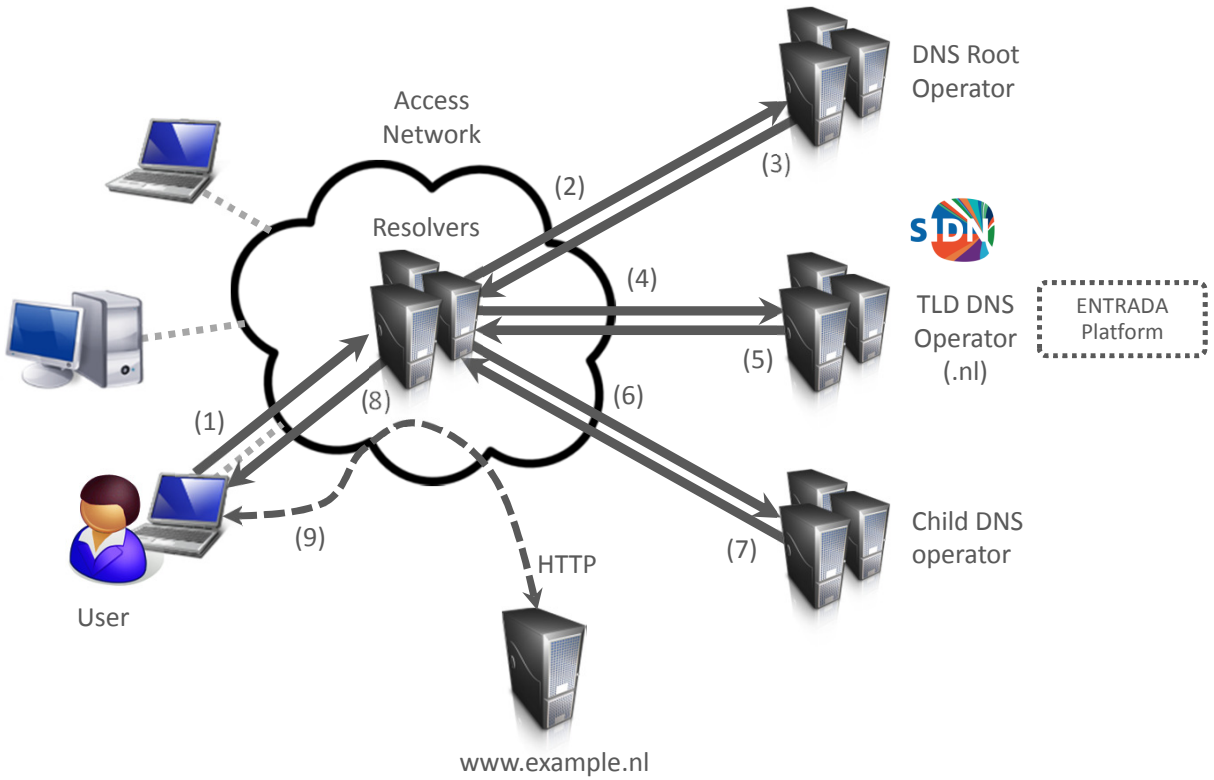
17 november 2016

SIDN: een zorgeloos digitaal bestaan voor iedereen

- Enhanced Top-level domain Resilience through Advanced Data Analysis
- Doel: Ontwikkelen en evalueren van (DNS) Big data applications
  - Waarborging stabiliteit '.nl'
  - Verhoging veiligheid van (Nederlandse) Internet
  - Detecteren van botnets en misbruik
- Hoe zit het met privacy?



ENTRADA binnen het DNS



Persoonsgegevens?

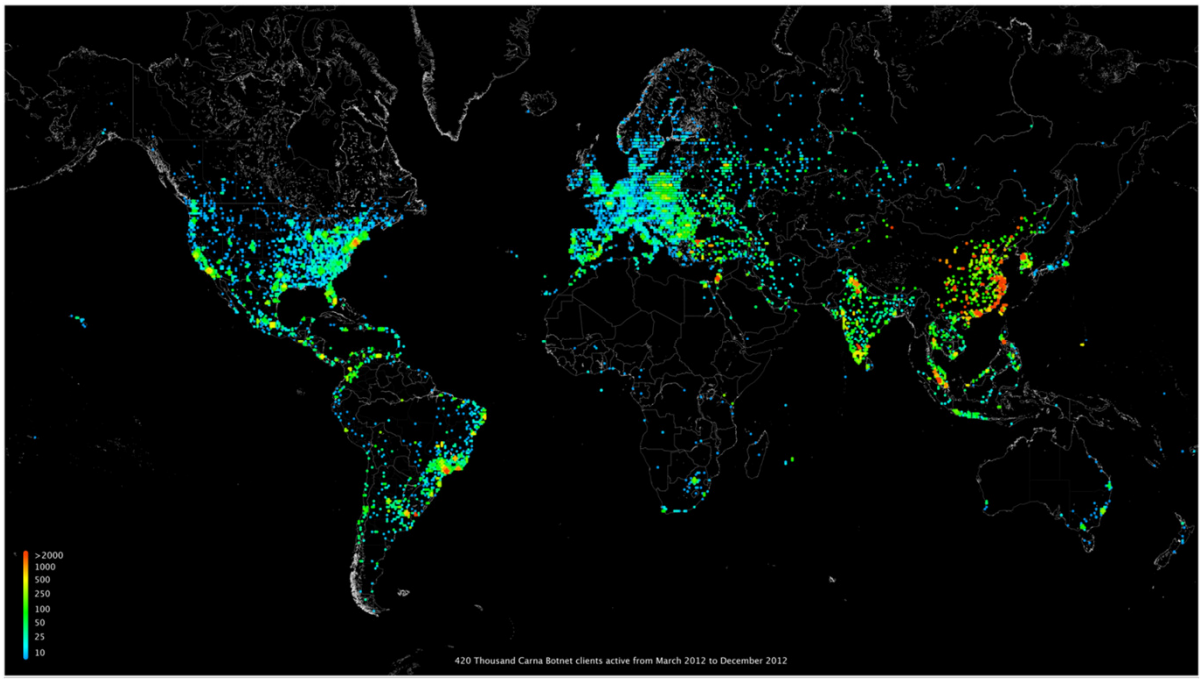
- Soms wel
  - Afzenderadres
  - Inhoud van query

