# I/O VIVAT

JAARGANG 30
NUMMER 3

## Verbod op encryptie?
Een verbod op veiligheid!

## Alan Turing
De vader van de informatica

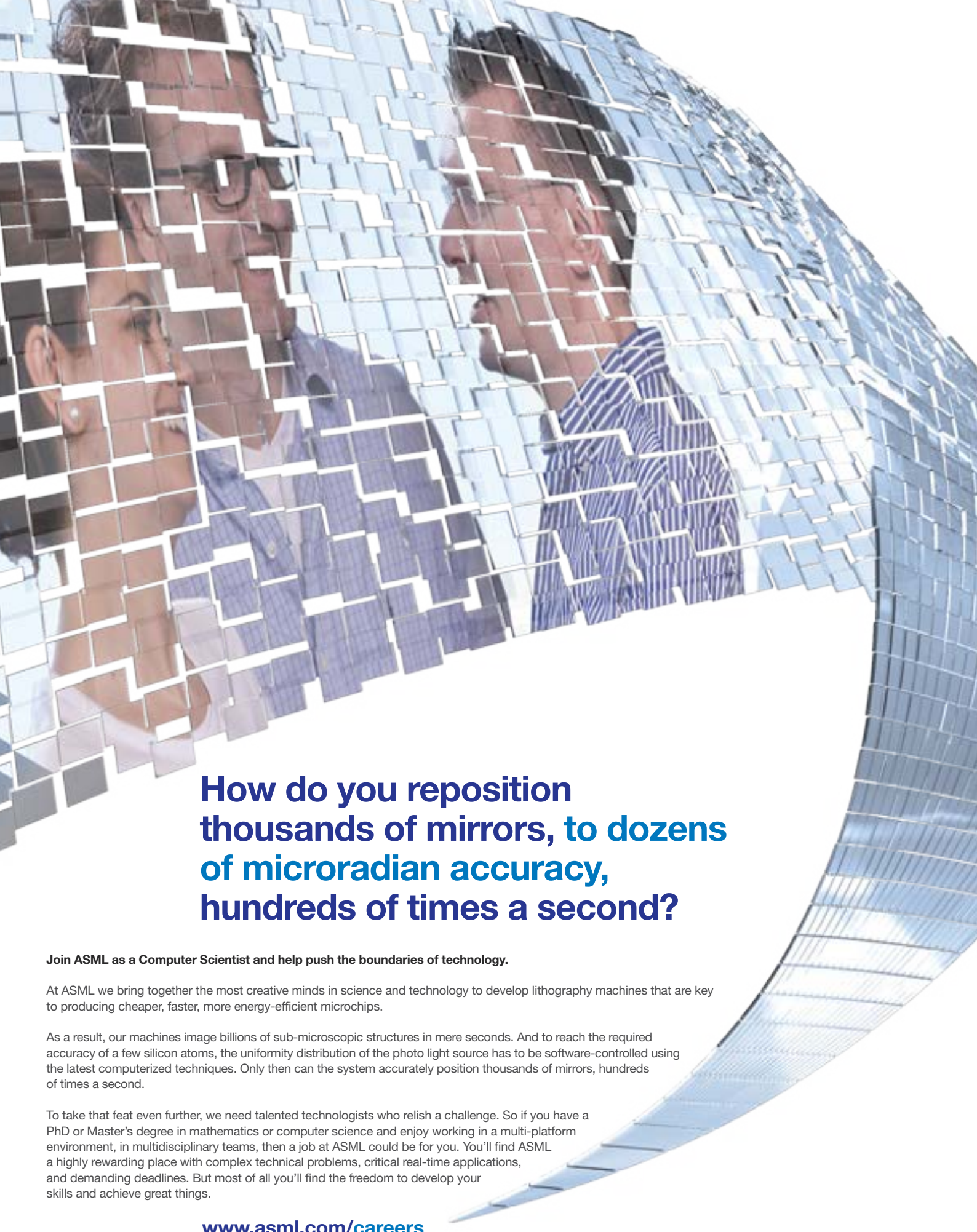
## Security Analytics
Toenemend inzicht in de staat van informatiebeveiliging

## Van Enigma tot RSA
Hoe zit dat nou eigenlijk met cryptografie?

## Identity & Access management
Aan de slag met de technieken van de toekomst!

## En verder...
Samen elke dag een beetje beter onderwijs
De kleine lettertjes van de cloud
Geert Heijenk stelt zich voor
De identiteit van Inter-Actief

Inter-Actief



# How do you reposition thousands of mirrors, to dozens of microradian accuracy, hundreds of times a second?

**Join ASML as a Computer Scientist and help push the boundaries of technology.**

At ASML we bring together the most creative minds in science and technology to develop lithography machines that are key to producing cheaper, faster, more energy-efficient microchips.

As a result, our machines image billions of sub-microscopic structures in mere seconds. And to reach the required accuracy of a few silicon atoms, the uniformity distribution of the photo light source has to be software-controlled using the latest computerized techniques. Only then can the system accurately position thousands of mirrors, hundreds of times a second.

To take that feat even further, we need talented technologists who relish a challenge. So if you have a PhD or Master's degree in mathematics or computer science and enjoy working in a multi-platform environment, in multidisciplinary teams, then a job at ASML could be for you. You'll find ASML a highly rewarding place with complex technical problems, critical real-time applications, and demanding deadlines. But most of all you'll find the freedom to develop your skills and achieve great things.

**www.asml.com/careers**

ASML

/ASML @ASMLcompany

**For students who think ahead**

## //Colofon

Jaargang 30, nummer 3,
april 2015
ISSN: 1389-0468

I/O Vivat is het populair-wetenschappelijke tijdschrift van I.C.T.S.V. Inter-*Actief*, de studievereniging voor Technische Informatica, Bedrijfsinformatie-technologie en Telematica van de Universiteit Twente. I/O Vivat verschijnt vier maal per jaar en heeft een oplage van 1800 exemplaren.

// Hoofdredactie
Kyra de Lange

// Redactie
Michel Brinkhuis, Kyra de Lange Florian Mansvelder, Meike, Nauta, Herman Slatman, Stijn van Winsen,

// Vormgeving
Arnold Averink, Kyra de Lange, Matthias van de Meent, Regie Mocking, Mart Oude Weernink, Remco Tjeerdsma

// Gastschrijvers
Geert Heijenk, Rien Heuver, Luís Ferreira Pires, Klaas Sikkel

Voor vragen, suggesties en tips is I/O Vivat bereikbaar via e-mail op vivat@inter-actief.net, twitter op @iovivat, telefonisch op 053-489 3756 of per post:
Studievereniging Inter-*Actief*
Postbus 217
7500AE Enschede

De studievereniging wil de adverterende bedrijven bedanken voor de samenwerking.

// Drukwerk
Drukkerij van den Bosch & Fikkert



I/O VIVAT

# //Redactioneel

Voor je ligt alweer de derde I/O Vivat van dit collegejaar en tevens de eerste I/O Vivat waar ik de hoofdredacteur van ben. Als thema hebben we ditmaal voor encryptie gekozen: niet alleen de technische kant komt aan bod, maar ook een sleutelfiguur binnen crypto-analyse en zelfs de informatica: Alan Turing.

Florian zet voor jullie enkele standaarden voor encryptie op een rijtje, voor een goed overzicht van de ontwikkelingen daaromtrent. Ook schrijft hij over een omstreden wetsvoorstel in het Verenigd Koninkrijk, wat inhoudt dat burgers hun communicatie niet mogen versleutelen. Daarnaast schrijft Herman een artikel over security analytics: methoden die bedrijven kunnen helpen bij het beter beveiligen van hun data. Michel laat identity en access management aan bod komen; welke rol spelen werknemers in beveiligingsproblemen?

Daarnaast kunnen jullie kennismaken met Geert Heijenk, die onlangs opleidingsdirecteur van Technische Informatica is geworden. Klaas Sikkel, de winnaar van de decentrale onderwijsprijs, vertelt over zijn visie op het verbeteren van het onderwijs. Uiteraard mag de column van onze voorzitter ook niet ontbreken.

Veel leesplezier bij deze I/O Vivat,

Kyra de Lange
Hoofdredacteur I/O Vivat

# //Inhoud 30.3


# Nieuws //

## Google wijzigt zoekalgoritme op mobiele apparaten

Om developers aan te moedigen met mobiele versies van hun websites te komen, heeft Google op 21 april zijn zoekalgoritme voor mobiele apparaten aangepast. Mobiel-vriendelijkheid van websites wordt nu meegenomen als 'zoekcriterium', waardoor websites met een mobiele versie hoger gerankt worden in de resultaten dan websites die dat niet geschikt zijn gemaakt voor mobiele apparaten. Google geeft zelf aan dat dit een significante invloed zal hebben op de zoekresultaten op mobiele apparaten. De wijziging geldt alleen voor mobiele telefoons, niet voor tablets en uiteraard niet voor normale pc's

Google kondigde de wijziging in februari al aan, om developers de tijd te gunnen hun websites te verbeteren. Ook zijn er hulpmiddelen beschikbaar gesteld om websites geschikt te maken voor mobiele apparaten, door een handleiding voor mobiele sites en zelfs een test-tool beschikbaar te stellen.

Volgens de BBC halen bijvoorbeeld (delen van) de sites van Wikipedia, de EU en BBC zelf deze mobile-friendlytest niet. Lang niet alle grote en veelbezochte websites zijn dus mobielvriendelijk. Door de maatregel hoopt Google het gemakkelijker te maken voor gebruikers om op hun mobiele telefoon toch op een gebruiksvriendelijke manier informatie te kunnen vinden, en daarmee de user experience te verhogen.

Bron: http://googlewebmastercentral.blogspot.co.nz/2015/02/finding-more-mobile-friendly-search.html

http://www.computerworld.com/article/2912237/is-your-site-ready-for-googles-mobilegeddon-on-tuesday.html

## Amerikaanse overheid maakt zich zorgen over het gevaar van encryptie

De Amerikaanse minister van Binnenlandse Veiligheid heeft in een toespraak aangegeven dat encryptie een lastig punt is voor de Amerikaanse overheid. Aan de ene kant zien ze het belang in van encryptie wat betreft de privacy, aan de andere kant zien ze ook de uitdagingen die dit oplevert op het gebied van antiterrorisme en handhaving van de wet.

