

Identiteitsfraude als uitdaging in ketens!

Jan Grijpink



Thema: Privacy by Design

Telecommunicatie 25-05-2016

Begrippen

Wat bedoelen we met een *identiteit*?

- Iemands *maatschappelijke* identiteit: een aantal *officiële* kenmerken (waaronder persoonsgegevens),
 - waarmee we een persoon uniek kunnen aanduiden
 - waarmee iemand zich vereenzelvigd
- Te onderscheiden van:
 - iemands biologische identiteit
 - pseudo-identiteiten

Wat bedoelen we met *identiteitsfraude*?

- Iemand gebruikt met **kwade** bedoelingen de identiteit van iemand anders, bestaand of verzonnen
- **Elk** persoonsnummer, foto, handeling of gebeurtenis bevat **suggesties** waaruit mensen afleiden wie ze tegenover zich hebben; een identiteitsbewijs is niet vereist
- Identiteitsfraude kan **overal** plaatsvinden en op allerlei manieren, niet beperkt tot specifieke situaties, procedures of documenten

Identiteitsfraude, iets nieuws?

- **Nee**, maar het wordt wel **anders**, door de digitalisering en anonimisering van onze samenleving. Die leidt tot een **explosieve toename** van
 - elektronische identiteits-‘bewijzen’ en
 - elektronische identiteitscontroles
 - vervlechting van stukjes fysiek en digitaal proces
- Slachtoffers hebben het niet, of te laat in de gaten en eventuele **sporen** leiden naar het slachtoffer, **niet naar de dader**
- Geslaagde identiteitsfraude in een proces of keten **verspreidt zich ongemerkt** over andere processen of ketens.

Oorzaken

Een blinde vlek voor identiteitsfraude?

Wij **vertrouwen spontaan** op **administratieve** (fysieke of elektronische) **identiteiten**, zelfs als ze gebaseerd zijn op ongecontroleerde of oncontroleerbare gegevens!

Wij kijken bij identiteitscontrole naar het **document** in plaats van naar de **persoon**; bij een serieuze verdenking is het meestal te laat; sporen leiden naar het slachtoffer!

We zetten de **controlegegevens op het document**; een naam-nummercontrole slaagt dan altijd, ongeacht wie zich van het document bedient!

Regelgeving en vaste procedures maken het de identiteitsfraudeur onbedoeld gemakkelijk om te **voorspellen** waar, hoe en wanneer hij zal worden gecontroleerd. En hij heeft het verrassingselement aan zijn kant (fall back procedures)

Wat zijn de gevolgen? Voorbeelden

Voorbeeld

Identiteitsfraude in de strafrechtketen

- **Alias**misbruik (identiteitsfraude) in de strafrechtketen heeft in de loop van de tijd geleid tot ernstige vervuiling van het **strafblad**register
- Gevolgen:
 - niet onderkennen van **recidive**
 - arrestatie of aanhouding van de **verkeerde persoon**
 - foutieve beslissing op een aanvraag **Verklaring omtrent gedrag (VOG)**
- Hoe pak je
 - schoonmaken van vervuilde strafbladen aan?
 - voorkomen/blokken van nieuwe aliases aan?
 - voorkomen van onterechte verdenking, onterechte weigering VOG?

Voorbeeld

Identiteitsfraude in de gezondheidszorg

- Het burgerservicenummer (BSN) in de zorg als **identificatiemiddel** of als **koppelmechanisme** zal ertoe leiden, dat bij raadpleging ongemerkt medische gegevens van méérdere patiënten worden gepresenteerd
- Gevolg:
 - **verkeerde behandeling** of **onderbehandeling** van BSN-houder *en* meelifters, doordat een ziekte van de ene patiënt een contra-indicatie oplevert voor de juiste behandeling van de andere patiënt
- Hoe pak je
 - schoonmaken van vervuilde medische dossiers aan?
 - blokkeren van meelifters aan?
 - bewijsvoering bij letselschade aan?
 - elkaar tegensprekende behandelingsresultaten aan?

Gevolgen op de lange termijn

1. Als je als slachtoffer moet bewijzen dat je het niet gedaan hebt komt ons rechts-beginsel *onschuldig tot het tegendeel bewezen is* onder spanning. Betekent dat je nog weer extra privacy moet opgeven om er een beetje van terug te krijgen!
2. Als men zich tegen deze dreiging zelf moet verweren komt privacybescherming in een nieuwe fase waarin *zelfverdediging* en *actieve* waakzaamheid geboden zijn. Je moet je eigen identiteit beschermen en tegelijkertijd meeliften belemmeren: anonimiteit en pseudonimiteit krijgen een nieuwe betekenis

Hoeveel
identiteitsfraude is er?