- Vaak ook niet
  - Gedeelde resolvers
  - Algemene vragen

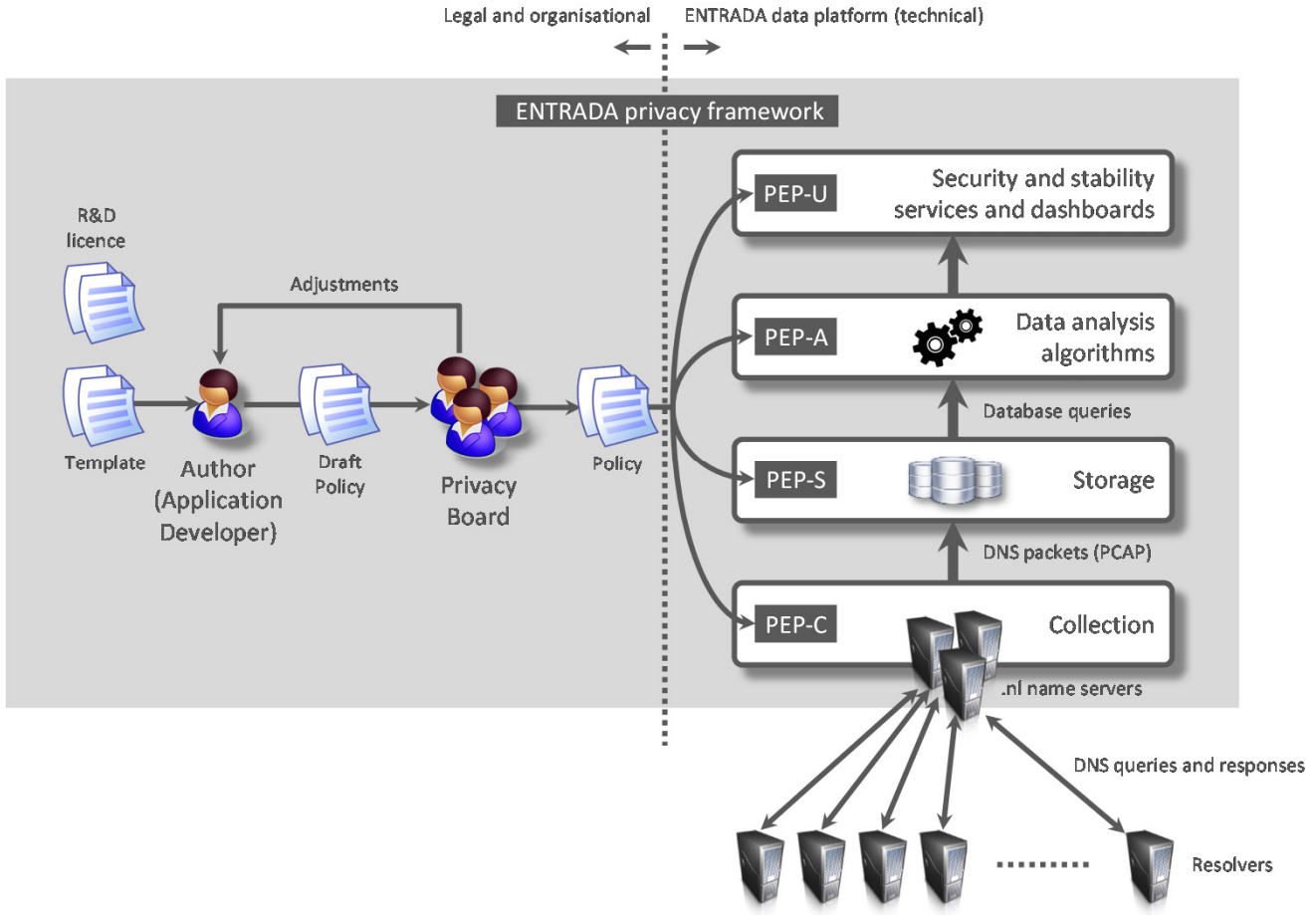
Datagebruik kan verschillen per toepassing

- Voorbeeld: botnetdetectie
  - Queryinhoud niet belangrijk
  - IP-adres wel!

- Voorbeeld: meting DDoS
  - IP-adres niet relevant
  - Queryinhoud wel



ENTRADA privacyraamwerk



Position paper (2014)