'Stel dat we, terwijl de telefoons al lang en breed in gebruik zijn, als overheid enkel toegang zouden mogen krijgen tot de normale post.' stelt de minister.

Het feit dat de overheid geen toegang heeft tot bepaalde informatie leidt tot problemen betreffende de volksveiligheid. Het wordt voor de overheid moeilijker om criminaliteit en terrorisme op te sporen en tijdig in te grijpen, met alle gevolgen van dien.

Een oplossing hiervoor is moeilijk, omdat er een compromis moet worden gevonden tussen het recht op privacy van het Amerikaanse volk, maar ook het belang van nationale veiligheid. "De overheid kan niet meer barrieres opwerpen, meer personen ondervragen en iedereen elkaar laten verdenken en daarmee de veiligheid verhogen, zonder dat de vrijheid van de Amerikanen hiermee wordt beperkt. Uiteindelijk is het het belangrijkst dat wij ons als volk niet laten terroriseren."

https://www.dhs.gov/news/2015/04/21/remarks-secretary-homeland-security-jeh-johnson-rsa-conference-2015

# Verbod op encryptie?

## Een verbod op veiligheid!

*Door: Florian Mansvelder*
*Redacteur I/O Vivat*

**Het niet mogen versleutelen van persoonlijke data is voor de inwoners onder andere Rusland, Vietnam, Iran en China de normaalste zaak van de wereld. Recentelijk heeft David Cameron - de premier van het Verenigd Koninkrijk, die een 'digital Britain' voor ogen had - aangegeven een soortgelijk verbod te willen instellen.**

Op maandag 12 januari 2015 gaf David Cameron aan bij een persconferentie dat hij een staatsbeleid wilde instellen waarmee hij een groot deel van de Engelse economie om zeep zou kunnen helpen. Het staatsbeleid gaat om end-to-end encryptie, met het doel dit in zijn geheel te verbieden. David Cameron gelooft dat dit nodig is om de laatste 'safe spaces' voor terroristen te dichten. Wat David Cameron niet meldt is dat dit betekent dat dit verbod zal worden gebruikt om burgers te observeren. Dit betekent dat wederom privacy de dupe zal zijn van veiligheid. Tevens zou dit verbod betekenen dat services als SnapChat en WhatsApp landelijk verboden zullen zijn, omdat deze apps ook end-to-end encryptie toepassen. Maar niet alleen veilige communicatie, ook generieke online veiligheid, internetbankieren, transacties en veel meer zou niet meer betrouwbaar zijn, of in zijn geheel niet meer mogelijk zijn door een verbod als deze.

### Illegale doeleinden

De grootste reden voor het verbod op end-to-end encryptie is volgens David Cameron het feit dat terroristen hiervan gebruik maken om onzichtbaar te handelen en communiceren. Hiermee doelt de premier waarschijnlijk op apps zoals SnapChat en WhatsApp. Deze apps laten mensen ongestoord communiceren over lange afstand, door middel van encryptie. Maar het feit dat terroristen dit gebruiken zien als reden om het te verbieden, is eigenlijk als het verbieden van het openbaar vervoer omdat een mogelijke terrorist dit kan gebruiken om van A naar B te komen. Het is waar dat de regering van een land zoveel mogelijk moet doen om de inwoners te beschermen tegen terreur, maar de regering moet niet vergeten dat ze de inwoners ook moeten beschermen tegen de regering zelf. In het voorjaar van 2013 heeft Minister Opstelten van Veiligheid en Justitie een voorstel gedaan voor een zogeheten decryptieplicht. Dit betrof mensen die verdacht werden van het bezit van kinderporno. Volgens deze regeling zouden deze verdachten verplicht kunnen worden om hun data te ontsleutelen voor de regering. Het probleem met het voorstel was dat het volgens Raad voor de Rechtspraak haaks staat op het beginsel dat niemand aan zijn eigen veroordeling hoeft mee te werken, volgens artikel 6 van het EVRM (het Europees Verdrag voor de Rechten van de Mens). Wanneer het verplichten om onzichtbare dingen zichtbaar te maken

Figuur 1: David Cameron, premier van Verenigd Koninkrijk

in strijd is met mensenrechten , is het dan niet ook in strijd is met mensenrechten om mensen te verbieden überhaupt dingen onzichtbaar te maken?

### Effectiviteit

Stel een decryptieplicht zou worden ingevoerd, dan rest tevens de vraag of dit effectief is. Het feit blijft dat een verdachte zich kan beroepen op het beginsel dat stelt dat een verdachte niet hoeft mee te werken. Ook los hiervan kan men eraan twijfelen of decryptieplicht effectief is. Wanneer iemand wordt verplicht zijn of haar data te ontsleutelen, en deze persoon wist van tevoren dat dit gevraagd kon worden. De persoon in kwestie zou van tevoren zowel zijn/haar verdachte data als een groot aantal mooie landschapsfoto's samen kunnen hebben versleuteld. Het ene wachtwoord geeft dan de verdachte data vrij, het andere de landschapsfoto's. Met het alternatieve wachtwoord vindt de politie nu juist bewijs dat de versleutelde data uit enkel landschapfoto's bestaat, en kan niet per se aantonen dat het mogelijk meer bevat. Het kan tevens zorgen voor onterechte beschuldigingen. Stel een persoon heeft tien jaar geleden een groot aantal bestanden versleuteld, en heeft er nooit meer iets mee gedaan, en deze persoon is dit wachtwoord inmiddels allang vergeten?

Als deze persoon vervolgens zou worden verplicht de data te ontsleutelen, maar hij of zij weet het wachtwoord simpelweg écht niet meer, wordt er dan vanuit gegaan dat het inderdaad om bestanden ging die je schuld zouden bewijzen, wat vervolgens reden tot vervolging kan zijn?

> "Mensen zullen zich onveilig voelen bij het gebruik van internet.."

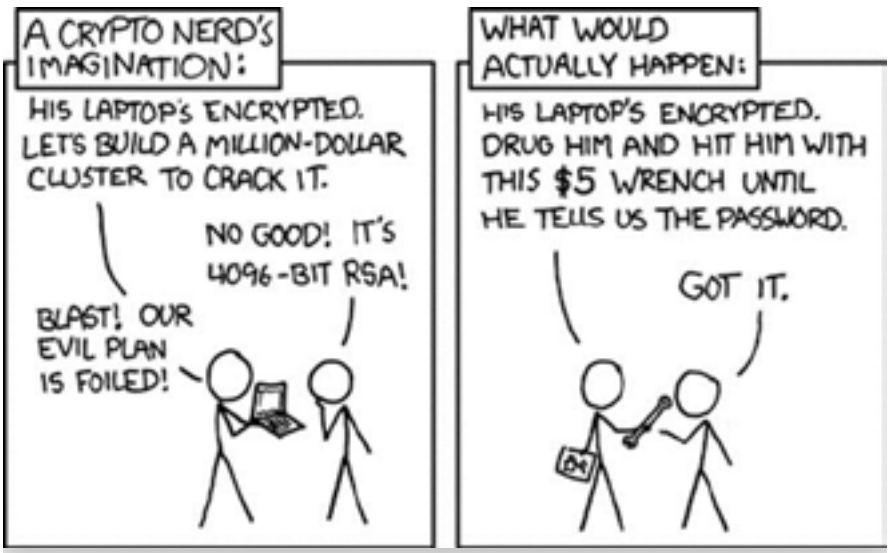
### Digitale privacy verdwijnt

Een verbod op end-to-end encryptie zou als gevolg hebben dat privacy achteruit gaat en de levensvrijheid van burgers wordt beïnvloed. De regeringen van Rusland en China hebben een reputatie met het onderdrukken van diens burgers, waarbij het verbod op encryptie één van de manieren is waarop zij dit uitoefenen. David Cameron beloofde een 'digital Britain'. Nu stelt hij voor in de voetsporen van Rusland en China te stappen door diens regelingen na te volgen. Maar zonder encryptie is er geen WhatsApp en geen veilige e-mail. Jong en oud zal minder gebruik maken van digitale middelen om te communiceren. Mensen zullen zich onveilig voelen met het gebruik van internet, want alles wat men zegt kan woordelijk nagelezen worden. Tegenwoordig sturen mensen steeds vaker berichten en foto's naar elkaar die enkel voor elkaar bedoeld zijn.

Zonder encryptie kan een bedrijf, een buurman of een willekeurige computernerd met vrijwel geen ervaring deze berichten en foto's achterhalen. Deze moeite zou niet eens vallen onder de definitie van hacken.

### Economische aanslag

Wanneer encryptie verboden wordt, zou ook de economie hard achteruit gaan. Internetbankieren en online winkelen zouden niet meer betrouwbaar zijn. Alles wat je stuurt over het internet is af te vangen en elke verbinding is ineens extreem kwetsbaar voor verscheidene cyberaanvallen. Op deze manier zijn services als internetbankieren of andere online geldzaken simpelweg niet meer mogelijk. David Cameron crëeert op deze manier juist een 'analogue Britain'. Communicatie van bedrijven over gevoelige informatie wordt vaak beveiligd door het gebruik van services als een VPN, een zogeheten virtual private network. Dit is een netwerk waar enkel geautoriseerde mensen toegang tot hebben, door middel van encryptie. Dit soort netwerken zijn zonder encryptie niet meer mogelijk, dus moeten bedrijven ineens weer verouderde en inefficiënte middelen gebruiken om te communiceren. Alle persoonlijke informatie zou publiek worden en cybercriminaliteit zou hoger liggen dan ooit. The gedigitaliseerde beschaving van nu zou binnen korte tijd niet meer bestaan.




