Cloud security in vogelvlucht

Wolter Pieters, Universiteit Twente

Cloud computing is dé hype in IT op het moment, en hoewel veel aspecten niet nieuw zijn, leidt het concept wel tot de noodzaak voor nieuwe vormen van beveiliging. Het idee van cloud computing biedt echter ook juist kansen om hierover na te denken: wat is de rol van informatiebeveiliging in een wereldwijd netwerk van afhankelijkheden? Op een workshop in Brussel in januari 2010 kwamen experts uit technische, juridische en filosofische hoek bijeen om hierover van gedachten te wisselen. Binnenkort verschijnen de bijbehorende artikelen in het boek “Computers, privacy and data protection: an element of choice” (Gutwirth et al., 2011). Ter gelegenheid daarvan een overzicht over het thema.

Massaproductie

Wat opvalt is dat zowel begrippen als gevolgen nog niet duidelijk in kaart gebracht zijn. Dat geldt in eerste instantie voor het begrip cloud computing zelf. Volgens Paolo Balboni, advocaat en lid van de European Privacy Association, is het karakteristieke van cloud computing dat het als een “commodity”, een massaproduct, wordt aangeboden. Daardoor is, in tegenstelling tot bij outsourcing, onderhandeling over de voorwaarden vaak onmogelijk. Net zoals je niet kunt onderhandelen over de eigenschappen van artikelen in de supermarkt.

Deze standaardisatie van voorwaarden heeft belangrijke gevolgen. In de bestaande privacywetgeving is sprake van een “data subject”, “data controller” en “data processor”. Hierbij wordt er van uit gegaan dat de data controller verantwoordelijk is voor de informatieverwerking, en dat deze kan controleren dat de uitvoering daarvan door de data processor ook daadwerkelijk aan de eisen voldoet. Juist die auditing is in een cloud scenario echter vaak onmogelijk: je kunt niet even bij Google of Amazon binnenwandelen en kijken hoe het met de beveiliging staat. Daardoor moeten deze begrippen wellicht in een nieuwe versie van de wetgeving, die op dit moment in voorbereiding is, worden herzien. De wet zal echter pas over een jaar of vijf van kracht worden, en de vraag is natuurlijk hoe de technologie zich in de tussentijd ontwikkelt.

Een ander belangrijk juridisch struikelblok is de locatie van de data. Privacygevoelige data mag niet zomaar naar alle landen worden geëxporteerd, maar hoe kun je dit beleid afdwingen? Immers, je kunt je data wel aan een Nederlands bedrijf in beheer geven, maar het zou best kunnen dat via een aantal stappen de data toch in India terechtkomt. Dit kun je natuurlijk in je contract uitsluiten, maar interessanter is wellicht of er technische oplossingen te bedenken zijn voor dit probleem. Dit is dan vergelijkbaar met het zogenaamde “location-aware access control” (Van Cleeff et al., 2010), alleen gaat het dan niet om de locatie van de gebruiker, maar om de locatie van de data zelf. Vergelijkbare oplossingen zijn al voorgesteld voor het ontoegankelijk maken van gegevens na een verloopdatum, dus voor tijd in plaats van locatie (zie bijvoorbeeld Tang, 2010).

Versleuteld bewerken

In het algemeen is het versturen van data in de cloud met behulp van standaard PKI technieken goed te doen. Afgezien van het vraagstuk van locatie is ook opslag in de cloud niet zo moeilijk: je versleutelt de data, stuurt ze naar een server, haalt ze weer op als je ze nodig hebt, en ontsleutelt ze dan weer. Ze kunnen dan door de server niet gelezen worden.

Eventueel kun je ook de integriteit nog controleren met een hash of een handtekening. De grote vragen liggen op het gebied van het *bewerken* van data in de cloud.

Afgelopen jaar is er een theoretische doorbraak bereikt op het gebied van versleuteling. Het grote vraagstuk dat is opgelost is of het mogelijk is een versleutelingsmethode te maken waarmee je willekeurige bewerkingen kunt toepassen op versleutelde data, zodat je de data niet meer “in the clear” hoeft te hebben om deze te kunnen bewerken. Met het zogenaamde *fully homomorphic encryption* zou dit mogelijk zijn. Hiermee kun je versleutelde gegevens optellen èn vermenigvuldigen, en je kunt laten zien dat daarmee alle mogelijke bewerkingen voorhanden zijn. Er is dus nu theoretisch aangetoond dat zo’n methode bestaat (Gentry, 2009). Het slechte nieuws is dat dit voor de praktijk nog geen enkele betekenis heeft: de methode is bij lange na niet efficiënt genoeg voor praktische toepassingen.

Voor cloud computing zou fully homomorphic encryption betekenen dat ook de aanname van een “nieuwsgierige” server, die mogelijk je geheimen zou kunnen misbruiken, geen belemmering meer hoeft te vormen voor cloud processing. De server krijgt de plaintext data dan immers nooit te zien, maar bewerkt slechts een versleutelde versie. Nu dit nog niet praktisch is, wat kan er dan wel? Allereerst is er de mogelijkheid van “secure multi-party computation”. Hiermee kun je vergelijkbare dingen doen, namelijk bewerkingen uitvoeren zonder dat de deelnemers de oorspronkelijke data zien. In een bekend voorbeeld willen twee miljonairs weten wie er rijker is, zonder elkaar te vertellen hoeveel geld ze hebben. Echter, zoals de naam al zegt, moet je daarbij data heen en weer sturen. Dit wil je in de cloud nu juist niet: de cloud provider moet zelf de bewerkingen kunnen uitvoeren, want dat is waar de efficiëntiewinst te halen is.

