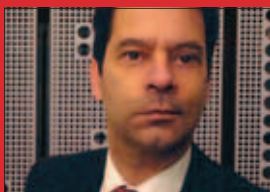




PRIVACY, ONDERNEMERS... EN INTERNETPROVIDERS

Het luid klinkende pleidooi online privacy te versterken door allereerst te kiezen voor andere aanbieders van internetdiensten roept een aantal vragen op. Dat heeft vooral te maken met het feit dat die andere aanbieders beoordeeld moeten kunnen worden, maar er geen sprake lijkt te zijn van eenheid in communicatie en definities.



*Rashid Niamat is journalist en werkzaam bij ISPam.
Rashid is te bereiken via rashid@niamatmediagroup.nl*

Medio december waren in Amsterdam twee events waar privacy centraal stond. Pl.lab [1] organiseerde de jaarlijkse bijeenkomst waarbij inzicht werd gegeven in lopende onderzoeken. Dit gebeurde door workshops en presentaties waarin privacy centraal stond. De andere activiteit was de tiende editie van de Big Brother Awards. Dat ook hier privacy centraal stond behoeft geen nadere uitleg.

Decentralisatie en distributie van data

Wat deze twee activiteiten verder gemeen hebben is dat onherroepelijk de machtspositie van een beperkt aantal grote partijen ter sprake kwam. Tijdens de keynote van Ian Goldberg [2] op Pl.lab werd, net als bij de latere workshop van Mireille Hildebrandt "TETs for PETs, transparency tools for profiling in social networks", duidelijk dat Facebook en Google de nodige aandacht verdienen. De keynote van Aral Balkan [3] tijdens de BBAX [4] deed daar niet voor onder. Hij illustreerde op heldere wijze waarom privacy en dit soort grote bedrijven per definitie nooit een gezonde combinatie zijn. Goldberg en Balkan pleitten voor verschillende oplossingen die een ding gemeen leken te hebben: stap af van de voorkeur voor dit soort giganten, kies voor decentrale opslag van data en andere distributie modellen. Dat klinkt logisch, zeker voor wie de enthousiast ontvangen presentaties van beide heren heeft gevolgd, maar iets ontbreekt. Wat bij dit soort betogen namelijk centraal staat zijn de burger, de consument en die paar grote Amerikaanse ondernemingen. Wat geheel ontbreekt is dat privacy iets is dat ook het bedrijfsleven raakt.

Focus moet breder

Die constatering is Goldberg voorgelegd: waarom alleen de focus en voorlichting voor de consument. Zou het niet beter zijn eveneens aandacht te besteden aan alle ondernemers. Zij zitten zo mogelijk in een nog lastigere positie dan de doorsnee consument. Zij vergaren en verwerken immers data van derden (de klanten) maar zijn zelf ook weer afhankelijk van leveranciers die dit mogelijk moeten maken. Goldberg was het volledig eens met dat standpunt. Ja natuurlijk moeten – vooral – kleinere ondernemers te horen krijgen hoe zij kunnen bijdragen aan meer en betere privacy voor hun klanten en voor zich zelf. En onvermijdelijk volgde daarop de vraag: wie moet dat dan doen? Moet je van de overheid verwachten dat die frequent voorlichting geeft aan ondernemers door het toezenden van een gedrukt exemplaar van de WBP? Wie kijkt naar de privacy incidenten die afgelopen jaar de landelijke pers hebben gehaald en waarbij Nederlandse ondernemers blijkbaar de fout in zijn gegaan moet de indruk krijgen dat het bijbrengen van zulke basiskennis wel het minste is dat nodig is. Maar de kans dat de overheid dit doet met enig effect is gering. Daarom is

het wellicht verstandiger het initiatief te laten aan bepaalde marktpartijen en belangenorganisaties.

