Door Jurgen van der Vlugt

Privacy by design

Privacy op orde in drie stappen

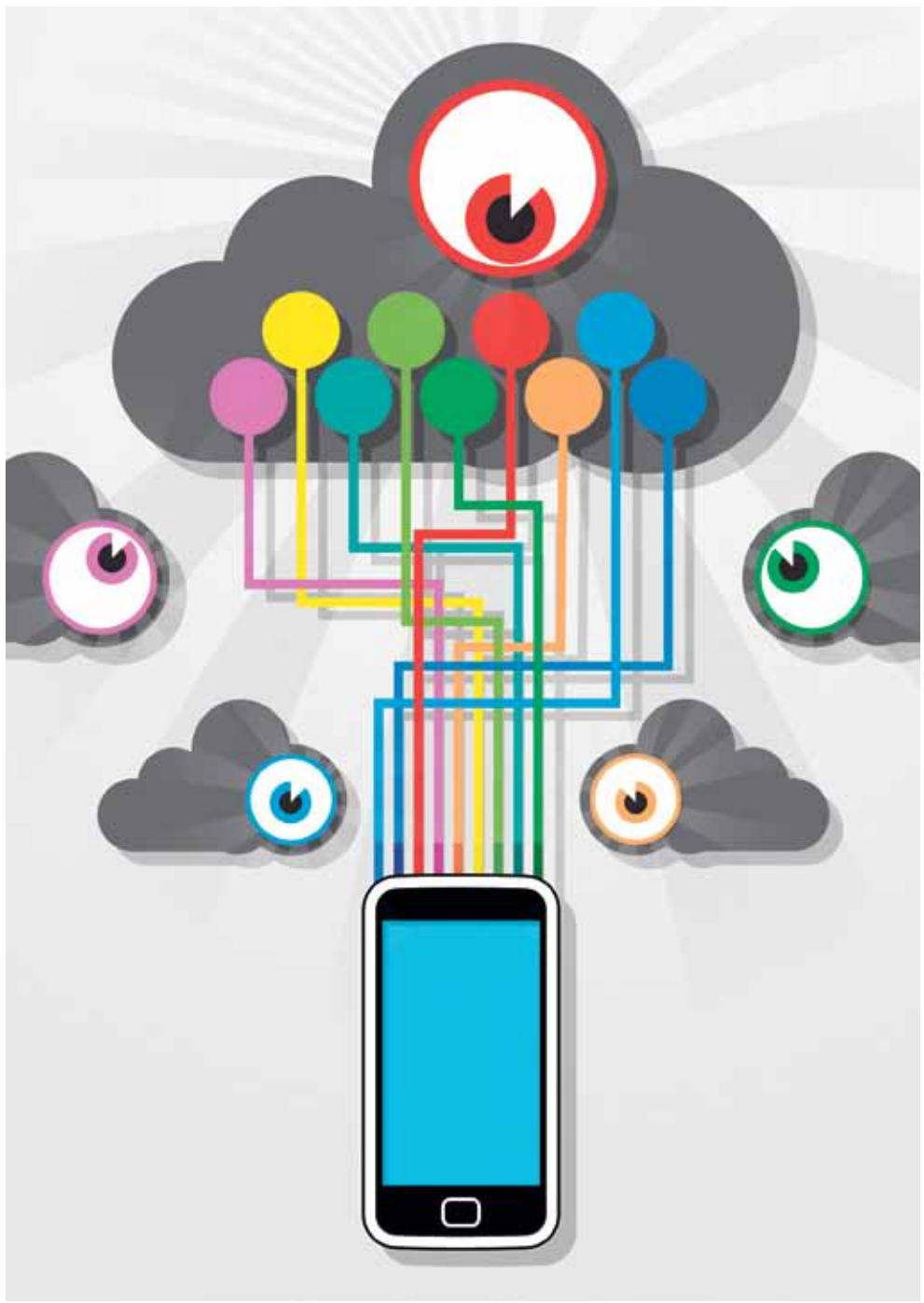
VUGHT - Zeker in tijden van big data lijkt het wel alsof we niet genoeg kunnen verzamelen. Alleen al voor het gemak. Hoe meer data we van en over klanten verzamelen (identificerende gegevens, masterdata, en transactie- en gedragsgegevens), hoe gemakkelijker we onze systemen kunnen bouwen. Met alle verzameldrang komt ook de privacy om de hoek.

Klanten willen zowel privacy als gebruiksgemak (van de site), maar zien zich vaak gesteld voor een 'Hobson's Choice': *take it (all) or leave it*. Zonder de 'benodigde' gegevens te leveren, komt een klant er niet in. Kennelijk zijn we niet bang dat de klant wegloopt: de concurrent doet even slecht (sic) en de klant denkt ook niet zo over privacy na.
Maar hier is verandering op til; de wetgeving en handhaving worden strenger en de klant kritischer. De klant wil steeds minder identificatie- en andere privacygevoelige gegevens ophoesten, zeker als die niet relevant zijn voor de transactie. De klant heeft sowieso steeds minder vertrouwen in het hele e-commercegebeuren. Als na het ene incident na het andere de conclusie doordringt dat de beloofde afscherming van privé- en privacygevoelige data een wassen neus is, zal de klant langzamerhand steeds minder willig zijn om meer gegevens te delen. Hoe kan dit probleem worden verkleind?

Stap één: Waar we staan
De kunst is om zo min mogelijk in huis te hebben dat risico's zou kunnen vormen. Dat betekent dat we, stap één, flink moeten spitten en nadenken om te weten te komen hoe groot de schade op dit moment eigenlijk is. We moeten inzicht zien te krijgen in welke data we nu al in huis hebben. Vervolgens moeten we uiteraard bezien of we al die gegevens wel nodig hebben. Dat moet wel in het licht gebeuren van de moeite die het kost om systemen te verbouwen zodat er meer *lean and mean* met gegevens kan worden omgegaan.