https://www.sidnlabs.nl/downloads/whitepapers/PEI_2014_6_Hesselman.pdf

Privacy board

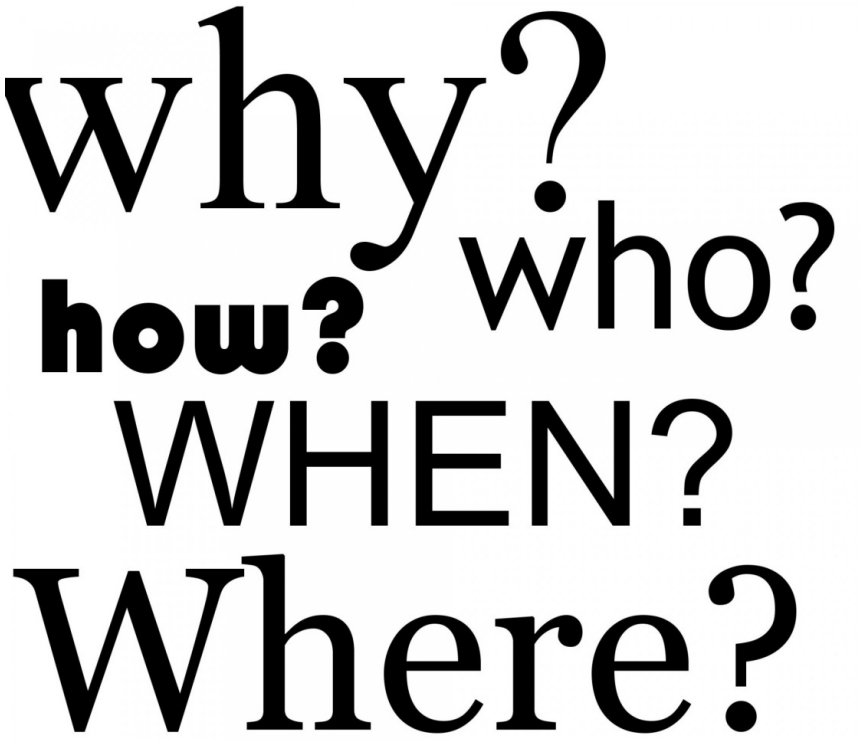
- Opgericht in 2015
  - Manager, jurist en technisch adviseur
- Processen opgezet
  - Privacy policy template
  - Beoordelingsrapporten van policy's
- Bewustzijnscampagne

De eerste policy

- Bleek nog belangrijke informatie te ontbreken of onduidelijk te zijn
  - Grondslag
  - Publicatie / delen
  - Procesmatige zaken (naam/datum)

Veel vragen over privacy

- Wanneer persoonsgegevens, wat mag?
- Hoe zit het met ‘publieke’ data?
- Wat als er meerdere verantwoordelijken zijn?
- Is een geheimhoudingsverklaring niet genoeg?
- Etc.



Ingediende policy niet altijd nodig

- Soms werd er een policy ingediend over een proces waar geen persoonsgegevens verwerkt werden
  - Dan ook geen privacy policy nodig
  - Wel goed dat het nagegaan werd

Policy wordt niet zomaar goedgekeurd

- Geen policy was ‘in een keer’ goed
  - Grondslag
  - Informatie ontbrak
  - Maar ook: te veel details
  - En natuurlijk: project/dienst/proces kon beter

- Meestal slechts kleine wijzigingen in beschrijving
- Een enkele keer proceswijziging

SIDN LABS

Voorbeeld: JTIE

- Kijkt naar DNS-kenmerken na melding phishing
  - Hoeveelheid queries voor phishdomein
  - Informatie over registratie

- Ingediende policy:
  - Geen individuele query-informatie, alleen totalen over tijd
  - Naam van bedrijf waar domein geregistreerd is

- Na feedback:
  - Pseudoniem van bedrijf waar domein geregistreerd is

Lessen

- Gebruik ‘privacy by design’
- Zorg voor bewustzijn
- Houd het overzichtelijk
- Zorg voor weinig ‘red tape’
- Wees bereikbaar voor vragen

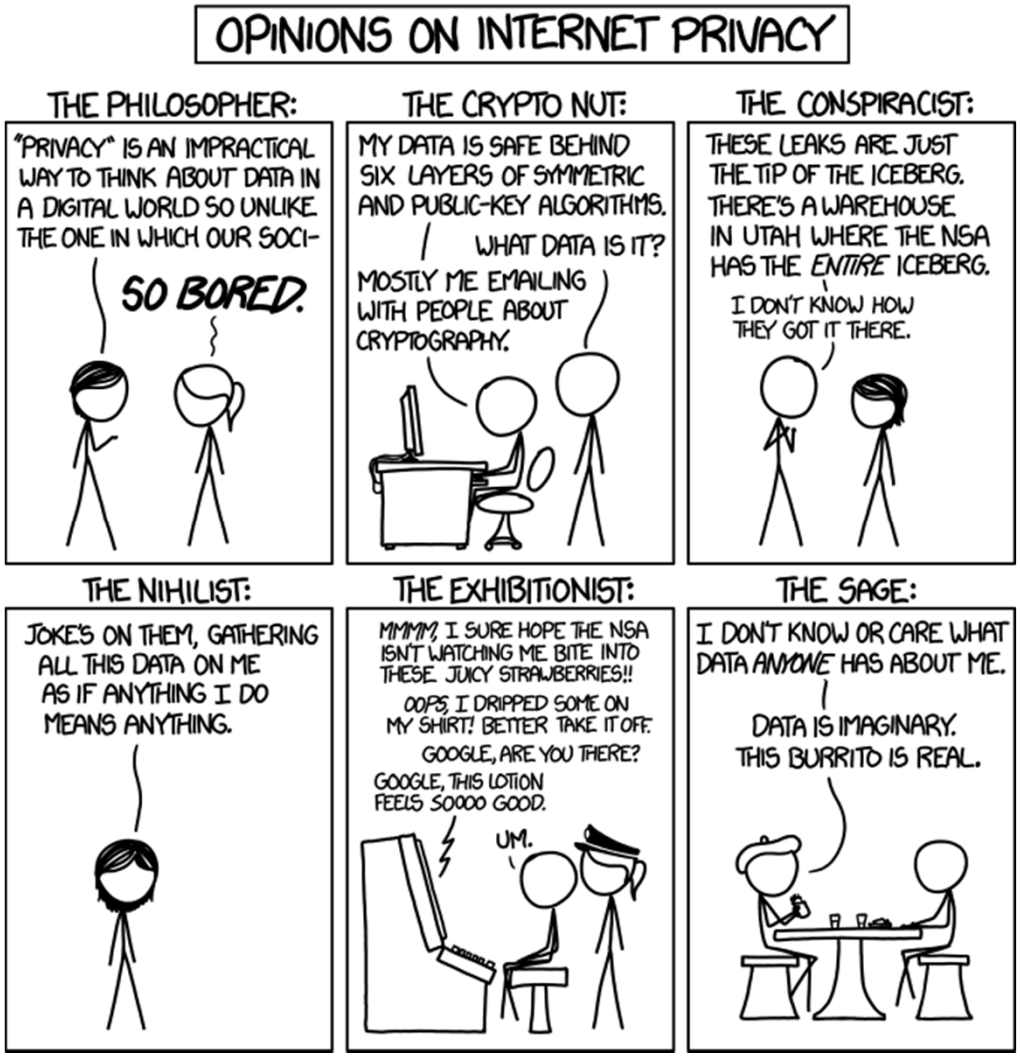
Vervolgartikel

https://www.sidnlabs.nl/downloads/papers-reports/SIDN-TR-2016-001-NL.pdf

Vragen?