Waarom nationale aanbieders

Er is een type ondernemer dat dan direct genoemd moet worden. Als je namelijk – in lijn met het pleidooi van zowel Goldberg als Balkan – kiest voor decentrale opslag van data kom je vanzelf uit bij partijen van een hele andere omvang dan Google en co. Nederlandse ICT bedrijven, in deze context vooral de providers, zijn heel goed in staat diensten op Nederlandse bodem (wel zo handig als je privacy hoog in het vaandel hebt staan) aan te bieden die privacyvriendelijk zijn. Dat klinkt onvermijdelijk als een verkoopargument, maar het is eigenlijk iets anders. Tijdens de Pl.lab bijeenkomst werden de aanwezigen door Rence Damming, de privacy officer van KPN, gewezen op een simpele bevinding: wat klanten van KPN verwachten is Trust. Met andere woorden privacy, als onderdeel van het brede begrip Trust, is een verwachting. Het is dus vraag in plaats van aanbod. Dat KPN daar naar behoren invulling aan geeft en op meerdere plekken prominent aandacht besteedt aan privacy, inmiddels ook in de commerciële uitingen, is daarmee niet meer dan logisch en verstandig.

KPN is echter niet de enige aanbieder van provider diensten in Nederland. Afhankelijk van de definitie zijn het tussen de 800 en 2.000 ondernemers die een of meerdere e-diensten aanbieden waarbij data wordt opgeslagen en/of verwerkt. Hebben die allemaal de zaken net zo goed voor elkaar als KPN? Voldoen zij al in de eerste contactmomenten (lees: het bezoeken van de website) aan de schijnbaar aanwezige verwachting van prospects en klanten om hier iets over te vinden?

Privacykennis bij de providers

Meten is weten! De eerste constatering is, dat op basis van een steekproef door het bezoeken van twintig willekeurig gekozen provider websites, zeker niet iedereen het belang van privacy lijkt in te zien. In ieder geval is duidelijk dat er op verschillende wijze invulling aan wordt gegeven. Er zijn enkele partijen die in de privacy policy keurig melden persoonsgegevens te verwerken en dit bij het CBP te hebben aangemeld. De meesten maken daar geen melding van. Of zij bekend zijn met WBP en CBP blijft vooralsnog gissen, de verstrekte informatie reikt niet verder dan dat in de leveringsvoorwaarden is opgenomen dat men uiterst professioneel met klantdata omgaat. Een aparte vermelding van het begrip privacy, laat staan een verwijzing naar data minimalisatie als leidraad, op de website via een privacy statement of opname in de FAQ ontbreekt. Als het voor die ondernemers al niet top-of-mind is dat ze hier kunnen dan wel moeten communiceren, hoe kun je dan

verwachten dat zij in staat zijn de klanten (pro-) actief over deze materie te informeren of zelfs te adviseren.

Een aantal providers is vervolgens de bewust open vraag voorgelegd: wat betekent privacy voor je onderneming. TransIP [5], een van de grootste aanbieders van domeinnamen, hostingservices en VPS in het land, werd gekozen omdat het op de voorpagina een intrigerende melding heeft staan: "We gaan voorzichtig om met jouw privacy gevoelige gegevens. Omdat we telefonisch niet met zekerheid kunnen vaststellen wie ons belt, verzoeken we je voor inhoudelijke vragen het controlepaneel te gebruiken." Dit lijkt een mooi voorbeeld te zijn van privacy-awareness uitstralen en zo indirect je klanten bewust te maken dat ook op dit niveau privacy een rol speelt. Maar goed, privacy wat betekent dat (verder) voor TransIP? Het antwoord maakt duidelijk dat men heel goed doorheeft een dubbele rol te vervullen: "Wij beheren niet alleen de persoonlijke informatie van meer dan 120.000 klanten, onze klanten beheren ook persoonlijke of privacy-gevoelige data". Dat betekent concreet: "systemen zodanig in te richten dat wij niet direct bij persoonlijke gegevens kunnen". Verder wordt er nog gewezen op het principe van dataversleuteling en het feit dat TransIP medewerkers zelf niet zomaar bij persoonlijke gegevens kunnen komen.

