Ik ben een bezorgde burger

Stefan van den Oord[1], 6 maart 2020

Ik maak me zorgen. Ik maak me zorgen over het feit dat overheden en bedrijven steeds verder gaan in het verzamelen van data over mij, en mij met die data manipuleren. En dat terwijl de vooruitgang op het gebied van manieren om mijzelf daartegen te beschermen niet alleen ver achterloopt, maar ook nog eens veel langzamer verloopt. Laat ik wat voorbeelden geven.

DigiD

Velen van ons zijn inmiddels bekend (maar nog niet vertrouwd) met DigiD. Een paar jaar geleden was er nog geen app voor, toen werkte het met een login op basis van gebruikersnaam en wachtwoord. Optioneel kon daarbij een SMS verificatie gebruikt worden, waarbij via SMS een code werd gestuurd naar eerder opgegeven telefoonnummer. Die code moest je dan invoeren, naast je gebruikersnaam en wachtwoord, om in te kunnen loggen. Het probleem was dat je *bij de inlogpoging moest kiezen of je wel of niet de SMS verificatie wilde gebruiken.* Als ik dus kwaad wil doen en iemands gebruikersnaam en wachtwoord heb achterhaald, dan kies ik gewoon de SMS verificatie niet te gebruiken en niets staat me verder in de weg. Dit verkeerd toepassen van *second factor authentication* zorgt ervoor dat het volstrekt waardeloos is geworden.

Tegenwoordig hebben we een DigiD app en gelukkig is er veel verbeterd. In plaats van tijdens het inloggen zelf, kies ik er nu in mijn DigiD instellingen voor dat de app gebruikt moet worden bij inlogpogingen. Maar nog steeds laat het veel te wensen over. Je kan bijvoorbeeld een zogenaamde “ID-check” uitvoeren. Als je de DigiD app opent, lijkt het iets te maken te hebben met een identiteitskaart, op basis van de afbeelding. Het is niet duidelijk waarom ik dit zou willen doen en wat er dan gebeurt. De sprong in het diepe wagend kies ik ervoor om door te gaan. Er wordt me gevraagd mijn identiteitsbewijs te scannen met mijn smartphone. Aangezien ik weet dat er in Nederland alleen al honderden mensen *per dag* slachtoffer worden van identiteitsfraude, twijfel ik. Er staat namelijk nog steeds niets over wat er gebeurt met de gegevens die worden gescand, en waarom ik het eigenlijk zou willen. Er staat wel een klein vraagtekenknopje. Daar wordt je niet veel wijzer van: *“Bij de ID-check verwerken wij de volgende gegevens: (*) documentnummer/rijbewijsnummer, (*) geboortedatum, (*) geldigheid. De gegevens worden niet opgeslagen.”* De gegevens worden wel verwerkt, maar niet opgeslagen? Wat houdt dat verwerken dan in? Waar worden die verwerkt, en hoe? Normaal gesproken zou ik nu al afgehaakt zijn, maar omwille mijn onderzoek ga ik door. Na enige moeite lukt het me om mijn rijbewijs te scannen. Ik wordt gefeliciteerd met het feit dat ik *“nu nog meer met de DigiD app kan”*! Tjonge, nou, bedankt.[2]

Als software architect voel ik plaatsvervangende schaamte. We moeten echt beter onze best doen om dingen begrijpelijk en transparant te maken.

Wie weet wat?

Stel dat je kind mogelijk een aandoening heeft waarvoor DNA onderzoek gewenst is. Dus gaat het ziekenhuis het genoom bepalen van zowel je kind als van jou en je partner, om die met elkaar te kunnen vergelijken. Dat is in sommige gevallen een krachtig en belangrijk hulpmiddel, daar sta ik achter. Maar bedenk wel dat het niet veel persoonlijker kan worden dan je DNA als het om persoonlijke data gaat. De manieren waarop die informatie misbruikt kan worden zijn angstaanjagend. Dus misschien wil je over een paar jaar, als je er geen meerwaarde in ziet dat het ziekenhuis die informatie bewaart, dat die verwijderd wordt. Immers, het is niet de vraag óf informatie gestolen kan worden, maar wie er bereid is voldoende moeite voor te doen. Dat betekent dus dat je zelf moet onthouden dat het ziekenhuis die informatie heeft, en jezelf er over vijf jaar aan herinneren dat je daar nog eens goed over na moet denken. Hoe doe je dat? “Hé Siri, herinner me over vijf jaar dat ik nadenk of ik onze DNA informatie wil laten verwijderen.” Dat voelt niet als een betrouwbare methode.