Figuur 2: Encryptie in de praktijk

## Productbeveilingen

Grote bedrijven als Apple en Google hebben recent veel kritiek gehad op privacyregelingen, omdat Apple en Google niet zouden garanderen dat zij hun producten niet monitoren. Apple heeft hierom de iPhone zo beveiligd dat Apple de middelen niet heeft om de telefoon te ontsleutelen. Zelfs met een bevelschrift. Stel encryptie zou verboden worden, dan wordt bijvoorbeeld ook deze beveiliging van een product niet langer toegestaan. Cameron wil dat er zogeheten 'backdoors' worden gemaakt voor dit soort producten, waarlangs bevoegde personen toch het product kunnen ontsleutelen. Dit zou betekenen dat Apple de iPhone encryptie wederom zou moeten aanpassen om de telefoon in het Verenigd Koninkrijk te kunnen verkopen zonder de wet te overtreden. Er bestaat de kans dat grote bedrijven als Apple die voor dit soort dilemma's komen te staan besluiten om het land simpelweg over te slaan. Het kost mogelijk minder geld om niet te verkopen in het Verenigd Koninkrijk, dan om het product dusdanig aan te passen.

## Encryptie, encryptie, encryptie

Zoals Travis Carelock, de technisch directeur van Black Hat - een organisatie die al jaren conferenties en trainingen over informatie-beveiliging geeft - zei: "the three most important words to remember in regard to protecting data are encryption, encryption and encryption." Het verbieden van encryptie elimineert misschien de mogelijkheid voor terroristen om veilig over lange afstand te communiceren, en maakt het beter mogelijk terroristen te identificeren. Het elimineert echter ook de mogelijkheid voor gewone mensen om veilig over lange afstand te communiceren, en maakt het schrikbarend makkelijk alles over deze mensen te weten te komen. Het is mogelijk een inbraak op mensenrechten om te verbieden dat dingen worden achtergehouden, terwijl dit mogelijk niet eens effectief te handhaven is. Apps als WhatsApp en SnapChat kunnen niet meer gebruikt worden, en zelfs e-mail is niet meer betrouwbaar. De economie gaat drastisch achteruit doordat transacties onveilig worden en alle persoonlijke gegevens in een handomdraai kunnen worden uitgelezen. Bedrijven zullen niet meer veilig zaken kunnen doen en internationale bedrijven zouden kunnen besluiten een land geheel buiten te sluiten. Een encryptieverbod klinkt op het eerste gezicht misschien als een mooie oplossing tegen terreur, maar het doet misschien meer schade dan de terreur die het voorkomt ooit zou kunnen aanrichten.

> "Dit maakt het erg makkelijk alles over mensen te weten te komen.."


Figuur 3: Encryptie en privacy

## Bronnen


*http://webwereld.nl/beveiliging/78553-rechters-decryptieplicht-in-strijd-met-mensenrecht*

*https://rejo.zenger.nl/vizier/wetsvoorstel-decryptieplicht-voorbereiding/*

*http://tweakers.net/nieuws/88842/opstelten-houdt-vast-aan-omstreden-hackbevoegdheden-politie.html*

*https://www.bof.nl/2012/11/28/decryptiebevel-werkt-niet-en-maakt-nederland-onveiliger/*

*http://vidar-security.nl/index.php/blog/entry/blijf-af-mijn-privacy-blijf-af-van-encryptie*

*http://uk.businessinsider.com/britains-proposed-encryption-ban-is-totally-unworkable-2015-1?r=US*

*http://www.theguardian.com/technology/2015/jan/16/david-cameron-encryption-lavabit-ladar-levison*

*http://www.bbc.com/news/technology-30794953*

*http://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror*

*http://www.automatiseringgids.nl/nieuws/2013/29/raad-voor-rechtspraak-veegt-vloer-aan-met-opstelten*

*Header: http://media.nu.nl/m/m1mx6aoaqf31_wd1280.jpg/sint-maarten-schrapt-levenslange-straffen-wetboek.jpg*

*Figuur 1: http://www.lgl.lt/en/files/Cameron.jpg*

*Figuur 2: http://imgs.xkcd.com/comics/security.png*

*Figuur 3: http://www.ciphercloud.com/wp-content/uploads/2014/02/Cloud_Encryption_HIPAA_Compliance_1280.jpg*

# Historisch persoon: Alan Turing

## De vader van de informatica

*Door: Kyra de Lange*
*Redacteur I/O Vivat*

**Op 7 juni 1954 stierf op 41-jarige leeftijd een man die de wereld misschien wel veel verder had kunnen brengen dan hij al had gedaan: Alan Turing. Tegenwoordig staat hij ook wel bekend als 'de vader van de informatica' en als naamgever van de zogeheten Turingmachine, Turingtest en de Turingaward. Toentertijd was hij eerder berucht dan bekend: twee jaar voor zijn dood werd hij gearresteerd wegens homoseksualiteit en over zijn dood verschillen de meningen: was het een ongeluk, zelfmoord of is hij vanwege een veiligheidsrisico door de Britse geheime dienst vermoord?**

### Jonge jaren

Alan Turing volgde zijn onderwijs aan een Engelse kostschool en later aan de universiteit van Cambridge, waar hij zich in eerste instantie verdiepte in de wiskunde. Hij boog zich hier onder andere over de vraag of er een methode bestaat om te bepalen of iets berekenbaar is. Hij schreef hier een artikel over op 24-jarige leeftijd, waarin hij ook zijn Turing-machine introduceerde.

Een Turingmachine is een gedachte-experiment waarin een algoritme wordt voorgesteld als een machine die op een bepaalde manier tekens op een oneindige band manipuleert. De machine bestaat uit een oneindige band, die dataopslag simuleert, gecombineerd met een 'uitvoerder' (een apparaat, in Turings oorspronkelijke idee een mens) die tekens op de band leest en schrijft. Deze uitvoerder schrijft tekens op de band en verplaatst zich over de band aan de hand van een set van instructies, die gegeven de toestand van het apparaat en het afgelezen karakter vertelt welke acties de 'uitvoerder' moet verrichten.

Het praktisch nut van deze machine is het volgende: als er heel veel Turingmachines zijn die elk één algoritme kunnen uitvoeren, is er dan een Turingmachine die al deze Turingmachines kan uitvoeren? Deze zogenoemde 'Universele Turingmachine' heeft veel weg van onze huidige computers, die in essentie niets anders doen dan zaken berekenen. Het duurde nog een flink aantal jaar voor de eerste computer daadwerkelijk gebouwd werd, maar het oorspronkelijke idee zat al eerder in Turings hoofd.

Figuur 1: Alan Turing

### Turings werk in de oorlog

Turings wiskundige vaardigheden waren hard nodig in de oorlog en na een korte periode aan de Princeton University keerde hij dan ook weer terug naar Engeland. Daar ging hij aan de slag bij de crypto-analytische afdeling van de Britse overheid. Nadat de oorlogsverklaring daadwerkelijk een feit was, ging hij fulltime werken in Bletchley Park, waar hij met wiskundigen en andere wetenschappers werkte aan het ontcijferen van de Enigma, het encryptiesysteem van de Duitse strijdkrachten. De Duitse Enigma versleutelde berichten door letters te veranderen volgens een combinatie van rotorwielen en daarbovenop het uitwisselen van letters. Dit leverde, afhankelijk van de tijd in de oorlog en de afdeling van de strijdkrachten (de marine gebruikte een Enigma met meer wielen) een aantal mogelijke instellingen tussen de $1{,}0*10^{11}$ en $1{,}8*10^{20}$. De instellingen werden elke dag veranderd en het spreekt uiteraard voor zich dat er teveel instellingen waren om met de hand door te kijken, voordat de dag voorbij was en al het werk voor niets was.

De mede door Turing ontwikkelde Bombe, een verbeterde versie van de Poolse Bomba, automatiseerde het aflopen van deze instellingen gedeeltelijk.

Een flink aantal instellingen is namelijk in de praktijk niet mogelijk; de Bombe controleerde dit door een (van het soort Enigma afhankelijk) aantal rotors te laten draaien en zo combinaties van rotorstanden te proberen; bij standen die mogelijk waren ging er een elektrische stroom lopen, waardoor alle draaiende rotoren tot stilstand kwamen. Een persoon nam deze instellingen dan over en startte het apparaat opnieuw, op zoek naar de volgende instelling. De op deze manier als praktisch mogelijk bepaalde instellingen werden dan aan verder onderzoek onderworpen, waarbij er steeds meer weggestreept werden en uiteindelijk de juiste instellingen van de Enigma van die dag gevonden. Er wordt vermoed dat de ontcijfering van de Duitse communicatie de oorlog met enkele jaren verkort heeft en zo duizenden levens gespaard zijn.

Turing stond op zijn werkplek bekend als een excentrieke man, met soms wat rare karaktertrekken en gewoontes. Zo droeg hij in de lente een gasmasker tegen zijn hooikoorts, en in plaats van dat hij zijn kapotte fiets liet repareren, telde hij het aantal omwentelingen om periodiek de ketting strakker te zetten. Ook vroeg hij een collega ten huwelijk, Joan Clarke, maar hij verbrak de verloving later vanwege zijn homoseksualiteit.

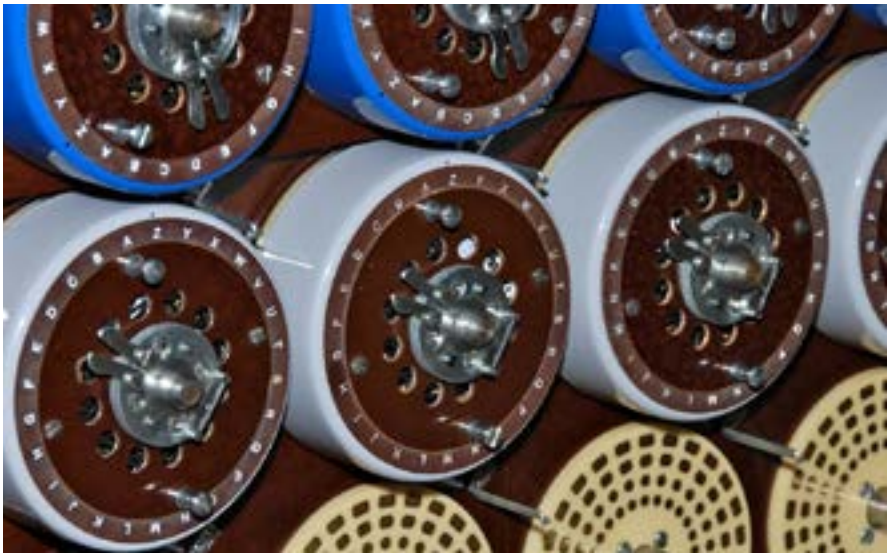
## Na de oorlog

Al het werk wat Turing in de oorlog verricht had, was voor hem verder niet bruikbaar omdat er vanwege veiligheidsredenen niet over gepraat mocht worden. Hij sloot zich aan bij een onderzoeksgroep in Manchester, die zich bezighield met rekenmachines en computers. Turing zelf verdiepte zich in het programmeren van computers en was betrokken bij de ontwikkeling van de eerste schaakprogramma's. In het verlengde hiervan stelde hij een experiment voor: de zogeheten Turing-test, waarin een menselijke jury door middel van conversatie met zowel een mens als een computerprogramma moet bepalen welke van de twee een computerprogramma is: de basis onder de kunstmatige intelligentie. Een computer slaagt voor de test als zij een bepaald percentage van de jury kan overtuigen van haar menselijkheid. Deze Turingtest is op dit moment nog steeds actueel als maat voor de kracht van een kunstmatig intelligentieprogramma.