Een andere aanbieder die is benaderd, Fundaments [6], is een IaaS provider. IaaS staat voor de onderste cloudlaag en daarmee het type provider dat – in tegenstelling tot partijen als TransIP – in principe geen eindgebruikers als klant heeft. Het antwoord op dezelfde vraag was daardoor compleet anders: "Wanneer je privacy serieus neemt, dien je te kijken naar de hele keten van de dienstverlening: een applicatie kan nog zo goed beveiligd zijn, maar als in de onderliggende infra de data te grabbel ligt, is het een schijnbeveiliging. Vanuit deze ketenvisie proberen we de juist de onderliggende infrastructuur en virtualisatie software zo krachtig mogelijk te kiezen."

Het begrip ketenvisie illustreert in dit antwoord treffend de rol van een provider. Hij is een schakel in het geheel, maar wel een waaraan aanvullende eisen gesteld worden die veel minder vaak voorkomen bij partijen elders in de keten. Het is daarom ook verklaarbaar waarom partijen als Fundaments door ISO en/of NEN certificering aantonen de zaakjes voor elkaar te hebben. Overigens was dat een punt waar ook met Goldberg over is gesproken. Zag hij mogelijkheden de nieuwe ISO certificering voor cloud diensten [7] in te zetten om privacy (awareness) van elk type gebruiker te vergroten? Goldberg ziet het als een interessante optie waar hij echter nog te weinig van afwist om een tot een beter onderbouwd oordeel te komen.

Stellen dat je je zaakjes voor elkaar hebt of een intrigerende beschrijving op je website dat je privacy hoog in het vaandel hebt staan, is een manier van communiceren. Vervolgens is gevraagd: hoe pro-actief zijn jullie op dat vlak? Hier werd het verschil tussen de beide providers door de plek die ze in de waardeketen hebben en de diensten duidelijk. Bij de IaaS provider is maatwerk de regel. Dat betekent dat in offertes, contracten en SLA's ruimte is aandacht te besteden aan dat onderwerp. Voorbeeld daarvan was de opmerking dat: "privacy- en beveiligingsmechanismen dienen te worden ondersteund door de leveranciers. De keuze voor leveranciers is daarmee onderhevig aan harde eisen". Voor de meer standaarddiensten die TransIP levert is de communicatie per definitie anders en daarmee ook de mogelijkheid pro-actief te acteren. Desalniettemin, is er een heldere uitgebreide privacy-policy waarnaar vanaf elke pagina wordt gelinkt en er is de policy, "als er vragen over [privacy] worden gesteld zullen wij deze helder beantwoorden".

Conclusie

Het verschil tussen de providers die reageerden op de vragen (een aantal deed dat overigens niet) en wat er op basis van de steekproef is geconstateerd blijft opvallend. Als burgers en bedrijven meer en betere privacy maatregelen willen voor e-communicatie, digitale opslag en verwerking is er nog een hoop werk te verrichten. De kans dat alle providers hier een rol willen en kunnen vervullen lijkt vooralsnog klein, omdat niet iedereen op het zelfde kennisniveau zit. De vraag of en hoe dit kan worden gerealiseerd is lastig te beantwoorden. Het ontbreekt in ieder geval aan een verplicht bedrijfsschap voor providers dat kwaliteitseisen zou kunnen opleggen.

Voor iedereen die privacybewust is en zijn eigen data of klantdata koestert, blijft het zaak alert te blijven en niet elke aanbieder op zijn blauwe ogen te geloven. Gelukkig zijn er partijen die de zaakjes wel voor elkaar hebben en daarover helder communiceren. Alleen al dat laatste is een bruikbaar criterium.

Links

- [1] pilab.nl/
- [2] en.wikipedia.org/wiki/Ian_Goldberg
- [3] aralbalkan.com/
- [4] www.bigbrotherawards.nl/
- [5] www.transip.nl
- [6] www.fundaments.nl
- [7] www.iso.org/iso/catalogue_detail?csnumber=60545