Jelte Jansen
jelte.jansen@sidn.nl
@twitjeb

sidn.nl | sidnlabs.nl
@sidnlabs



Internetfraude bestrijden door samenwerking Fraudehelpdesk en SIDN

ECP Jaarcongres 17.11.2016 Utrecht

Elmer Lastdrager en Maarten Wullink

Introductie FHD en SIDN

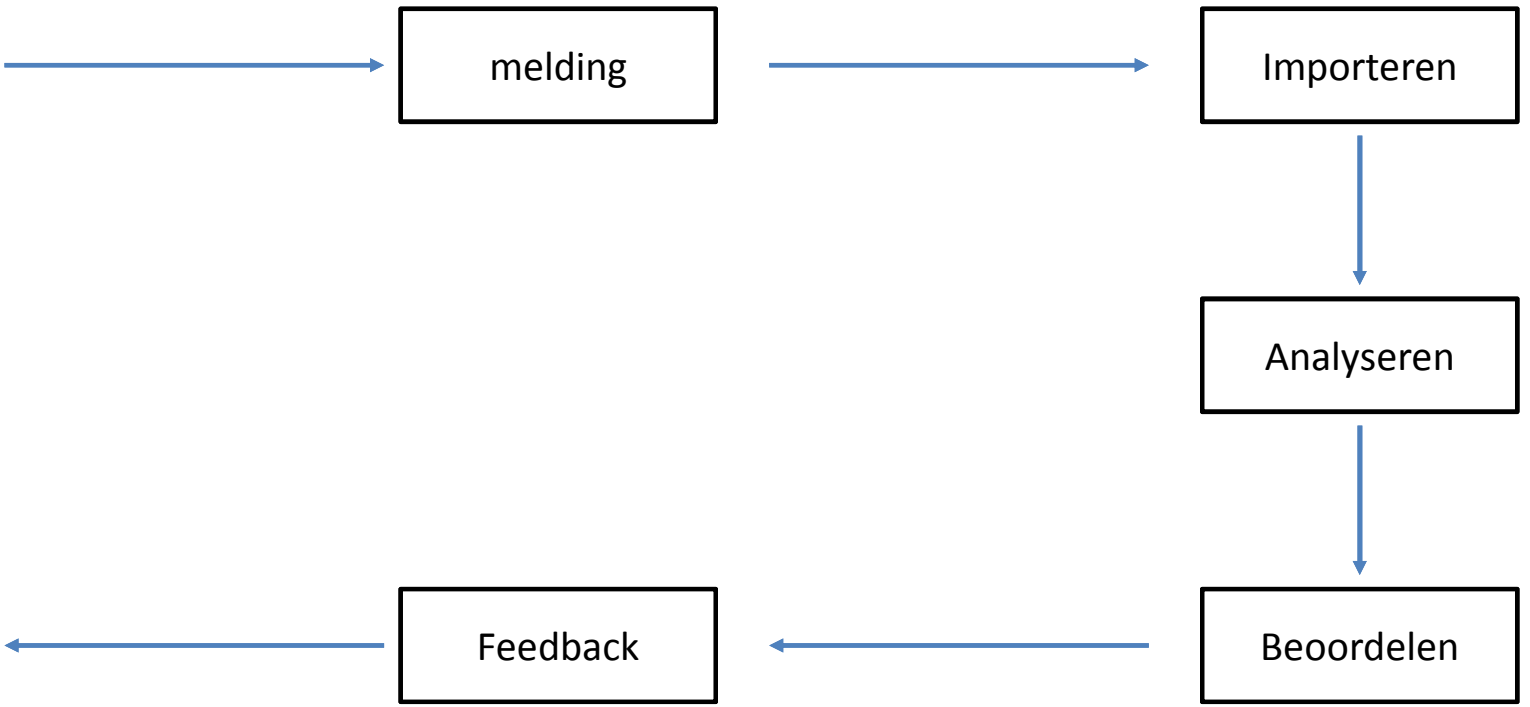
Doel van JTIE

- Joint Threat Intelligence Enrichment
- Samen sneller bepalen of een mail een phishingmail is om meer gebruikers voor dit soort van misbruik sneller te beschermen
- Aanpak: pilot