> "het werk aan de ontcijfering van de Enigma heeft duizenden levens gespaard"

Helaas ging het hierna bergafwaarts met Alan Turing. In 1952 werd hij veroordeeld voor zijn homoseksualiteit, nadat hij dit had toegegeven bij een aangifte van een overval bij hem thuis. Hij verkoos experimentele chemische castratie boven een gevangenisstraf. In 1954 werd hij dood gevonden, met een halfopgegeten appel naast zich en verhoogde concentraties cyanide in zijn lichaam. De officiele doodsoorzaak is zelfmoord, maar door de jaren heen hebben verscheidene mensen aangegeven dat het wellicht ook een ongeluk kan zijn geweest; Turing experimenteerde thuis met cyanide en was niet altijd even voorzichtig. De appel is nooit getest op cyanide, dus ook een vergiftiging door de Britse geheime dienst, waar hij naar zijn veroordeling vanwege veiligheidsredenen niet meer welkom was, wordt door sommigen niet uitgesloten.

Pas in de 21e eeuw, in 2009, maakte de Britse regering openbaar excuses voor de behandeling van Alan Turing. In 2013 volgde een postuum eerherstel door Queen Elizabeth II. Tegenwoordig is ook de 'nobelprijs in de informatica', de Turing Award, naar hem vernoemd. Na ruim 50 jaar krijgt hij toch nog de eer die hij verdient.



Figuur 2: Rotoren van de Bombe

## Bronnen


*http://www.bbc.co.uk/timelines/z8bgr82#zq9k87h*

*http://www.kennislink.nl/publicaties/alan-turing-oorlogsheld-wiskundegenie-en-martelaar*

*http://www.turing.org.uk/bio/*

Figuur 1
*http://lib.irb.hr/web/media/k2/items/cache/8c4a664fa4cf4c8ae026ba2b433cf60_XL.jpg*

Figuur 2
*http://www.cryptomuseum.com/crypto/bombe/img/bombe_rotors_full.jpg*

Header
*http://upload.wikimedia.org/wikipedia/commons/3/3c/Four-rotor-enigma.jpg*

//Advertorial

Keylane | Quinity
non-life insurance software

# Na een master wiskunde de IT in

## Menno Bootsveld vertelt erover!

*Door: Menno Bootsveld*
*Consultant bij Keylane|Quinity*

**Ik ben Menno Bootsveld en nu bijna twee jaar werkzaam als consultant bij Keylane|Quinity. Na mijn master Applied Mathematics aan de Universiteit Twente zocht ik naar een baan bij een bedrijf die uitdaging, doorgroeimogelijkheden en een gezellige werksfeer combineert. Dit vond ik bij Keylane|Quinity.**

Keylane|Quinity is een softwarebedrijf dat zich specialiseert in het ontwikkelen van verzekeringssoftware. Ons belangrijkste product is de Quinity Insurance Solution, kortweg QIS. Verzekeraars gebruiken QIS als standaardpakket voor hun polis- en schadeadministratie.

### Consultant

Als consultant kun je bij Keylane|Quinity in aanraking komen met meerdere rollen: functioneel ontwerper (denk aan het leiden van ontwerpsessies en uitwerken van nieuwe gewenste functionaliteiten), docent, inrichten van systemen, tester en meer. Ik ben de afgelopen voornamelijk actief geweest in de rol van systeemtester. Ervaring leert dat de meesten een nogal eenzijdig beeld hebben van de werkzaamheden van een tester. Testen is echter veel meer dan op een knopje klikken en controleren of het systeem de juiste handeling uitvoert. Als tester ben je de eindredacteur van het systeem: als je vindt dat de kwaliteit niet op peil is wordt er niet opgeleverd. Je hebt contact met ontwerpers, testers en de klant en bent dus eigenlijk de spin in het web van het softwareontwikkelproces.

### Detachering bij Reaal

Keylane|Quinity is als software leverancier Nederlands marktleider of het gebied van schadeverzekeringen. Een van onze klanten is Reaal, een grote Nederlandse verzekeraar. Vanuit Reaal kwam het verzoek binnen of wij een tester konden leveren die mee kon helpen bij het uitvoeren van de acceptatietest, de laatste test van het systeem die bij de klant wordt uitgevoerd. Aangezien ik inmiddels een klein jaartje ervaring als tester meedroeg en ik een avontuurtje wel zag zitten ben ik de uitdaging aangegaan. Gedurende negen maanden werd ik gedetacheerd en werkte ik op locatie bij de klant mee aan het verzorgen van acceptatietests. Het komt overigens niet vaak voor bij Keylane|Quinity dat consultants gedetacheerd worden. De meesten werken vanaf onze vestiging in hartje Utrecht.

Bij Reaal draaide ik mee in het testteam dat speciaal was opgezet om QIS af te testen. Dit was een leuke en leerzame ervaring omdat je als Keylane|Quinity-medewerker een kijkje in de keuken van de klant krijgt. Zo krijg je pas echt door wat er leeft bij klanten, welke wensen en ergernissen ze hebben en hoe zij ons softwarepakket gebruiken. Mijn focus lag op het testen van productinrichting die aangeleverd werd door andere consultants bij Keylane|Quinity. De productinrichting is het vertalen van een verzekeringsproduct van een klant naar dialogen en polisdefinities. Denk bijvoorbeeld aan het ontwerpen van een aanvraagdialoog van een autoverzekering. Ik had wekelijks contact met de teamleider bij Keylane|Quinity om de kwaliteit van de productinrichting door te spreken. Tijdens deze meetings was het mijn verantwoordelijkheid om de wensen van Reaal kenbaar te maken aan Keylane|Quinity. Dit was erg uitdagend werk omdat het deels mijn verantwoordelijkheid was dat Reaal de functionaliteit kreeg waar ze om gevraagd hadden, en uiteraard dat het foutloos werkt.

Inmiddels ligt mijn detacheringsperiode bij Reaal alweer achter me en heb ik het werk overgedragen aan een collega consultant. Nu zit ik op een interne testafdeling bij Keylane|Quinity en komt de volgende detacheringsklus er alweer aan: bij onze klant Ennia op Curaçao! De tropische bestemming, mooi weer en witte stranden incluis, is zeker geen vervelende bijkomstigheid.

Keylane|Quinity ontwikkelt flexibele standaard software voor kernprocessen van leven- en schadeverzekeraars. Onze oplossing omvat een complete polis- en schadeadministratie voor verzekeraars, volmachten en intermediairs. Nu we al enige tijd Nederlands marktleider zijn, hebben we onze pijlen gericht op Europa.

We zijn een informele, collegiale en platte organisatie. We hebben veel hoogopgeleide, jonge en enthousiaste medewerkers in dienst. De gemiddelde leeftijd ligt rond de 32 jaar.

Contact
Kijk voor meer informatie op www.werkenbijkeylanequinity.nl of neem contact op met Tessa van Rijnsoever of Fleur Aalbersberg via telefoonnummer 030-2335999 of stuur een e-mail naar werkenbijquinity@keylane.com. Volg ons op Twitter of Facebook en blijf op de hoogte van onze vacatures en activiteiten.

# // Puzzel



*Door: Joey Haas*
*Redacteur I/O Vivat*

"Recentelijk waren we bezig met het luisteren naar de radio, tijdens het scannen van de frequenties viel ons een opmerkelijke transmissie op. Het lijkt alsof het uit Rusland komt, want tijdens de rest van het contact werd Russich gepraat. Een informant vertelde ons dat het van de KGB komt en ze het over een datum hebben. Wij hebben geen idee wat dit is, maar onder de mensen die deze datum kunnen vinden verloten wij een bioscoopbon t.w.v. 10 euro! Hieronder zijn de opgenomen stukken te vinden. Antwoorden kunnen worden gestuurd naar iovivat@inter-actief.net met het onderwerp: 'Vivat Puzzel [DATUM]'. Veel succes!"

Kom je er helemaal niet uit? Mail dan naar bovenstaand adres voor een hint!

//Column

# Van Luís

## Speerpunten van het Onderwijsmanagement: Internationalisering en Digitalisering



*Door: Luís Ferreira Pires*
*Onderwijsdirecteur van de studie Business & IT en Business Information Technology*

**Tijdens de BIT Champagneborrel op 19 maart werd mij de volgende vraag gesteld: 'Wat doet een Opleidingsdirecteur eigenlijk?' Dat vond ik een interessante vraag. Ik ben redelijk druk met mijn werkzaamheden als OLD, maar wat 'doe' ik? Ik begon met een vrij abstract antwoord, over beleid en (inhoudelijke) aansturing. Toen ik een concreter antwoord wou geven noemde ik het herstructureren van de Master opleiding, met de nieuwe specialisatie en eenvoudigere regels als voorbeeld. Daarnaast moeten we als OLD nog andere taken doen. Variërend van snel bijspringen in het geval van crisis, tot het lange termijn plannen, met een soort 'tentamen' wanneer een visitatie plaatsvindt.**

Ik vind dat een OLD een aantal speerpunten moet hebben, en dan met name de stippen op de horizon. Zelf ben ik zeer geïnteresseerd in internationalisering en digitalisering. De BIT opleiding heeft een unieke combinatie van Bedrijfskunde en Informatica, en dit is maatschappelijk gezien bijzonder belangrijk, wat keer op keer bevestigd wordt in gesprekken met het bedrijfsleven. Hetzelfde bedrijfsleven wordt steeds internationaler, dus we moeten professionals opleiden die in staat zijn om in een internationale omgeving te opereren. Niets beters dus om deze internationale omgeving alvast tijdens de studie te creëren, vanaf de start, en daarom waren we van plan om per 2015-2016 de BIT Bachelor Engelstalig (en dus toegankelijk voor buitenlanders) te maken. Dit plan werd gefrustreerd door de politieke en bureaucratische molen van de UT, maar ik ga er vanuit dat dit met ingang van 2016-2017 wel lukt. Als OLD van een relatieve kleine opleiding hoop ik dat de BIT Bachelor daardoor ook veel buitenlanders aantrekt, met een verhoogde instroom als consequentie.

