

Lucipher maakt cloudopslag veilig



Pieter van Beek en Evert Lammerts moeten zich haasten

De veiligheid van vertrouwelijke gegevens is doorgaans een van de eerste bedenkingen die directies uiten zodra de cloud ter sprake komt. De Nederlandse start-up Lucipher lijkt het ultieme antwoord in huis te hebben. Maar het idee is zo elegant, en eigenlijk ook wel voor de hand liggend, dat het niet waarschijnlijk is dat Lucipher de enige is.

door: ROLF ZAAL / R.ZAAL@SDU.NL beeld: ANTHONY DONNER / ANTHONYDONNER.COM

Start-up Lucipher won begin deze zomer de IBM Mentor Day. Met deze innovatiewedstrijd ondersteunt IBM veelbelovende softwareontwikkelaars in de Benelux. Volgens de jury heeft Lucipher 'een enorme marktpotentie met hun veilige cloudomgeving en maken ze de wereld een stuk slimmer met hun technologie'.

Wordt Lucipher de nieuwe Nederlandse IT-topper? Oprichters Pieter van Beek (links op de foto) en Evert Lammerts kunnen geen garanties geven, maar kansen zien zij in ieder geval wel. Ceo Lammerts: "We denken dat een hoop organisaties (en mogelijk ook een groeiend aantal individuen, met nieuws over zaken als PRISM en DigiD) hun data nu nog niet opslaan en delen in de cloud vanwege een begrijpelijk gebrek aan vertrouwen in de veiligheid van diensten als Dropbox, iCloud en Drive. Maar daardoor lopen deze bedrijven wel de voordelen van de cloud mis – geen noodzaak voor kapitaal intensieve investeringen in eigen

infrastructuur meer, toegenomen flexibiliteit, betere bruikbaarheid en toegankelijkheid, et cetera. Die patstelling te doorbreken, dat is toch wel een veelbelovende business case, zou ik zeggen."

Wat is Luciphers concept?

Intrinsiek veilig opslaan en delen in de cloud mogelijk te maken, door documenten te versleutelen nog voordat deze de cloud in worden gestuurd. De versleuteling vindt plaats met een stukje lokale software dat behalve versleuteling en ontsleuteling ook zorgt voor presentatie van de achterliggende cloudopslag als een ogenschijnlijk lokale drive. Voor de encryptie gebruikt Lucipher het AES256-algoritme. Het 'brute force' kraken van een daarmee versleuteld bestand zou voor de grootste supercomputer ter wereld, langer duren dan de verwachte levensduur van ons zonnestelsel. De encryptie is steeds real-time en end-to-end, zodat de onversleutelde informatie alleen als er daadwerkelijk mee

wordt gewerkt – tijdelijk – in het lokale geheugen van de eigen computer aanwezig is. Zodra wordt opgeslagen, wordt nog voor de feitelijk schrijfactie plaatsvindt, automatisch opnieuw versleuteld. Het Lucipher-systeem zal elk opgeslagen bestand met een eigen unieke sleutel symmetrisch versleutelen. Dat houdt in dat het betreffende bestand alleen met die specifieke code weer kan worden gereconstrueerd. De beheerder van de clouddienst kent de sleutel niet (een zogeheten zero-knowledge omgeving). Om toch 'sharing' mogelijk te maken kunnen de symmetrische sleutels via een PKI (Public Key Infrastructure) worden gedeeld.

Dat real-time versleutelen en ontsleutelen, neemt dat niet veel tijd en processorvermogen in beslag?

"Dat zou je denken, maar in de praktijk valt dat enorm mee, vooral als gebruik wordt gemaakt van de nieuwste processors, waarin Intel en AMD het AES256-algoritme standaard meebakken", stelt Van Beek.

Lucipher is dus eigenlijk een Dropbox-kloon met encryptie?