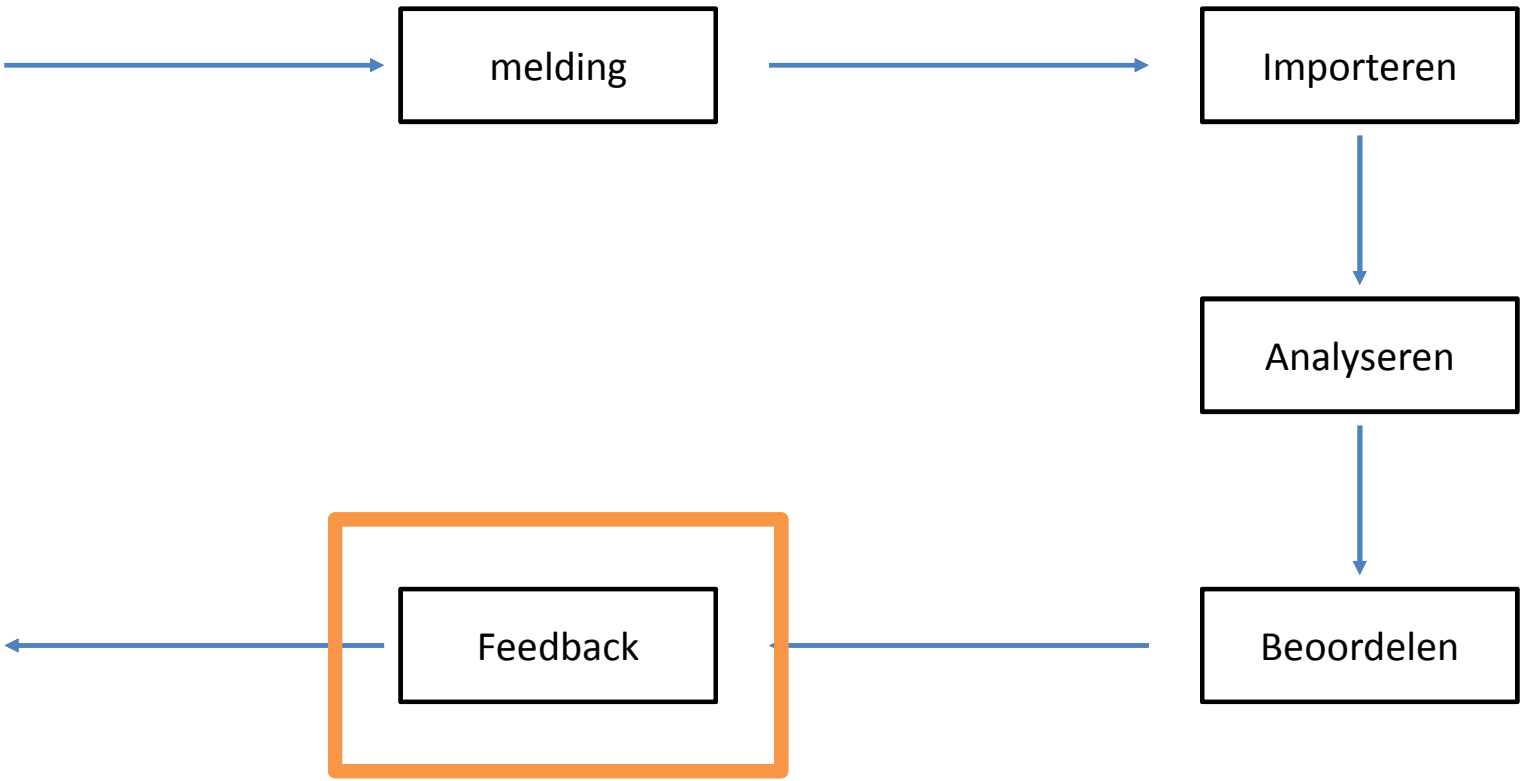
Phishing en FHD

- Meldpunt: valse-email@fraudehelpdesk.nl
- +- 48.000 meldingen per maand
- 7.500.000 meldingen in totaal
- 40-150 .nl domeinen per dag