Stap twee: Hek erom
Die inventarisatieslag zal veel omvangrijker zijn dan er in het algemeen wordt verwacht. Misschien kan er dan maar beter worden aangesloten bij werk wat toch al gedaan moet worden in stap twee: beveiligen. En wel op zo'n manier dat er in ieder geval geen *mis*bruik van de gegevens kan worden gemaakt. Oneigenlijk gebruik buiten én binnen de organisatie voorkomen, en het liefst *aantoonbaar* in control zijn, is het doel. Hoe minder gegevens onder dit regime vallen, hoe beter. Maar als we toch bezig zijn, kunnen we beter aan de veilige kant gaan zitten. Daar hoort (wettelijk) ook control bij over de gegevens waar derden aan kunnen komen; of die *ergens* in de cloud staan. Maar uw IAM is toch helemaal top, net als uw SIEM, ISO-XYZ-compliance, et cetera. Toch? En u hebt uiteraard volledig zicht op alle advanced persistent threats. Alle informatiebeveiligingszaken waar we in het verleden met veel brandjes blussen nog wel een mager zesje op scoorden, moeten nu veel beter.

Stap drie: Kraan dicht by design
Verbetering van de privacy is ook niet eenvoudig op te lossen door de privacyofficer van buitenaf naar projecten te laten kijken als die al lopen. Want als een timmerman



"De communicatie over privacy blijkt lastig"

een stoel maakt, heeft het niet heel veel zin om halverwege het maakproces twee poten half af te zagen. En die privacyofficer is, door de bank genomen, meer een jurist of een bedrijfskundige dan een *techie*. Natuurlijk is het heel prettig om hoog in de staf over de compliancefijnslijperij te kunnen meepraten en daar enige autoriteit te (kunnen) laten gelden. Maar het betekent ook dat als het erop aankomt, de communicatie binnen een project over privacy lastig blijkt. Het denken over raw data, de emergent-propertyprivacy in het licht van identificeerbaarheid en andere gevoeligheid, en technische en logische slimmigheden om die data niet nodig te hebben ofwel goed te beveiligen, is een berg expertwerk. We kunnen dus beter met Privacy By Design het voortouw nemen zodat het zich vernieuwende systemenlandschap groeit naar iets waar we qua privacy tevreden over kunnen zijn. Dat betekent flink wat specifieke aansturing en control.

Eerst PIA? Liever in PBD
Inhoudelijk is er overigens best wel wat meer te doen dan alleen maar een privacy impact assessment voor de compliancebühne. Zo'n PIA wordt nogal eens verwacht buiten de details van een systeemontwerp om. Dat kán, maar dan wordt juist de mogelijkheid gemist om privacyverbeterende ontwerpkeuzes in te bouwen.
Het wordt pas echt wat als u zich in het privacy-by-systeemontwerp richt op de volgende punten:

1. Minimaliseer; wat je niet in huis hebt, hoef je niet te beveiligen. En anonimiseer en gebruik zo mogelijk pseudoniemen, dan is er al minder in huis waarmee iets zou kunnen misgaan.
2. Zorg voor goede afscherming door de architectuur. Dat betekent dat de gegevensverwerking zo veel mogelijk 'onder water' dient te gebeuren. En transparante encryptie kan zorgen voor afscherming van de datasets als collectief.
3. Werk waar mogelijk met reeds geaggregeerde gegevens. Door alleen een 'tussenstand' (aggregatie over tijd) van bepaalde gegevens bij te houden bijvoorbeeld, blijven identificerende (gedrags)patronen buiten beeld.
4. Doe de gegevensverwerking zoveel mogelijk gedistribueerd. Dit voorkomt dat iemand die ongewenste toegang heeft tot gegevens op een locatie, al te veel gegevens ineens te pakken kan krijgen.

De keuzes die we zo maken, hebben een sterke invloed op de mogelijke, haalbare privacy. Een PIA doen zonder deze details in het oog te houden, levert dan ook vaak gemeenplaatsen op met onvoldoende handvatten voor verstandige ontwerpkeuzes. Een PIA hanteren als graadmeter voor de privacykwaliteit van een systeem dat we aan het ontwerpen zijn, helpt daarentegen om de privacy daar te brengen waar we dat willen en moeten hebben. In die volgorde.

Begin met aftellen
Samenvattend kunnen we dus al met drie stappen thuis zijn. Waarbij het aftellen beter met stap drie kan beginnen... Zelfs uw auditors zullen moeten accepteren dat 'in control zijn' niet betekent 'foutloos zijn', maar wel: de verbeterpunten kennen en daar planmatig aan werken. *First things first*: eerst de kraan van nieuwe systemen qua privacy 'under control' krijgen, en dan de huidige plas

"Zelfs auditors moeten accepteren dat 'in control zijn' niet betekent 'foutloos zijn'"

gebreken opdweilen – als die niet al vanzelf opdroogt. Maar ga wel zelf aan de gang voor het te laat is. Immers, liever zelf sturen dan gestuurd worden.

Ir. drs. J. van der Vlugt RE CISA CRISC RCX CCX (i.e., Jurgen) is auditor (IT) bij een internationale organisatie, met uitgebreide ervaring in externe en interne IS-audit, -advies en -consultancyrollen bij onder andere KPMG en ABN Amro Bank. Hij is een vaste auteur van het Cqure Kennisplatform, waar dit artikel eerder is gepubliceerd.