Wat Lucipher met Dropbox gemeen heeft, is dat het een cloudinfrastructuur is, en in die zin dezelfde behoeften van gebruikers adresseert. Het belangrijkste verschil is de versleuteling. Maar Lucipher is wel meer dan een versleutelde Dropbox, zoals BoxCryptor of CloudFogger:

- Lucipher laat geen mappen of bestanden achter op de eigen computer of laptop, die vaak onbewaakt op het bureau staat of van hot naar her wordt gesleept. Met Lucipher is er alleen de virtuele server met de versleutelde bestanden.
- Lucipher zal naast de inderdaad wel met Dropbox of SkyDrive vergelijkbare publieke cloud ook leverbaar zijn als 'gehoste private cloud' en als zelf op te zetten 'cloud-onder-eigen-dak'. Dat kan voor bedrijven het verschil maken tussen wel en geen compliancy.
- Doordat data niet lokaal worden opgeslagen, is er geen synchronisatie nodig. Dat betekent dat het ook kan worden ingezet voor big data: je kunt grote datasets openen en verschillende secties lezen (random access) zonder de volledige set te moeten down- en uploaden.

Wat wordt het verdienmodel van Lucipher?

De basisversie voor individuele gebruikers wordt gratis. Inkomsten wil het bedrijf halen uit het op basis van Lucipher-technologie beschikbaar maken van versleutelde dataopslagcapaciteit, het in licentie geven van de software aan bedrijven die, ten behoeve van eigen business units, zelf private clouds willen inrichten en het in licentie geven van de software aan providers die hun klanten veilige opslagcapaciteit in de cloud willen bieden.

Wat is er op dit moment te zeggen over de pricing van Lucipher?

Weinig. Het bedrijf houdt nog even open of licenties zullen gelden per gebruiker, per datavolume of toch nog iets anders. Wel weet Lammerts dat hij de prijsstelling 'een stuk simpeler' wil maken dan Amazon doet. "Dat is veel te complex."

Wanneer komt Lucipher beschikbaar?

De planning op dit moment is dit najaar werkende prototypes beschikbaar hebben voor Windows en Mac. Begin 2014 moet Lucifer in gebruik zijn bij een aantal launching customers. Versies voor Linux, iOS en Android moeten dan snel volgen. Dat 'snel' is voor Lucipher meer dan alleen maar een kwestie van ongeduld. Lammerts: "Het is niet te verwachten dat wij de enigen zijn die deze mogelijkheid zien. Vorige maand ging er 1,5 miljoen euro risicogeld naar Tresorit, een Hongaars bedrijf dat nu al een versleutelde cloudoplossing in de markt zet. Lucipher zet in op een technisch wat geavanceerder oplossing, maar dat mag natuurlijk niet erg veel langer duren, want de IT-geschiedenis wijst uit dat goede oplossingen die als eerste op de markt komen, vaak succesvoller zijn dan betere oplossingen die naderhand op de markt komen."

Lucipher lijkt daarmee nogal een 'hoog rendement/hoog risico'-onderneming. Wat als straks blijkt dat je gewoon te laat bent; als Google Drive of Dropbox hun tekortkomingen al hebben onderzocht en Spideroak bij iedereen op 'top of mind' is als van meet af aan versleutelde cloud. Is dan alles voor niets geweest?

Lammerts: "De markt rondom cloud-gebaseerde data diensten heeft een enorm potentieel. Veilige opslag en veilig delen van data is nu hét issue. Maar het is ook pas het begin. Integratie met processing-frameworks zoals Hadoop, Spark, Storm en vergelijkbare systemen zou wel eens de volgende stap kunnen worden. Het zou enorm jammer zijn als we met Lucipher straks niet de 'top of mind' zitten, maar er liggen nog genoeg andere kansen. Dus nee, het is nooit voor niets geweest."

Hoe zit het met Luciphers financiële slagkracht?

"Pieter en ik besteden wekelijks elk 12 uur aan advieswerk op het gebied van databeveiliging. Dat levert net genoeg inkomsten om onze kosten te dekken gedurende deze fase, waarbij de nadruk nog sterk op de technische ontwikkeling ligt. We zitten dan ook nog te springen om een programmeur, die we zo nu en dan ook kunnen inzetten op onze externe opdrachten. Inmiddels zijn we ook op zoek naar een vijfde man, die zich primair met de marketing zal bezighouden. Die heeft natuurlijk ook een budget nodig; daarom praten we nu met potentiële investeerders over seed capital. Waarschijnlijk wordt dat zo'n half miljoen. Dan kunnen we begin volgend jaar een A-ronde doen, waarbij het dan uiteraard om een aanmerkelijk groter bedrag moet gaan."