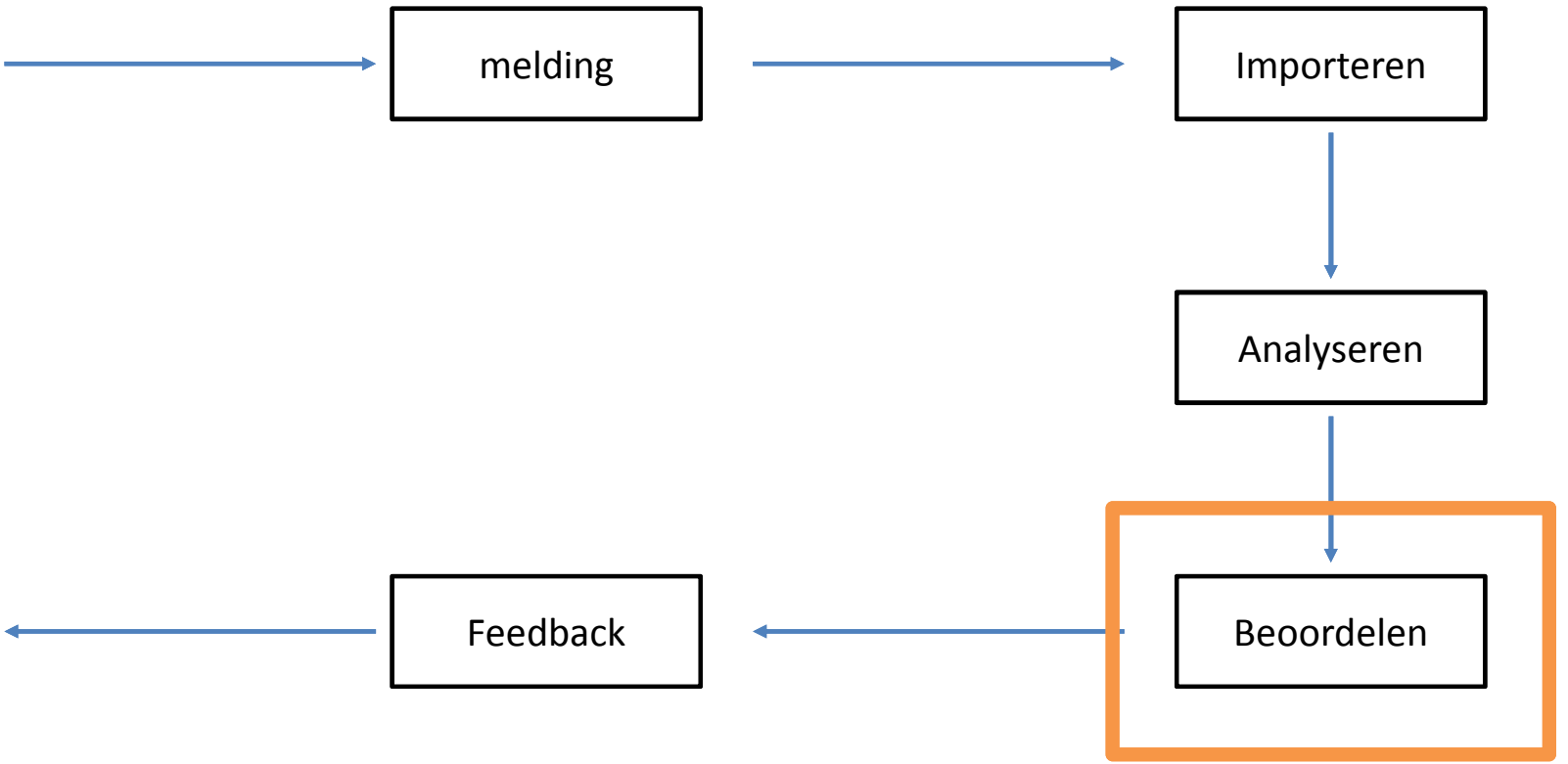
Phishing en FHD



Phishing en FHD



Phishing en FHD



FRAUDE HELPDESK.nl

SIDN LABS

Phishing en SIDN

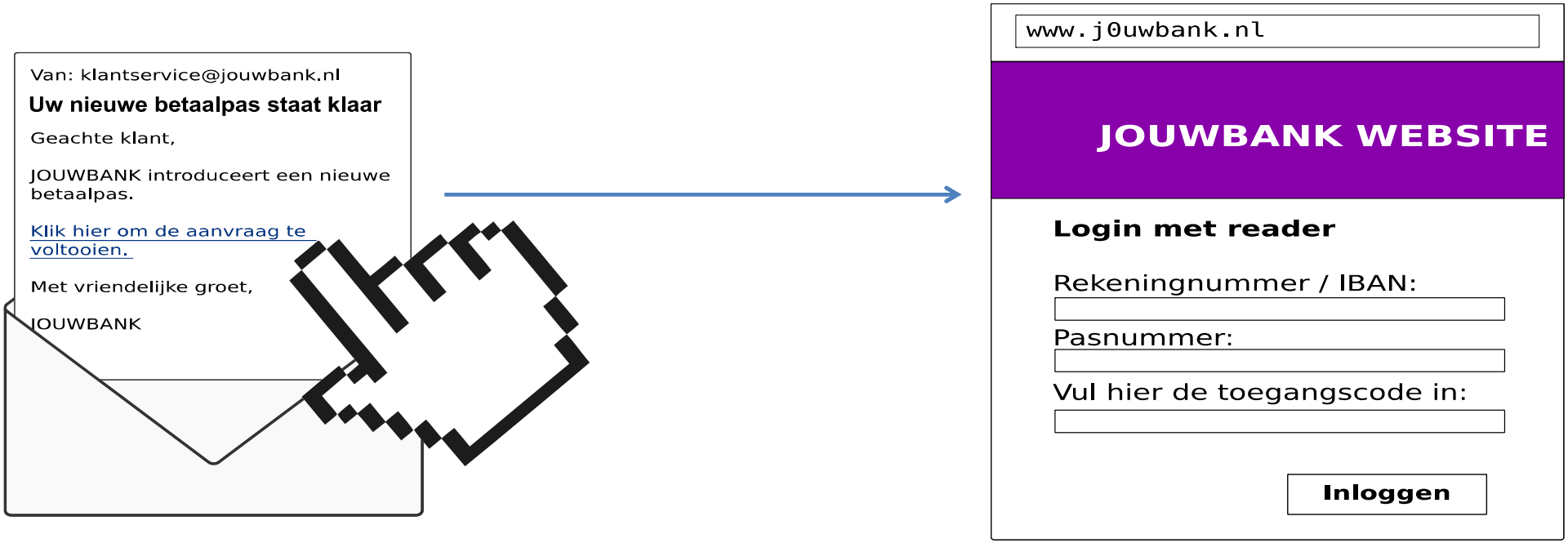
Hoe werkt het?

Phishing en SIDN

Hoe werkt het?

Phishing en SIDN

Hoe werkt het?



Phishing en SIDN

Hoe werkt het?

IP-adres:
198.51.100.4

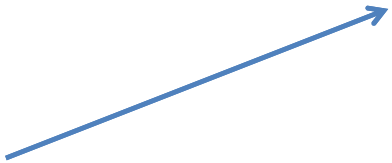
FRAUDE HELPDESK.nl

SIDN LABS

Phishing en SIDN

Hoe werkt het?

Wie heeft het adres jouwbank.nl?



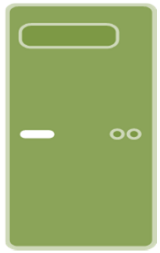
JOUW INTERNETPROVIDER

IP-adres: 198.51.100.4

Phishing en SIDN

Hoe werkt het?

Wie heeft het adres
j0uwbank.nl?

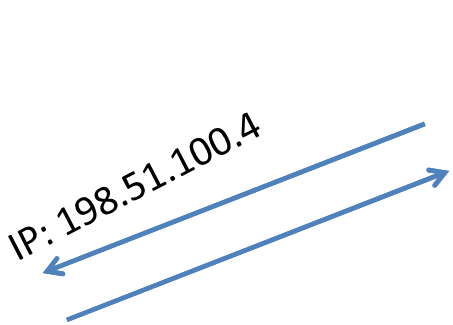


JOUW
INTERNETPROVIDER

IP-adres:
198.51.100.4

Phishing en SIDN

Hoe werkt het?



JOUW
INTERNETPROVIDER

IP-adres:
198.51.100.4

Phishing en SIDN

Hoe werkt het?