'Digitalisering' klinkt voor mij als een oplossing waarvoor we het probleem nog moeten zoeken. We zijn vorig schooljaar met TOM begonnen, en de modules zijn met veel inspanning en soms met enige haast ontwikkeld. Veel modules zijn daardoor opgesteld door bestaande vakken in elkaar te schuiven en soms zijn ze gegeven dankzij een enorme hoge inzet van studentenassistenten (relatief inefficiënt en duur, dus). Ik ben van mening dat een tweede ronde van ontwikkeling nu nodig is, waarin vooral gekeken moet worden naar de effectiviteit en de 'duurzaamheid' van de modules. En daar zie ik de rol van digitalisering. Wanneer iemand over onderwijsdigitalisering begint wordt er meestal gelijk gedacht aan het beschikbaar stellen van colleges als videoclips, alhoewel dit eigenlijk het minst kritische (en dus het minst interessante) aspect van het onderwijs is. De uitdaging zit o.a. in het aanbieden van veel oefeningen met snelle terugkoppeling, zodat de studenten 'meters kunnen maken'. Daarnaast het verbeteren van de toetsing, hopelijk ooit met vraagstukken die op laptops beantwoord kunnen worden, en die automatisch nagekeken worden (en die verder gaan dan saaie 'multiple choice' vragen). Een oplossing voor deze uitdagingen vereisen echter niet alleen een digitale omgeving, maar ook een verandering in de manier van het kijken naar onderwijsprocessen.

Mijn stip op de horizon is dat ik hier iets in kan betekenen voor het BIT onderwijs, en dat ik deze twee speerpunten volledig kan waarmaken.

Sinds 1994 is dr. Luís Ferreira Pires universitair hoofddocent aan de Universiteit Twente, momenteel bij de 'Services, Cyber-security and Safety' groep van de faculteit EWI. Luís werd op 7 april 1961 geboren in São Paulo (Brazilië), en sinds maart 1988 woont hij in Nederland. Hij heeft een ingenieursdiploma van 'Instituto Technológico de Aeronaútica' (São José dos Campos, Brazilië) en een Masterdiploma van 'Universidade de São Paulo' (São Paulo, Brazilië). In 1994 is hij bij de Universiteit Twente gepromoveerd.

Luís houdt van sporten, in het bijzonder voetbal, zoals elke typische Braziliaan. Luís is een fanatieke supporter van São Paulo FC, maar hij is ook regelmatig te vinden tussen de FC Twente supporters in de Grolsch Veste. Hij speelt tennis, de laatste tijd iets minder vanwege zijn knie. Hij is getrouwd en heeft drie kinderen: Elena (14), Melinda (12) en Caio (7)



# Van Geert

## Wie is Geert Heijenk?



*Door: Geert Heijenk*
*Onderwijsdirecteur van de studie Technische Informatica*

**Dit is de laatste keer dat ik een stukje zoals dít schrijf voor I/O Vivat. Mocht dit voor de redactie van het blad wat verontrustend klinken; geen zorgen: dit is zeker niet mijn laatste column voor I/O Vivat. Maar dit is wel mijn laatste bijdrage waar ik zelf het hoofdonderwerp ben. Ik denk dat ik als nieuwe opleidingsdirecteur Informatica voor veel lezers van dit blad toch een onbekende ben. Daarom lijkt het me goed deze column te misbruiken en mezelf te introduceren.**

Het vakgebied Informatica is inmiddels oud genoeg om een alumnus als opleidingsdirecteur te hebben. Voordat ik mij in 1983 aanmeldde voor de toen nog heel jonge studie Technische Informatica aan de Universiteit Twente had ik mijn jeugd doorgebracht op het platteland tussen de fraaie Hanzesteden Zutphen en Deventer. Mijn ervaring met het vakgebied informatica beperkte zich op het moment van aanmelden tot het schrijven van enkele simpele computerprogrammaatjes in de programmeertaal ECOL. De editor voor ECOL programma's bestond uit een potlood en een set schrapkaarten, één per programmaregel. Een syntax-error kostte je al snel twee weken, de tijd tussen het opsturen van je programma, een stapel schrapkaarten, en het terugkrijgen daarvan, inclusief een uitdraai van de foutmelding van de compiler, en eventuele output van het programma. Na 5 jaar waarin ik onder andere in aanraking kwam met modernere programmeertalen heb ik mijn studie verlengd met een promotieonderzoek op het gebied van pakketgeschakelde computernetwerken, zeg maar het Internet.

Tussen mijn promotie en mijn terugkeer op de Universiteit Twente als universitair hoofddocent heb ik voor Ericsson gewerkt. Het bedrijf is wellicht het meest bekend van hun producten op het gebied van mobiele netwerken. Ik heb hier eerst als strategisch onderzoeker, en later als hoofd van een onderzoeksafdeling gewerkt aan, onder andere, Internettechnologie, 3G en Bluetooth.

Sinds het begin van mijn promotieonderzoek heb ik met allerlei internationale partijen samengewerkt. Ik heb die internationale dimensie van mijn werk altijd bijzonder waardevol gevonden. Ook heb ik meerdere malen een periode van 3 a 4 maanden in het buitenland doorgebracht, als onderzoeker aan de University of Pennsylvania in Philadelphia, als visiting professor aan de University of California in Irvine, en later bij INRIA Rocquencourt, nabij Parijs. Privé is reizen jarenlang een grote hobby van mij geweest, liefst naar enigszins ongebruikelijke bestemmingen, bijvoorbeeld op een paard door de steppen van Mongolië, of met een vrachtboot over de rivier de Niger naar Timboektoe.

Omdat de wereld in hoog tempo kleiner wordt, en onderzoek, ontwikkeling en handel internationaler, is de kans dat degene die op dit moment een studie Technische Informatica doet ook in een internationale omgeving komt te werken zeer groot. Daarom, en omdat ik het persoonlijk zeer waardevol vind, wil ik als opleidingsdirecteur internationalisering een grotere rol geven in de studie informatica dan het nu heeft. Internationalisering heeft twee kanten: als student zelf naar het buitenland gaan voor een (afstudeer)stage of om aan een buitenlandse universiteit vakken te volgen, en op de Universiteit Twente zelf een meer internationale omgeving creeren, met buitenlandse studenten. Voor dat laatste is het belangrijk dat we de opleiding Informatica volledig Engelstalig maken.

Ondanks mijn affiniteit met het internationale ben ik enkele jaren geleden teruggekeerd naar de bossen tussen Zutphen en Deventer, waar ik nu woon met mijn vriendin en ons dochtertje. De plek is grotendeels verstoken gebleven van de technologieën waaraan ik flinke bijdragen heb geleverd: mobiel netwerk: geen dekking, Internet: 2 Mbit/s adsl. Kortom alle gelegenheid om een goed boek te lezen, lekker muziek te luisteren (of te maken), voor sporten in de natuur, of om samen met vrienden lekker te eten en een goed glas wijn te drinken.

In 1983 begonnen met de studie Technische Informatica aan de Universiteit Twente. Nadat hij met 5 jaar de studie afgerond had, is hij doorgegaan met promoveren. Voordat hij terugkeerde als universitair hoofddocent aan de Universiteit Twente, heeft Geert voor Ericsson gewerkt. Daarnaast heeft hij veel van de wereld gezien. In privéreizen, maar ook vanuit zijn functie als universitair onderzoeker. Wellicht komt hier zijn passie voor internationalisering vandaan.

Sinds collegejaar 2014-2014 heeft Geert Heijenk het stokje overgenomen van Rom Langerak als OLD van Technische Informatica.

# Security Analytics

## Toenemend inzicht in de staat van informatiebeveiliging

*Door: Herman Slatman*
*Redacteur I/O Vivat*

**Veel organisaties zijn al jaren bezig met het verbeteren van hun beveiligingsmaatregelen om kwaadwillenden buiten de deur te houden. Daarbij werd in de meeste gevallen vooral de focus gelegd op defensieve maatregelen. Die maatregelen bestaan onder andere uit technologieën die er voor moeten zorgen dat buitenstaanders geen toegang krijgen tot bezittingen van de organisatie, zoals bedrijfskritische databases en documenten, en daar bovendien geen schade aan kunnen toebrengen.**

Het lijkt er tegenwoordig echter steeds meer op dat preventieve maatregelen niet meer toereikend zijn. In een veranderend landschap van informatietechnologie, beïnvloed door onder andere een grotere mobiliteit, de groeiende mogelijkheden wat betreft thuis werken en grotere afhankelijkheid van informatietechnologie, krijgen organisaties te maken met nieuwe en onbekende dreigingen die soms jarenlang ongedetecteerd blijven. Daarnaast lijkt het niet langer de vraag te zijn óf er ingebroken wordt op de IT systemen, maar wánneer dat gebeurt.

Een toenemend aantal experts en bedrijven ziet in dat het zeer belangrijk is om er in het geval van een beveiligingsincident op tijd bij te zijn om zo de schade te kunnen beperken. Door Network World geïntroduceerd in mei 2013 als 'the next big thing in IT security', zou Security Analytics wel eens het antwoord kunnen zijn op de groeiende vraag naar betere detectiemethoden. Verschillende bedrijven bieden inmiddels producten aan die aangeprezen worden over next generation en state-of-the-art detectiemethoden te beschikken.

De rest van dit artikel zal dieper ingaan op het ontstaan van Security Analytics, wat de fundamentele elementen ervan zijn en zal naast het introduceren van enkele producten ook enkele belangrijke vraagstukken voor de toekomst introduceren.