Gelukkig blijkt dat, hoewel willekeurige berekeningen toepassen op versleutelde data nog niet haalbaar is, dit voor specifieke bewerkingen wel degelijk kan. Een beperkte versie van homomorphic encryption (alleen optellen) wordt bijvoorbeeld al toegepast voor het tellen van stemmen in de toekomstige generatie elektronische verkiezingssystemen (zie bijvoorbeeld Cramer et al., 1997). De stemmen kunnen dan in versleutelde vorm worden opgeteld, zodat het stemgeheim gewaarborgd blijft, waarna de uitslag kan worden ontsleuteld.

Ook kunnen we bijvoorbeeld zoeken in versleutelde databases (Brinkman, 2007). Dat laatste gaat als volgt. Voordat het document naar de server wordt verstuurd, voeg je aan het document de keywords toe waar je op wilt kunnen zoeken. Je versleutelt deze gegevens nu zodanig dat de server 1) het document niet kan lezen, en 2) de keywords niet kan zien, maar 3) wel kan controleren of een later aangeboden (versleuteld) keyword overeenkomt met de oorspronkelijke keywords. Je kunt nu dus zoeken in de data zonder dat de server informatie verkrijgt over je document of zoektermen.

Informatievoorzorg

Bovenstaande laat zien dat er in de cloud naast risico’s ook kansen liggen voor informatiebeveiliging, in termen van nieuwe technische mogelijkheden. De vraag die overblijft is of er een algemeen principe ten grondslag ligt aan wat we met informatiebeveiliging willen bereiken in het tijdperk van cloud computing. Op dit moment lijkt beveiliging nog te veel als een uitvoeringskwestie te worden gezien, terwijl het steeds duidelijker wordt dat al in het ontwerp belangrijke keuzes moeten worden gemaakt. In dit kader hebben wij eerder voorgesteld het zogeheten voorzorgsprincipe, dat in de milieuethiek met name binnen de EU zeer succesvol is geweest, ook op IT toe te passen (Pieters en Van

Cleeff, 2009). Daarbij geldt dat bij twijfel over mogelijk misbruik van een systeem, zelfs als niet zeker is hoe groot de kans daarop is, ontwerpmaatregelen moeten worden genomen om dergelijke risico's af te dekken. De vraag die gesteld zou moeten worden is hoe machtsverhoudingen verschuiven door het nieuwe systeem. We hebben hier problemen gezien met de uitbesteding van het verkiezingsproces via stemcomputers, maar het gaat ook over rechten van bijvoorbeeld administrators en veiligheidsdiensten. Een dergelijk principe zou er bijvoorbeeld toe hebben kunnen leiden de vingerafdrukken van de paspoorten *niet* in een centrale database op te slaan, en sociale netwerksites veel eerder te dwingen iets aan hun privacy te doen.

"You decide"

De tendens lijkt op dit moment te zijn vooral in te zetten op gebruikerseducatie ter voorkoming van misbruik van informatie. Zo heeft de overheid actief campagne gevoerd om mensen ervan bewust te maken dat ze niet alle data, zoals wanneer ze met vakantie zijn, zomaar op Internet moeten zetten. In Noorwegen zijn filmpjes gemaakt om kinderen en jongeren te wijzen op de gevaren van sociale netwerksites (www.dubestemmer.no).

Ondanks de sympathieke uitstraling van deze initiatieven lijkt de nadruk op de gebruikers een onmacht te laten zien ten aanzien van de technische mogelijkheden. Het voorzorgsprincipe kan hierin verandering brengen, maar alleen als wij als informatiebeveiligers het standpunt uitdragen dat "in the cloud" informatiebeveiliging niet alleen maar een technische kwestie is, maar iets dat al op beleidsniveau verankerd moet worden. Alleen dan kunnen we ook in de toekomst rekenen op veilige systemen.

Literatuur

Brinkman, R. (2007) *Searching in encrypted data.* PhD thesis, University of Twente. CTIT Ph.D.-thesis series No. 07-98.

Van Cleeff, A., Pieters, W. & Wieringa, R.J. (2010) Benefits of Location-Based Access Control: A Literature Study. To appear in *Proceedings of the 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing (CPSCom-2010).*

Cramer, R., Gennaro, R. & Schoenmakers, B. (1997) A Secure and Optimally Efficient Multi-Authority Election Scheme. *European Transactions on Telecommunications* 8(5): 481-490.

Gutwirth, S., Poullet, Y., De Hert, P. & Leenes, R. (Eds.) (2011) *Computers, Privacy and Data Protection: an Element of Choice*. Dordrecht: Springer. http://www.springer.com/law/international/book/978-94-007-0640-8

Gentry, C. (2009) On homomorphic encryption over circuits of arbitrary depth. In *the 41st ACM Symposium on Theory of Computing (STOC).*

Pieters, W. & Van Cleeff, A. (2009) The Precautionary Principle in a World of Digital Dependencies. *IEEE Computer*, 42 (6):50-56.

Tang, Q. (2010) Timed-Ephemerizer: Make Assured Data Appear and Disappear. In *Sixth European Workshop on Public Key Services, Applications and Infrastructures*. Volume 6391 of LNCS, Berlin: Springer.