IP: 198.51.100.4

JOUW
INTERNETPROVIDER

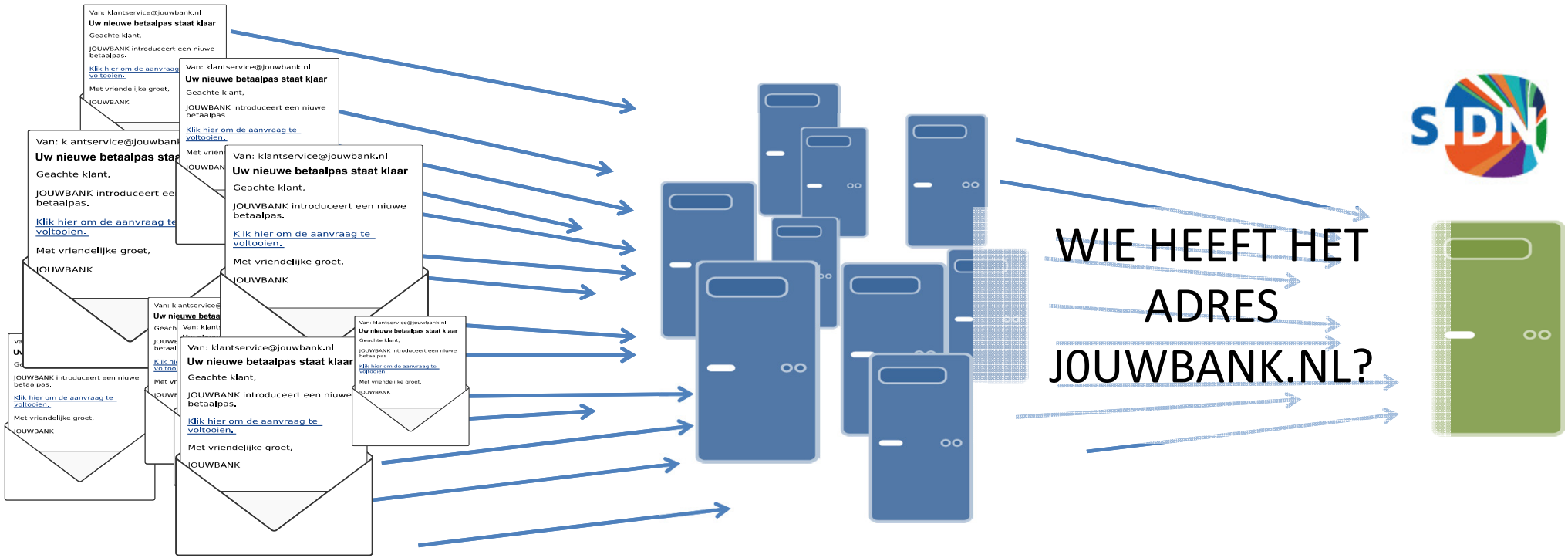
IP-adres:
198.51.100.4

FRAUDE HELPDESK.nl

SIDN LABS

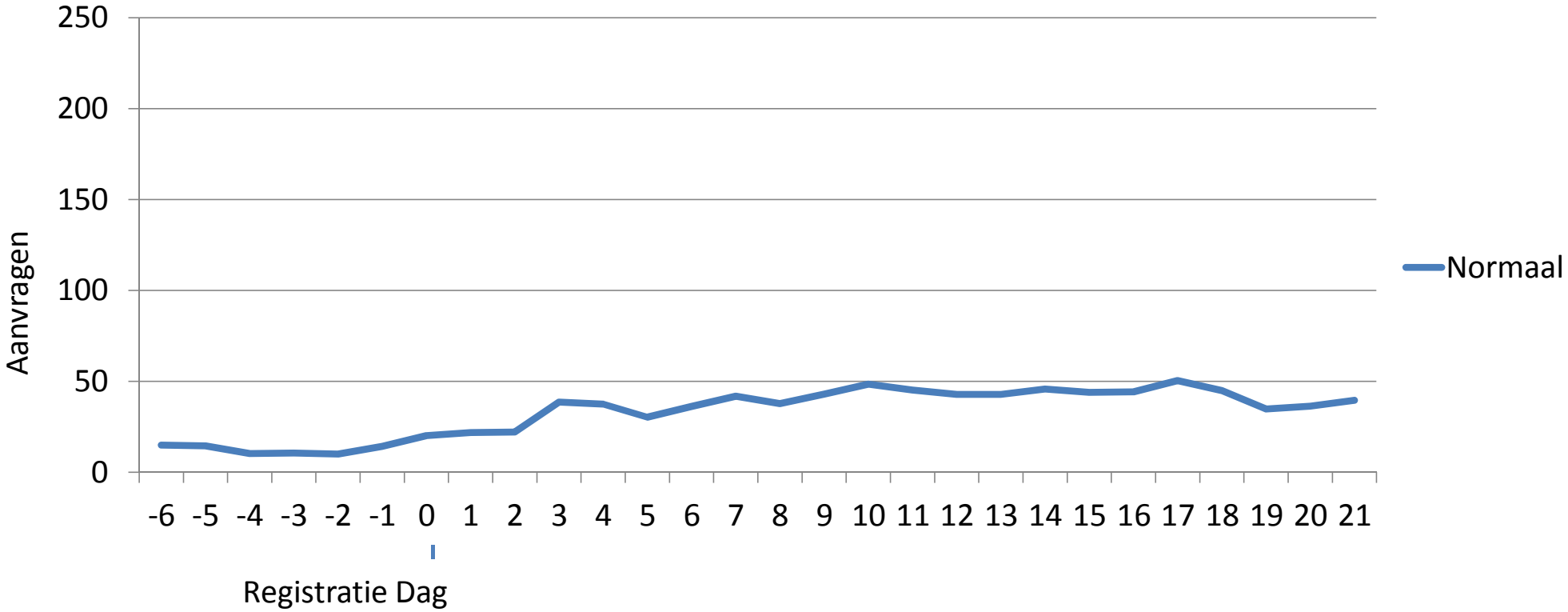
Phishing en SIDN

Hoe kan je het detecteren?