### Het ontstaan van Security Analytics

De meeste organisaties zijn tegenwoordig in sterke mate afhankelijk van informatiesystemen. In een simpel geval kan het daarbij gaan om de PC die gebruikt wordt voor de administratie, maar het kan ook gaan om gigantische netwerken bestaande uit duizenden workstations en mainframes die allemaal met elkaar in verbinding staan. Die informatiesystemen ondersteunen in veel gevallen bedrijfskritische processen en zodra een systeem niet bereikbaar is of als er met data is geknoeid, kunnen die processen in de war gestuurd worden. Het is dus van belang dat informatiesystemen beschermd worden.

Zoals in de introductie al werd beschreven, word er in veel gevallen al wel gebruik gemaakt van verschillende defensieve maatregelen. Een voorbeeld hiervan is een firewall: verbindingen van buitenaf die niet aan specifieke regels voldoen worden zo afgesloten en services die binnen de firewall draaien kunnen dan niet bereikt worden. Tegen-

woordig worden aanvallen echter geavanceerder en vinden kwaadwillenden steeds nieuwe manieren om defensieve maatregelen te omzeilen en systemen te compromitteren. Het is dus zaak om snel een beveiligingsincident te kunnen detecteren en gecompromitteerde systemen te isoleren indien mogelijk.

De eerste generatie van detectiemethoden bestond eigenlijk uit verschillende kleine stukken software die door systeembeheerders gecombineerd konden worden om zo een totaaloplossing te realiseren voor het monitoren van computernetwerken en –systemen. Zo zou je kunnen denken aan het parsen en interpreteren van de toegangsgegevens van een webserver. Eventuele eigenaardigheden zouden dan in ieder geval na het optreden van een beveiligingsincident naar buiten komen, maar real-time detectie vraagt daarnaast om meer intelligentie, bijvoorbeeld in de vorm van regelsets. Dat die oplossingen niet toereikend bleken moge duidelijk zijn.

Om meer overzicht te krijgen en tevens niet telkens opnieuw het wiel te hoeven uitvinden introduceerden verschillende aanbieders zogenaamde Security Information and Event Management (SIEM) systemen. Deze systemen aggregeren door systemen gegenereerde data uit verschillende bronnen, zoals webserver toegangsgegevens, netflow data en firewall logs, om deze vervolgens op te slaan en te controleren op verschillende aanvallen. Aanvallen kunnen gedetecteerd worden door deze te modelleren met regelsets, maar detectie kan ook gebaseerd zijn op het detecteren van afwijkende patronen in de data.

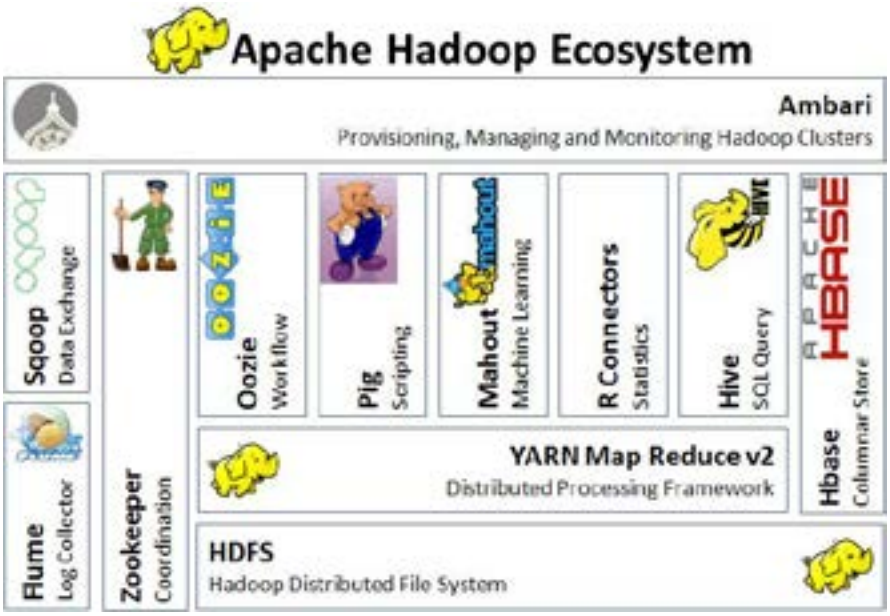
Het huidige dreigingslandschap vraagt echter om een zwaardere aanpak. De hoeveelheid dataverkeer, en dus de hoeveelheid te controleren netwerk data neemt toe. Daarnaast gaan ook de snelheden van dataverkeer omhoog, en willen organisaties in sommige gevallen real-time kunnen bekijken of er een aanval plaatsvindt. Naast een groter volume en snelheid van de data, is data tegenwoordig ook steeds vaker niet gestructureerd en dus niet in een (relationele) database te plaatsen. Een kenner zal ze al herkend hebben: de 3Vs van Big Data: Volume, Velocity en Variety.

> "...belooft een antwoord te zijn op verouderde technologie"

Security Analytics belooft een antwoord te zijn op de problemen die tegenwoordig aan het licht komen door het gebruik van snel verouderende technologie. Verschillende Big Data technologieën, zoals Hadoop en MapReduce, kunnen worden aangewend om grote hoeveelheden data te kunnen verwerken binnen kortere verwerkingstijden. Security Analytics stelt een menselijke analist in staat om bruikbare kennis te extraheren en te rapporteren om zo de mate van beveiliging te verhogen en bedrijfsrisico's te verminderen.

## State of the Art

Omdat de vraag naar beter toereikende analyseprogramma's voor beveiliging groeide, zijn er al verschillende aanbieders die complete softwarepakketten leveren die kunnen omgaan met de nieuwe wensen van organisaties. Enkele voorbeelden hiervan zijn Splunk, LogRhythm en het Security Analytics Platform van Bluecoat. Deze oplossingen zijn echter niet voor iedere organisatie weggelegd omdat er vaak een




Figuur 2: Schematische weergave van het Hadoop ecosysteem waarin verschillende technologieën voor het efficient verwerken van big data samenkomen.

## Threat Intelligence

Threat Intelligence is bedoeld om nog sneller in te kunnen spelen op huidige dreigingen. Het idee erachter is dat er uit verschillende bronnen informatie over bedreigingen wordt gehaald. Met die externe informatie kan een organisatie zich een beter beeld scheppen van de huidige dreigingen zonder dat er een incident heeft plaatsgevonden bij de organisatie zelf. Door de data die intern beschikbaar is, te verrijken met informatie over huidige dreigingen en die data in context te plaatsen kunnen gedegener analyses plaatsvinden.

Belangrijke eigenschappen van Threat Intelligencezijn onder andere het feit dat de informatie uit betrouwbare bronnen geput is en dat deze juist verwerkt is voordat deze aangeboden wordt als zijnde 'intelligence'. Bronnen kunnen daarbij uiteenlopen van Facebook tot ondergrondse fora, maar moeten te allen tijde door experts geselecteerd worden. Daarnaast moeten de gegevens accuraat en op tijd geleverd worden om van waarde te kunnen zijn voor organisaties.

groot prijskaartje aan deze oplossingen hangt. Daarnaast vergen deze pakketten in veel gevallen specialistische operationele kennis en zullen verantwoordelijke werknemers dus training moeten krijgen om met deze programma's te werken.

in te spelen zonder daarbij fouten te maken. Over het algemeen ligt het aantal false positives nog hoog, waardoor een analist veel tijd kwijt kan zijn aan valse meldingen. Het bedrijf SparkCognition lijkt echter fundamentele stappen te zetten om de menselijke analist te ontlasten. Zij combineren de kracht van IBM Watson, die reeds zijn kunnen heeft bewezen in verschillende andere disciplines, met hun eigen security analytics platform om zo hun klanten te kunnen voorzien van cognitive security analytics, iets dat SparkCognition zelf beschrijft als het toevoegen van menselijk denkvermogen en intuïtie aan bestaande detectiemethoden en security analytics oplossingen.

> "een analist zal nog lang een belangrijke schakel blijven"

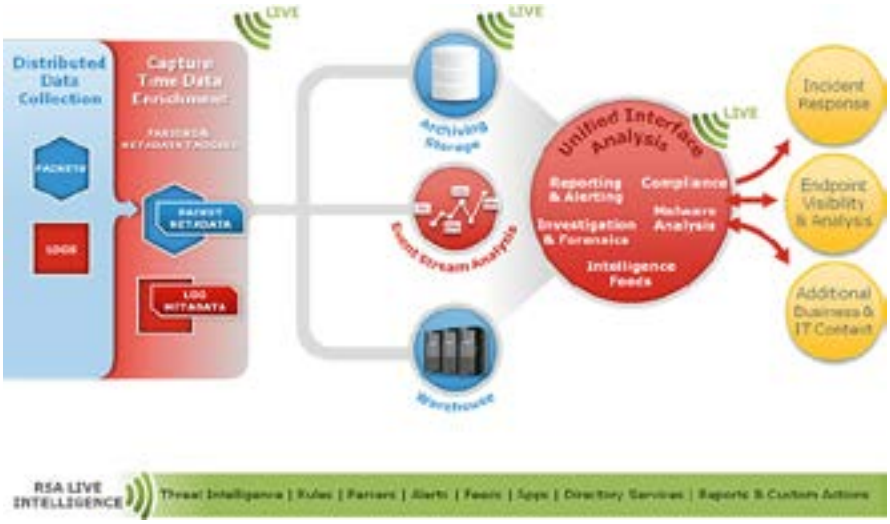
OpenSOC is een open source alternatief dat verschillende andere open source big data-technologieën combineert om zo uitbreidbare en schaalbare security analytics te bieden. Enkele technologieën waarvan gebruik gemaakt wordt, zijn Storm, Kafka, Hadoop, Hive en HBase, die allen onder paraplu van de Apache Software Foundation vallen. Verder bevat het platform verschillende algoritmen om onregelmatige patronen te kunnen detecteren en mogelijkheden om dataverkeer inzichtelijk te maken. Een organisatie die om wat voor reden dan ook geen duur, commercieel security analytics pakket wil en of kan aanschaffen kan mogelijk met OpenSOC uit de voeten.