Hoe ziet Luciphers ecosysteem er moment uit?

"We hebben – onder meer door ons advieswerk – contacten met een handvol instellingen die veel belang hechten aan beveiliging door versleuteling. Onder meer in de medische onderzoeksweld, maar ook in een paar andere organisatie die met grote hoeveelheden gevoelige en persoonsgebonden informatie werken. Verder zijn we doorlopend aan het netwerken. Zo zijn we nu op zoek naar partijen die mee willen doen aan onze alpha-tests, we hopen daaraan op termijn ook launching customers over te houden. Verder zijn we in gesprek met een grote hosting provider, die we mogelijk inschakelen om onze publieke cloud hardwarematig te hosten. Deze provider heeft aangegeven ook geïnteresseerd te zijn in de mogelijkheid om onze oplossing als reseller aan zijn klanten door te leveren. Tenslotte willen we zo snel mogelijk onze Lucipher smartphone-apps voor iOS en Android beschikbaar te hebben. Die zullen waarschijnlijk vooral worden gebruikt door niet-betalende particulieren, maar leveren wel uitstraling en naamsbekendheid op."

Wat was tot dusverre de belangrijkste praktijkles voor de mensen achter Lucipher?

"In de wereld van internet start-ups ritselt het van urban legends; succesverhalen over pitchdecks, durfkapitaal en extreme groei, overgewaaid uit Silicon Valley. Die verhalen, die je nooit uit eerste hand te horen krijgt, hebben ons wel even in verwarring gebracht; moeten we nou echt de toch al beperkte tijd die we hebben ook nog bezig zijn met het maken en perfectioneren van pitchdecks en zoeken naar durfkapitaal? Of moeten we gewoon hard werken aan onze kern en vooral tijd besteden aan product- en dienstontwikkeling, iets wat in onze oren eigenlijk veel logischer klonk? In ons geval blijkt dat laatste gewoon te kloppen. Uit de contacten met investeerders bleek wel dat daar echt niemand klaar staat om een bootstrap-fase te financieren, hoe goed je pitchdeck ook is. Het risico is simpelweg te groot. Een start-up is dus precies wat je met gezond verstand kunt verwachten: veel en hard werken en zelf het risico dragen."

Is er een bepaald bedrijf of een bepaalde ondernemer die Lucipher tot inspiratie strekt?

Evert Lammerts: "Nee, niet heel sterk althans. Maar er zijn genoeg voorbeelden. VPRO's Tegenlicht had begin dit jaar een reportage over Ricardo Semler, die stelt dat regels en druk van bovenaf creativiteit in de weg staan. Zijn werknemers kiezen hun eigen werktijden, baas en salaris. Zijn manier van bedrijfsvoering, waarbij werknemers intensief worden betrokken bij de inrichting van bedrijfsprocessen, lijkt mij sympathiek en vanuit het perspectief van mijn beperkte ervaring als technicus in verschillende organisaties is het iets dat ik zelf als werknemer enorm zou waarderen. Verder vind ik ook dat Google, voor zover ik het kan beoordelen tenminste, een sympathieke manier van werken heeft ontwikkeld. Het is bij Google beleid om zo open als mogelijk te zijn over onderzoek dat daar gedaan wordt, en dat heeft de laatste paar jaar een heel belangrijke rol gespeeld in de ontwikkeling van schaalbare systemen. Googles papers over MapReduce, GFS, Bigtable, Pregel, Dremel, Dryad, Fi, Spanner en andere papers staan aan de wieg van de open source big data beweging. NoSQL, NewSQL, Hadoop, systemen voor graph processing, methoden voor geografisch gedistribueren van databases; er zijn heel zinnige zaken te herleiden naar papers van Google. Verhalen over nieuwe en open manieren van bedrijfsvoering zijn voor mij een enorme bron van inspiratie."

Wanneer is Lucifer een succes?

Lammerts: "Als we eind 2014 zo ver zijn dat we klanten krijgen op grond van onze reputatie, dus zonder er zelf nog op te hoeven jagen."