Hoeveel identiteitsfraude weten we niet!

1. Geslaagde **identiteitsfraude** wordt meestal niet opgemerkt
2. **Gevolgfraude** wel (bijv pinpas-fraude), maar deze wordt door de desbetreffende instantie vaak stilgehouden (geen totaalbeeld)
3. Er is **geen neutraal meldpunt** waar slachtoffers van identiteitsfraude worden geholpen en de cijfers worden bijgehouden

Wat weten we wel?

- Meeliften op een andere identiteit is niet moeilijk, levert veel voordeel bij slagen en geen nadeel bij mislukken
- Voorspelbare identiteitscontroles met ééndimensionale, verplichte en algemene controle-instrumenten lokken identiteitsfraude uit
- Generieke voorzieningen zoals BSN en het oogmerk 'dienstverlening' vergroten de kwetsbaarheid van processen

Ketenvisie op identiteit

- **Grootschalige** stelsels werken **anders** dan je verwacht op basis van inzichten en proefnemingen op beperktere schaal: niveau-vergissing
- **Maatregelen** en **instrumenten** die nuttig zijn voor bestrijding van documentfraude zijn dat meestal niet voor bestrijding van identiteitsfraude. **Vaak werken ze (ook) averechts!**
Voorbeeld: biometrische visum!

Waait identiteitsfraude over?

Identiteitsfraude waait **niet** over!

- De relatie tussen fysieke werkelijkheid en administratieve afbeeldingen wordt steeds moeilijker te doorgronden
- Grootschalige voorzieningen werken anders dan men verwacht, soms zelfs omgekeerd (niveauvergissing)
- Digitalisering van processen leidt tot méér sporen, maar naar wie?

Wat kunnen we doen?

Wat kunnen we ertegen doen?

- **Preventie** is de enige effectieve aanpak omdat achteraf de sporen naar het slachtoffer wijzen
- Voor afdoende preventie moet de overheid veel meer uit de kast halen
- Controleprocedures moeten **slimmer** worden om identiteitsfraudeurs te kunnen ontmaskeren met **gesloten lussen!**
- Overheden, organisaties en burgers moeten zelf zorgvuldiger omspringen met gegevens waarmee een identiteit kan worden ge(re)construeerd

Slimmere identiteitscontroles

Meer aandacht voor de **persoon** van de gecontroleerde. Personen controleer je anders dan documenten!

Oplossing: **meeliften** moeilijk maken

Meer aandacht voor het **proces** van identiteitscontrole: iedere situatie van identiteitscontrole is anders (Schiphol, bank, politiebureau).

Oplossing: **variatie in werkwijze** (minder voorspelbaar of identiteitsfraude gaat lukken!) en **gesloten lussen**

Meer aandacht voor **controlegegevens**.

Oplossing: **onafhankelijke gegevens van elders**, gegevens op identiteitsbewijzen niet gebruiken of extra verifiëren

Meer aandacht voor de **waarde** van identiteitsbewijzen en persoonsnummers; hoe méér je ermee kunt doen, hoe harder de aanval!

Oplossing: **extra drempels toevoegen** (pincode, transactiecode, etc.), dus: **'vaker kloppen'**

Identiteitsfraude als uitdaging

- Hoe ontdek je identiteitsfraude?
- Hoe gebruik je gegevens uit een onafhankelijke bron voor persoonsgerichte identiteitscontrole?
- Hoe zie je of iemand een slachtoffer of een dader is?

Conclusies

- Identiteitsfraude is gemakkelijk en lonend; ze hebben (de) toekomst! Identiteitsfraude zal het eerste decennium eerder toe dan afnemen
- Identiteitscontroles moeten slimmer worden en meeliften kunnen afstoppen
- Identiteitsfraude zal onze rechtsorde aantasten (bewijzen van eigen onschuld, geen rechts- en eerherstel krijgen, verlies van vertrouwen in overheid)
- We moeten leren zelf actiever te waken over onze eigen identiteit en onze privacy

Identiteitsfraude als uitdaging in ketens!



Einde

www.keteninformatisering.nl
www.jcc.library.uu.nl