Dat een menselijke analist nog lange tijd een belangrijke schakel zal vormen bij het analyseren van de informatie die een willekeurige security analytics oplossing voortbrengt moge duidelijk zijn. Het blijft voor een systeem namelijk lastig om op nieuwe ontwikkelingen en het veranderende dreigingslandschap in te spelen zonder daarbij fouten te maken. Over het algemeen ligt het aantal false positives nog hoog, waardoor een analist veel tijd kwijt kan zijn aan valse meldingen. Het bedrijf SparkCognition lijkt echter fundamentele stappen te zetten om de menselijke analist te ontlasten. Zij combineren de kracht van IBM Watson, die reeds zijn kunnen heeft bewezen in verschillende andere disciplines, met hun eigen security analytics platform om zo hun klanten te kunnen voorzien van cognitive security analytics, iets dat SparkCognition zelf beschrijft als het toevoegen van menselijk denkvermogen en intuïtie aan bestaande detectiemethoden en security analytics oplossingen.

## Conclusie

Organisaties zijn zich al jaren bewust van de constante dreiging van beveiligingsincidenten. Oorspronkelijk namen organisaties voornamelijk preventieve maatregelen om zich te wapenen tegen deze dreigingen, maar in het huidige dreigingslandschap volstaat die aanpak in veel gevallen niet meer. Dreigingen blijken steeds langer ongedetecteerd te kunnen blijven en kunnen een organisatie zo veel imago- en financiële schade opleveren.

Security Analytics heeft tot doel om organisaties te helpen bij het voorkomen van beveiligingsincidenten. Door inzet van big data, machine learning en data science kunnen hopelijk nieuwe, onbekende bedreigingen gedetecteerd en geanalyseerd worden. Een ander voordeel van Security Analytics is dat de technologie ervoor zorgt dat er sneller gereageerd kan worden: het verwerken van data gaat sneller dan met traditionele oplossingen en data analyse kan in sommige gevallen zelfs real-time plaatsvinden. Ontwikkelen zoals die van SparkCognition beloven daarnaast nog slimmer en met intelligentie grenzend aan die van het menselijk kunnen te kunnen inspelen op hedendaagse cyberdreigingen. Of Security Analytics de zogenaamde silver bullet in het arsenaal van de security operations specialist wordt moet nog duidelijk worden, maar de vooruitzichten zijn veelbelovend.




Figuur 3: Schematisch overzicht van de onderdelen en mogelijkheden van Security Analytics

## Bronnen


Big Data Analytics for Security
*Alvaro A. Cárdenas et. al. http://www.utdallas.edu/~alvaro.cardenas/papers/IEEESnP.pdf (2013)*

OpenSOC
*http://opensoc.github.io/*

Apache Hadoop
*https://hadoop.apache.org/*

Anitian Intelligent Information Security Blog
*Anitian https://blog.anitian.com/*

ENISA Threat Landscape 2014
*ENISA https://www.enisa.europa.eu/ (2015)*

An Analysis of Security Information and Event Management Systems
*HENRIK KARLZÉN (2009)*

SparkCognition
*http://sparkcognition.com/*

Big data security analytics can become the nexus of information security integration
*Jon Oltsik, Network World (2014)*

# WE TURN **YOUR IDEAS** INTO TOMORROW'S PRODUCTS

## APPLIED MICRO ELECTRONICS

**AME is a fast growing organization developing and manufacturing high quality products with electronics. Our goal is to create innovative products for our customers that exceed market expectations by making use of state-of-the-art development facilities and a highly automated manufacturing environment. Driven by technology, we strive for the best solution combining the disciplines of applied physics, electrical, mechanical, software and industrial engineering.**

## OUR OFFER

**We offer you a challenging career full of opportunities for personal and professional growth.**

### JOIN OUR TEAM OF EXPERTS

Driven to exceed expectations and to excel in creating innovative solutions, our team of experts is continuously looking for future best-in-class colleagues within the technological disciplines of applied physics, electrical, mechanical, software and industrial engineering.

### CAREER POSSIBILITIES

If you are interested in working with a talented, ambitious and experienced team of professionals using the best tools available and would like to work in a fast growing organization full of career opportunities then you are most welcome to apply for a job or take a look at our opportunities by visiting our website.

### INTERNSHIP OPENINGS

AME is the ideal work environment to develop hands-on experience while completing your studies. You will be involved in challenging real-world projects and work with experts from a multitude of technological disciplines. We invite you to get in touch with us to discuss any internship openings.

AME

**Applied Micro Electronics "AME" B.V.**
Esp 100 | 5633 AA Eindhoven | recruitment@ame.nu | +31 40 2646400

WWW.AME.NU

# Van Enigma tot RSA

## Hoe zit dat nou eigenlijk met cryptografie?

*Door: Florian Mansvelder*
*Redacteur I/O Vivat*

**Het begon ooit allemaal vrij simpel, met de zogenoemde Caesar-cipher poogde Julius Caesar zijn berichten voor eventuele vijanden onleesbaar te maken. Dit ging als volgt: elke letter in een tekst werd vervangen door een andere letter in het alfabet, namelijk een letter een aantal posities naar links of naar rechts. Zo zou bijvoorbeeld een A een F worden, een B een G, enzovoorts. Wanneer een bericht onderschept werd, dan konden de onderscheppers alsnog het bericht niet lezen, tenzij zij de sleutel hadden - namelijk het aantal posities dat elke letter was opgeschoven. Het is echter niet zozeer nodig een wiskundig genie te zijn om deze sleutel alsnog te achterhalen, waardoor deze codering tegenwoordig niet meer wordt toegepast.**

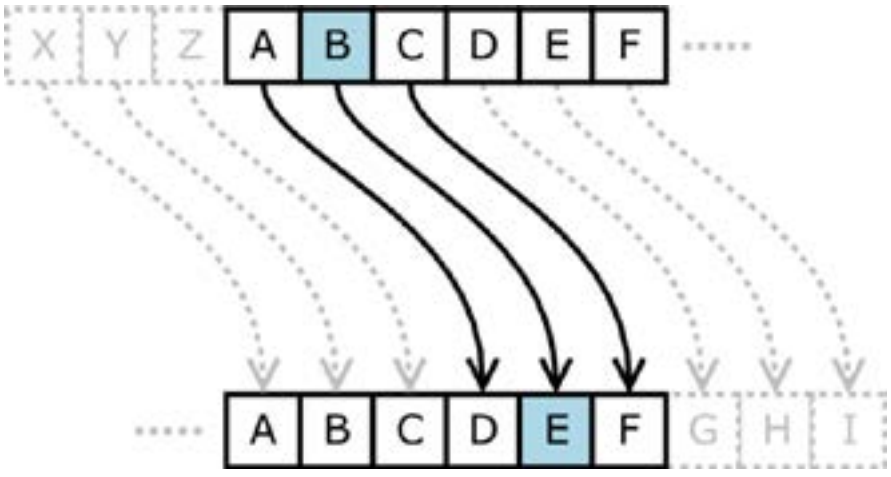
### Verzegeling en zegelring

Niet alleen was het van belang dat enkel degene voor wie een bericht bedoeld was deze kon lezen, het was ook zeker nodig aan te kunnen tonen wie de afzender was van een bericht, liefst met zoveel mogelijk zekerheid. In het vroegere Mesopotamië werden kleitabletten ondertekend met behulp van een zogehete zegelrol - een cilinder van vaak een edelsteen of ander hoogwaardig materiaal, waarin een afbeelding is uitgesneden. Deze zegelrol kon men over een kleitablet rollen om zo het tablet te ondertekenen. Zo ontstond een van de eerste methoden voor het zetten van een handtekening.

Een zegel als handtekening werd vele jaren later nog steeds gebruikt; hoogstaande mensen hadden rond de middeleeuwen een zogehete zegelring. Men kon een brief oprollen of dicht vouwen, en verzegelen met kaarsvet, door het heet op de brief te druppelen. Vervolgens werd hierin de zegelring gedrukt, en de afbeelding van de ring stond nu op de brief wanneer het kaarsvet was gestold. Niet alleen kon een ontvanger vaststellen dat de brief eerder gelezen was wanneer het zegel gebroken was, tevens wist men zeker wie de afzender was vanwege de afbeelding op het zegel, net als met de zegelrol.

### Beter, sneller, lastiger

Een goed voorbeeld van enryptie uit de vorige eeuw is de door Arthur Scherbius uitgevonden Enigma-machine. Tot na de eerste wereldoorlog was het nog de normaalste zaak van de wereld om berichten te versleutelen met pen en papier. Enkele uitvinders begonnen echter rond deze tijd de werken aan machines om het versleutelwerk te doen. Ze streefden naar het voorkomen van menselijke fouten, een sneller proces, en natuurlijk een lastiger te kraken versleuteling. In 1918 was de Enigma af. Hoewel de machine voor commerciele doeleinden niet goed verkocht, waren er uiteindelijk tussen 1925 en 1945 zo'n 30 000 Enigma's in omgang in het Duitse leger.