Maar het is natuurlijk veel meer. Ik wil een aanhanger huren bij een autogarage. Ze vragen mij om een identiteitsbewijs om er een kopie van te maken. Ik heb gezegd dat ze dat niet krijgen omdat ze dat

---

[1] Ik ben een software architect met een passie voor privacy en digitale identiteit. Ik werk in het “Digital Trust” lab van Philips Research. De opvattingen in dit artikel zijn die van mijzelf, niet noodzakelijk die van mijn werkgever.

[2] Ik heb overigens nog geen manier kunnen vinden om de “gecheckte ID” weer te verwijderen.

helemaal niet mogen. Je raadt het antwoord al: “Dat is prima, maar dan krijg jij geen aanhanger mee.” Oké, ik heb dus een kopie van mijn identiteitsbewijs gegeven (die ik thuis al had gemaakt met behulp van de “Kopie ID” app, en waarop ik mijn foto, geboortedatum, geboorteplaats en BSN onleesbaar had gemaakt, en die ik heb voorzien van een watermerk). Gelukkig accepteerden ze dat. Maar heel veel hotels accepteren dat niet. Wat doe je dan? Dan geef je dus toch maar je paspoort af en hoop je maar dat het goed komt.[3]

Laatste voorbeeld. In Nederland hebben we gelukkig veel geregeld voor kinderen die extra behoeftes hebben om te kunnen leren, bijvoorbeeld in de vorm van Speciaal Onderwijs. Om daarvoor in aanmerking te kunnen komen moet je een toelatingsverklaring (TLV) hebben. Het proces om die te krijgen houdt in dat er meerdere “deskundigen” (bv medewerkers van dagopvang/school) worden gehoord, en dat medische informatie in beschouwing wordt genomen. Daar komt dan een rapport uit met een samenvatting, en de TLV zelf. Die TLV zegt alleen maar: we hebben alle informatie beoordeeld en op basis daarvan mag dit kind toegelaten worden op speciaal onderwijs. Die TLV heb je ook nodig om bij de gemeente leerlingenvervoer aan te kunnen vragen. Nu zegt de gemeenteambtenaar ineens: alleen de TLV is niet genoeg, we moeten ook het hele rapport zelf hebben. Dat is niet waar. Bij navraag op school vraag een gemeente daar normaal nooit om. Het is ook extreem privacygevoelige informatie. Zeg je dan “nee” tegen de gemeenteambtenaar? Het zal misschien niet direct invloed hebben op de toekenning van het leerlingenvervoer. Maar de kans dat zo’n ambtenaar nog bereid is veel energie te steken in het met je meedenken zou wel eens flink afgenomen kunnen zijn.

Wat verwacht ik van de overheid?

Kennis van Zaken
De digitale samenleving is al een feit, en het gaat niet minder digitaal worden. Leiderschap vanuit de overheid is essentieel, omdat er aspecten zijn die niet aan de markt overgelaten kunnen worden. Dit vereist een hoger niveau van expertise bij de overheid. Discussies worden teveel vertroebeld door onwaarheden en onbegrip. Zie de discussie over “backdoors” bij encryptie. Iedereen gebruikt dezelfde software, dezelfde netwerkprotocollen, hetzelfde internet. Er zijn maar twee mogelijkheden: óf we maken onze hulpmiddelen veilig, en daarmee dus ook die van de “slechteriken”, óf we maken onze hulpmiddelen kwetsbaar om die slechteriken aan te kunnen vallen, en daarmee dus ook onszelf kwetsbaar. Dat is de keuze.

Ik verwacht niet dat ministers en staatssecretarissen zelf experts worden. Ik verwacht wél dat ze zorgen dat ze zichzelf en CIO’s omringen met experts. Laten we zorgen dat niet alleen de functie gecreëerd wordt waar nodig, maar ook dat er een carrièrepad naar die functie wordt gecreëerd.[4]

Publieke Infrastructuur
De overheid moet zorgen voor publieke basisinfrastructuur. Dat zie je bijvoorbeeld bij digitale identiteit. Als je het ze vraagt, bevestigen bedrijven dat ze behoefte hebben aan zo’n basisinfrastructuur voor digitale identiteit, maar geen enkel bedrijf gaat die bouwen. En als samenleving moeten we dat ook niet willen, want het is het fundament waarop alle andere diensten worden gebouwd. Dit fundament moet onvoorwaardelijk vertrouwd kunnen worden. Dus het moet niet door een bedrijf gemaakt worden, want dan heeft dat bedrijf er veel te veel controle over. Het moet *self-sovereign*[5] zijn. Het moet *open source*

---

[3] Als je wil weten hoe verschrikkelijk dat mis kan gaan moet je het verhaal van BNR Nieuwsradio journalist Kevin Goes maar eens opzoeken.

