

PDF hosted at the Radboud Repository of the Radboud University Nijmegen

The following full text is a publisher's version.

For additional information about this publication click this link.

<http://hdl.handle.net/2066/120056>

Please be advised that this information was generated on 2019-10-18 and may be subject to change.

Wat ben je?

BART JACOBS

Hoogleraar computerbeveiliging; lid nationale Cyber Security Raad

In een ziekenhuis gaan we ervan uit dat mensen in een witte jas tot de medische staf behoren. We nemen hun raad serieus. Ze zouden raar opkijken als we bij een consult eerst om hun diploma's zouden vragen – terwijl zo'n vraag eigenlijk volkomen terecht is. Dat we hem niet stellen, komt doordat we vertrouwen op de context: de witte jassen werken in een gebouw waar ZIEKENHUIS op staat en gedragen zich zoals we van medisch personeel verwachten. Maar zouden we ook online, op het web, medisch advies klakkeloos opvolgen dat tot ons komt via een website met een plaatje van iemand in een witte jas? De vraag naar medische kwalificaties is ineens een stuk relevanter. Op het web ontbreekt een vergelijkbare vertrouwenwekkende context. Sterker nog, online is het zeer eenvoudig om de context te manipuleren. Oplichters maken bijvoorbeeld met groot gemak een nepwebsite voor internetbankieren.

Dit voorbeeld toont aan hoe belangrijk het is om online zeker te zijn met wie je te doen hebt. Er blijkt veel schuil te gaan achter dit simpele woordje: 'wie'. Het gaat er niet zozeer om dat we weten dat de witte jas 'Meijer' of 'Bernard' heet; belangrijk is dat deze witte jas een gekwalificeerde dokter is. De identiteit, bijvoorbeeld gegeven door de naam, is zeker relevant, bijvoorbeeld in het sociale verkeer, bij het maken van een vervolgspraak, of bij het indienen van een klacht, maar van het grootste belang is toch de eigenschap 'dokter'. Kortom, *wat* je bent is belangrijker dan *wie* je bent.

Deze eigenschappen van mensen, ook wel attributen genoemd, spelen een grote, vanzelfsprekende rol in ons sociale leven. In het zwembad bepaalt het man/vrouw-attribuut (en niet je naam) naar welke kleedkamer je behoort te gaan. In een winkel bepaalt en-

kel het attribuut 'boven de 18' of je een heftige game of een fles sterkedrank mag kopen. In de praktijk gebruiken we veel verschillende eigenschappen, in wisselende combinaties, die als deelidentiteiten begrepen kunnen worden. Zo zijn op het werk andere attributen van belang dan bij de voetbalclub. Sommige attributen zijn uniek-bepalend, zoals je burgerservicenummer (bsn), je mobiele nummer, je bankrekeningnummer, het nummer van je gepersonaliseerde ov-chipkaart. Maar minstens zo nuttige attributen kunnen op meerdere personen van toepassing zijn, zoals geslacht, meerderjarigheid, Nederlanderschap, lidmaatschap, abonnementhouderschap, etc. Dergelijke attributen zijn niet-identificerend en kunnen een bepaalde mate van anonimiteit bewerkstelligen.

Bij de digitalisering van het sociale verkeer is het belangrijk zorgvuldig met zulke deelidentiteiten en attributen om te gaan, omdat nauwe aansluiting bij een intuïtieve sociale ervaring het vertrouwen en gebruiksgemak vergroot. Daarbij zijn verschillende grote belangen in het geding, zowel commercieel als maatschappelijk (veiligheid, fraudebestrijding, privacybescherming). In de onlinepraktijk zien we dat attributen nog niet of nauwelijks gebruikt worden. Aanbieders van (commerciële) diensten op het web willen graag bijhouden *wie* hun klanten zijn – denk aan Google, dat steeds vraagt in te loggen – en welke voorkeuren ze hebben, om daarmee advertenties zo gericht mogelijk te kunnen plaatsen. De digitalisering van de afgelopen decennia heeft geleid tot een vergaand gebruik van unieke identiteiten, ook als daar puur functioneel gezien geen enkele noodzaak toe is.

Is dat erg? Dat is zeker erg als je ook maar enigszins gehecht bent aan je privacy en niet wil dat wat je in verschillende contexten met verschillende deelidentiteiten doet onderling gekoppeld raakt, en in allerlei situaties weer op kan duiken. Het is ook erg als je je zorgen maakt om identiteitsfraude, waarbij bijvoorbeeld iemand anders jouw identiteit misbruikt en op jouw naam een lening of een mobiel abonnement afsluit. En het is ook erg als je wil dat burgers en klanten meer gebruikmaken van de digitale

infrastructuur, maar constateert dat ze dat niet doen vanwege een gebrek aan vertrouwen.

Nu is het makkelijk om te eisen dat er ook online op een intuïtieve en privacyvriendelijke manier met attributen omgegaan moet worden. De technische mogelijkheden moeten er natuurlijk wel zijn om dat op een betrouwbare wijze te doen, zodat je kleine neefje niet jouw ‘boven de 18’-attribuut kan misbruiken om online allerlei ongepaste zaken te bekijken of te bestellen. Het goede nieuws is dat die betrouwbare techniek er sinds kort is, in de vorm van attribuut-gebaseerde *credentials* die op een chipkaart geladen kunnen worden. Zo’n chipkaart vormt een handige, goed beveiligde drager. Het IRMA-project van de Radboud Universiteit Nijmegen, TNO, SURFnet en SIDN realiseert deze technieken (via opensourcesoftware, zie de bijbehorende website). Daarmee vervalt het excuus dat in de digitale wereld altijd vastgelegd moet worden met wie men van doen heeft: met een IRMA-kaart kun je online bijvoorbeeld bewijzen dat je boven (of onder) een bepaalde leeftijd bent voordat je toegang krijgt tot een bepaalde website, zonder verder iets anders van jezelf bloot te geven. Het spectrum aan mogelijke attributen is in principe onbeperkt, en kan zowel toegangskaatjes tot concerten als basale medische gegevens in een microdossier omvatten (denk aan medicijngebruik of allergieën).

Deze verschuiving van *wie* je bent naar *wat* je bent gaat in de digitale wereld voor een revolutie zorgen. Het beheer van een eigen waaier aan attributen kan plaatsvinden zoals nu bijvoorbeeld apps op een smartphone of tablet beheerd worden: je kunt attributen van jezelf bij een vertrouwde bron downloaden, verversen of verwijderen; je kunt geselecteerde attributen in verschillende situaties, zowel online als offline (in een winkel of bij een balie) tonen, namelijk precies die eigenschappen die noodzakelijk zijn voor de transactie. Beschikbaarheid en toegankelijkheid van informatie en diensten is een groot goed, maar vergt gepaste controle om misbruik en oplichting tegen te gaan en de betrokkenen

te beschermen. Daarmee wordt de digitale wereld meer zoals de dagelijkse, niet-digitale wereld. Een dergelijke vertrouwensbasis leidt tot innovatieve digitale kansen en mogelijkheden.

Onder experts op het gebied van digitaal identiteitsbeheer heerst een grote mate van consensus dat elektronische attributen (*wat* in plaats van *wie*) een belangrijke stap voorwaarts vormen. De kennis is aanwezig, vooral in Nederland, voor een open realisatie van een attribuut-gebaseerde infrastructuur zonder machtsconcentratie bij grote informatiemonopolisten. De vraag is: wie ziet de kansen en grijpt ze, en verandert daarmee de wereld?