Phishing en SIDN

Hoe kan je het detecteren?



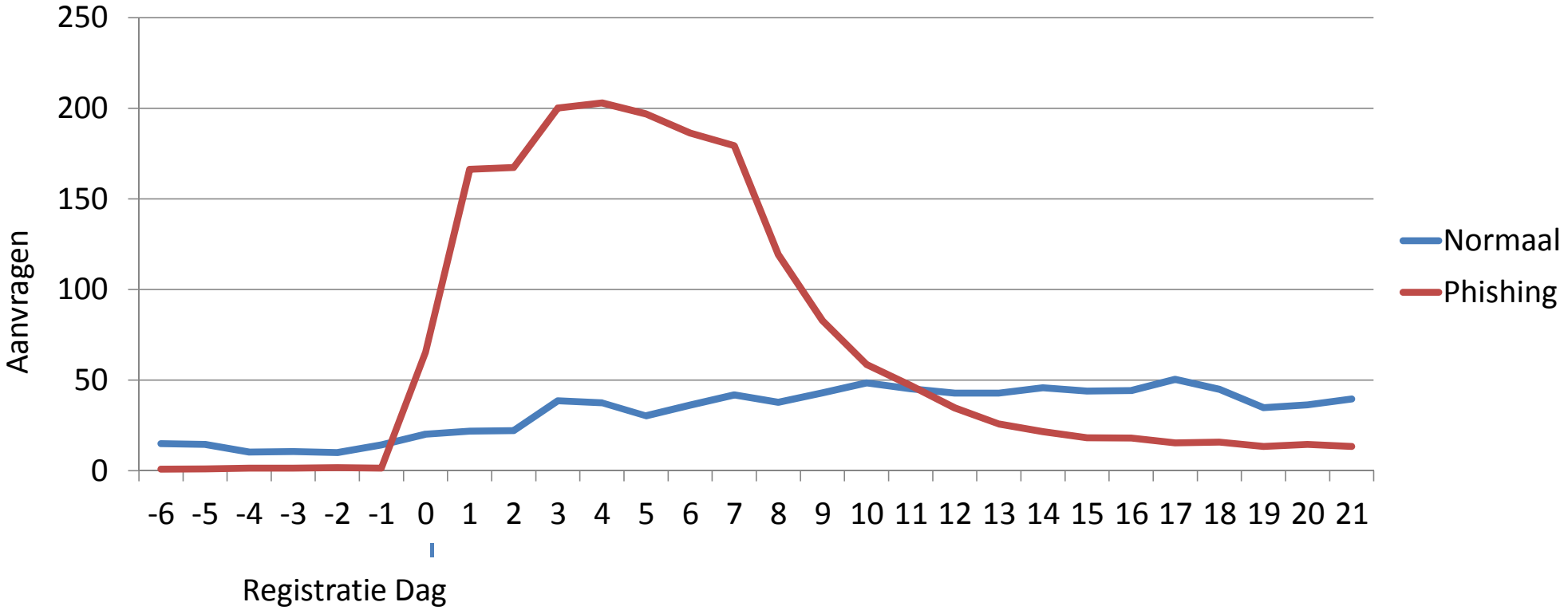
G. Moura, M. Mueller, M. Wullink, and C. Hesselman, *"nDEWS: a New Domains Early Warning System for TLDs"*, IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2016), Istanbul, Turkey, April 2016,https://www.sidnlabs.nl/downloads/presentations/sidn-annet2016.pdf

FRAUDE HELPDESK.nl

SIDN LABS

Phishing en SIDN

Hoe kan je het detecteren?



G. Moura, M. Mueller, M. Wullink, and C. Hesselman, *"nDEWS: a New Domains Early Warning System for TLDs"*, IEEE/IFIP International Workshop on Analytics for Network and Service Management (AnNet 2016), Istanbul, Turkey, April 2016,https://www.sidnlabs.nl/downloads/presentations/sidn-annet2016.pdf

FRAUDE HELPDESK.nl

SIDN LABS

Phishing en SIDN

Hoe kan je het detecteren?

- Vaak zijn de phishingdomeinnamen gehackt, maar af en toe ook door de phisher geregistreerd
  - Vaak met rare gegevens
  - Bij registrars met slechte reputatie

JTIE Workflow

Verdachte Mail van Gebruiker

FRAUDE HELPDESK.nl

Inhoudelijke analyse en filteren van .nl-domeinnamen

JTIE Workflow

FRAUDE HELPDESK.nl

Inhoudelijke analyse en filteren van .nl-domeinnamen

j0uwbank.nl

JTIE Workflow

FRAUDE HELPDESK.nl

Classificeren en bepalen prioriteit van mail

Aanvullende info over j0uwbank.nl

Voldoet aan het Privacyraamwerk

JTIE Workflow

Phishing!!!

FRAUDE HELPDESK.nl

Classificeren en bepalen prioriteit van mail

Aanvullende info over j0uwbank.nl

SIDN

(Voorlopige) Resultaten

- SIDN heeft een systeem voor automatische afhandeling van FHD-meldingen ontwikkeld.
- FHD heeft plugin ontwikkeld om alleen .nl- domeinnamen aan SIDN te sturen.
- Operationeel sinds 3 weken.

Vervolgstappen

- Analyse algoritme slimmer maken.
- Wederzijds uitwisselen van informatie.
- Automatische “phishing-score” ontwikkelen
- JTIE is een prototype, eerste evaluatie verwacht in december.
- Met meer partijen Threat Intelligence uitwisselen.

Vragen?

Maarten Wullink
Senior Research Engineer
maarten.wullink@sidn.nl
@wulliak

www.sidnlabs.nl

Elmer Lastdrager
Cybercrime onderzoeker
ELastdrager@fraudehelpdesk.nl
@elmerlastdrager

www.fraudehelpdesk.nl