[4] Bruce Schneier, wereldberoemde autoriteit op het gebied van security en privacy, heeft een goed pleidooi hiervoor gedaan: https://www.youtube.com/watch?v=U2jn4pXDZn0

[5] Dit is zo’n concept dat beslissers in de overheid moeten kennen, het zou niet nodig moeten zijn om het uit te leggen. Voor de overige lezers: je bent baas over je eigen identiteit. Je maakt die zelf, en kan vervolgens van andere partijen attributen verkrijgen die iets zeggen over jouw identiteit. Bijvoorbeeld de overheid kan mij een attribuut geven waarmee ik kan aantonen dat ik ouder dan 18 jaar ben als ik alcohol ga kopen, zonder verder ook maar iets over mezelf prijs te hoeven geven. Facebook kan je een attribuut geven waarmee je in kan loggen in Facebook. Dit in tegenstelling tot hoe Facebook logins nu werken, waarbij het Amerikaanse bedrijf Facebook de macht heeft om jou de toegang te ontzeggen tot *alle* diensten waarbij je je Facebook login gebruikt.

zijn. Eventuele servers moeten in Nederland staan, maar liever nog moeten systemen zoveel mogelijk decentraal opgezet worden, gebaseerd op peer-to-peer technologie. Het moet transparantie bieden: wanneer heb ik welke data met wie gedeeld? En het moet helpen met verwijderen van data, bijvoorbeeld door dat standaard na een bepaalde tijd automatisch te doen, en door herinneringen aan de gebruiker te geven.

Ik heb hoge verwachtingen van IRMA, omdat de uitgangspunten van IRMA de goede zijn, en het wordt ontwikkeld door een non-profit stichting.[6]

Data-minimalisatie
Ik ben blij met de AVG. Het is een flinke stap in de goede richting. Het is op zichzelf echter niet genoeg. De volgende stap is namelijk om basisinfrastructuur en systemen op te zetten die op het principe van data-minimalisatie *ontworpen* zijn. Dankzij de bijna dagelijkse onthullingen over data diefstal en *ransomware* aanvallen realiseren bedrijven en instellingen zich steeds meer dat data aansprakelijkheid met zich meebrengt. We leven in een wereld waarin het bewaren van data goedkoper lijkt dan het nadenken over welke data wel en niet bewaard moeten worden. Data heeft ook een ietwat magische belofte: laten we maar zoveel mogelijk data verzamelen, je weet nooit waar het in de toekomst goed voor is. Maar *data is giftig*.[7] Systemen moeten zodanig ontworpen worden dat de weg van de minste weerstand de *goede* weg is.

Voorbeeldfunctie
De lat voor deze basisinfrastructuur op het gebied van gebruikersvriendelijkheid en transparantie moet zéér hoog liggen. Enerzijds omdat het door zeer veel mensen gebruikt zal worden, en anderzijds omdat de overheid het goede voorbeeld moet geven voor diensten die op die infrastructuur gebouwd worden. Immers, als de overheid hierin steken laat vallen, kan je er vergif op innemen dat bedrijven ook niet het achterste van hun tong laten zien.

Beeldvorming
Iedereen vindt privacy belangrijk. Niemand wil een camera in huis die 24x7 alles wat er gebeurt op internet zet. Maar als je bepaalde gegevens over jezelf liever niet verstrekt, wordt je regelmatig raar aangekeken met zo'n blik van "waar doe je nou moeilijk over, joh?" Als ik mijn kind inschrijf op school, wil ik niet dat mijn religie wordt gevraagd. Niet relevant. Als ik een account maak op een web site, wil ik niet dat ik verplicht mijn geboortedatum in moet vullen. Niet relevant. Geslacht? Niet relevant. We moeten naar een situatie waarin het normaal is als je er voor kiest geen WhatsApp te gebruiken omdat je Facebook niet met je gegevens vertrouwt. Waarin het normaal is dat je niet je paspoort hoeft af te geven bij de hotelbalie. Dit gaat niet vanzelf, en de voorbeeldfunctie en voorlichting vanuit de overheid spelen hierin een cruciale rol.

Samenvattend

- Zorg voor voldoende kennis van zaken bij beslissers door daarvoor een functie en carrièrepad te creëren;
- Zorg voor een *publieke* basisinfrastructuur die begint met *self-sovereign* digitale identiteit;
- Maak data-minimalisatie een uitgangspunt, al in de ontwerpfase van systemen;
- Besef dat je als overheid een voorbeeldfunctie hebt op het gebied van gebruikersvriendelijkheid en transparantie;
- Besteed gericht aandacht aan de beeldvorming om burgers te ondersteunen in hun behoefte aan privacy.

---

[6] Stichting Privacy by Design, https://privacybydesign.foundation

[7] "Data is a toxic asset, so why not throw it out?", Bruce Schneier. https://www.schneier.com/essays/archives/2016/03/data_is_a_toxic_asse.html