Figuur 1: Voorbeeld van een Ceasar-cypher

## Hoe het precies werkt

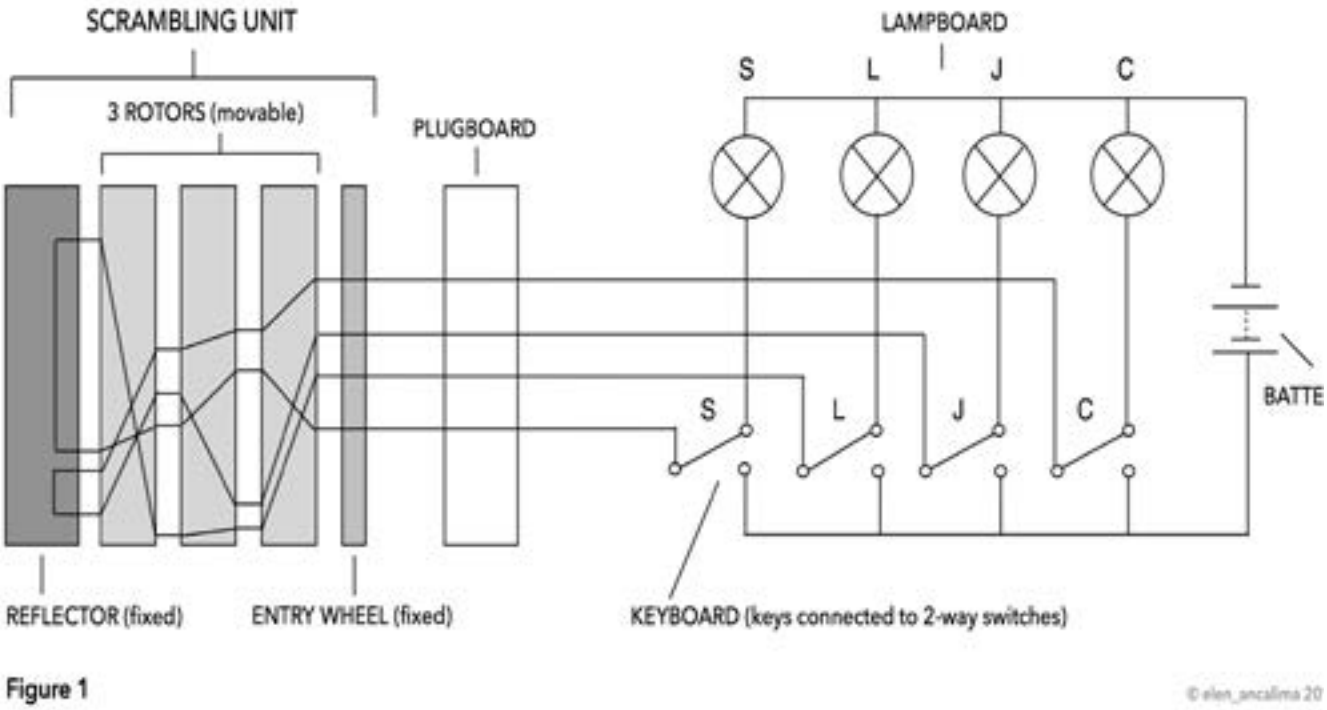
In principe is de Enigma gebaseerd op substitutie codering, net als de Caesarcipher. De Enigma neemt het principe echter veel en veel verder. In een gegeven staat van de machine is elke letter gelinkt aan een bepaalde cijfertekst-letter. Wanneer de ene letter wordt aangeslagen, wordt de andere letter teruggegeven. Tussen de links zit een zogeheten "scrambler". Wanneer een letter wordt aangeslagen verschuift de scrambler een bepaalde hoeveelheid posities, waardoor de links ook verschuiven. Dit betekent dat eenzelfde letter niet consequent eenzelfde cijfertekst-letter oplevert. Bij de Enigma staan de letters op ronde schijven die langs elkaar roteren. Telkens als er een letter wordt aangeslagen dan roteren de scramblers. De Enigma heeft niet één, maar vier scramblers, die elk een losstaande hoeveelheid posities kunnen roteren per ingevoerde letter. De eerste scrambler versleutelt de initiele tekst, de tweede versleutelt de output van de eerste, en de derde weer van de tweede. De vierde scrambler geeft de tekst terug aan de derde, waardoor de tekst nogmaals door alle scramblers gaat voordat het als cijfertekst wordt weergegeven. Alle letters werden dus zeven keer gescrambled.

Met behulp van een identieke machine is het heel gemakkelijk de tekst te ontcijferen, omdat de machine terug laten draaien precies de originele letters geeft. Dit vereist echter wel dat alle schijven hetzelfde zijn ingesteld als bij de machine die de tekst versleuteld heeft, en de beginopstelling moet ook exact hetzelfde zijn. De Enigma heeft $10^{20}$ mogelijke opstellingen, dus bijvoorbeeld brute forcen (elke mogelijkheid proberen tot de juiste gevonden is) is niet goed toepasbaar.

## Symmetrie

Tegenwoordig zijn er een stuk meer wiskundige mogelijkheden voor versleuteling, en het gebruik van snelle computers maakt lastige berekeningen die toentertijd simpelweg te veel tijd kosten, nu te doen in een handomdraai. Substitutie coderingen zoals de Caesarcipher en de Enigma vallen onder symmetrische encryptie. Dit wil zeggen dat het ontsleutelen van een cijfertekst in principe exact het tegenovergestelde is van het versleutelen van de originele tekst. Theoretisch zijn dit soort coderingen uiteindelijk bijna altijd te kraken, omdat er meestal een soort spoor terug te vinden is van de sleutel. Bij een simpele substitutie codering is bijvoorbeeld frequentie-analyse toepasbaar. Dit houdt in dat er wordt gekeken naar het aantal keren dat een letter voorkomt in normale teksten, en dit wordt vergeleken met het aantal keren dat letters voorkomen in de cijfertekst. De letter E komt over het algemeen het meest voor binnen onze taal, dus stel dat de M het meest voor komt in de cijfertekst van een simpele substitutie codering, is het zeer waarschijnlijk dat alle E's zijn vervangen door een M. De Enigma loste dit probleem enigszins op door telkens de substitutie aan te passen, maar ook de Enigma is uiteindelijk gekraakt. Vaak wordt symmetrische encryptie ook wel secret-key encryptie genoemd, omdat het ontsleutelen van de tekst in wezen enkel de sleutel vereist, deze dient dus geheim te worden gehouden.

> "Bij simpele substitutiecodering is bijvoorbeeld frequentie-analyste toepasbaar"




Figuur 2: Schema van de werking van Enigma

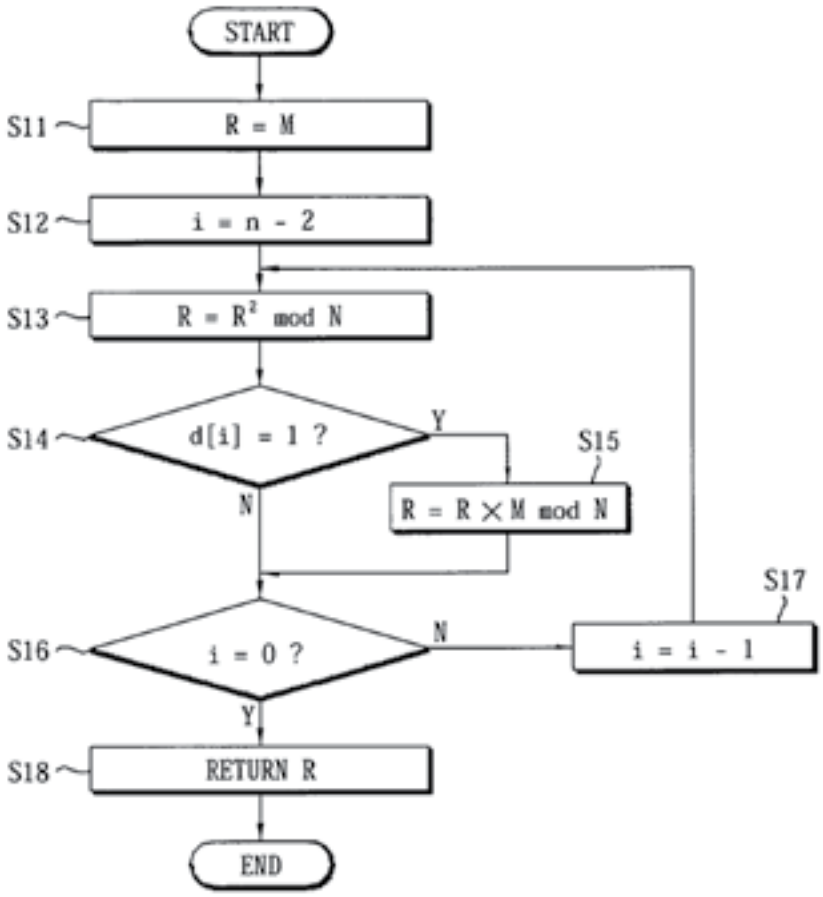
## Asymmetrie

Waar tegenwoordig veelal naar wordt gestreeft is het gebruik van asymmetrische encryptie. Hierbij probeert men een tekst zo te versleutelen, dat er een andere sleutel nodig is om te tekst te ontsleutelen. Deze encryptie wordt ook wel public-key encryptie genoemd, omdat de sleutel waarmee de tekst asymmetrisch versleuteld wordt over het algemeen publiek bekend is. Dit zorgt ervoor dat het mogelijk is een tekst te versleutelen en naar iemand te sturen, zonder eerst een geheime sleutel te hoeven uit te wisselen. De ontvanger is de enige die de tweede sleutel van de sleutelset heeft, en kan hiermee de tekst ontsleutelen; met enkel kennis van de publieke sleutel is ontsleuteling van een tekst in essentie niet mogelijk. Het probleem bij dit soort coderingen is dat het vaak lastige berekeningen betreft. Een goed voorbeeld is RSA codering, vernoemd naar de bedenkers Ron Rivest, Adi Shamir en Leonard Adleman. RSA codering betreft een berekening van een goede twaalf tot vijftien regels, die zelfs voor computers van deze tijd nog altijd relatief zwaar is.

> "ontsleuteling van een tekst is in essentie niet mogelijk."

## Afweging

Er moet dus een afweging worden gemaakt bij het versleutelen van berichten: is 100% veiligheid gewenst, of moet het redelijk goed zijn, maar wel snel? De beste oplossing dusver is een combinatie van zowel symmetrische, als asymmetrische codering. Een groot probleem bij symmetrische encryptie is dat beide partijen de geheime sleutel moeten weten, voordat er überhaubt iets versleuteld kan worden. Wat men tegenwoordig doet is het volgende: door middel van RSA codering wordt een geheime sleutel onleesbaar gemaakt voor derden, en deze wordt vervolgens verstuurd. Hierna verloopt de communicatie symmetrisch versleuteld met deze sleutel. Dit werkt vrij goed, omdat het niet mogelijk is de geheime sleutel te onderscheppen, en er tegenwoordig symmetrische encryptie-algoritmen bestaan die zonder kennis van de geheime sleutel een jaar of tien kunnen duren om te ontcijferen, en toch snel toepasbaar zijn. Tot op heden heeft deze combinatie van twee soorten encryptie bij velen de voorkeur, en blijkt tot zover tevens zeer effectief.




Figuur 3: Werking RSA

## Bronnen


http://www.kennislink.nl/publicaties/cryptografie
*kennislink.nl*

http://kunst-en-cultuur.infonu.nl/geschiedenis/51807-rolzegels-handtekeningen-in-klei.html
*kunst-en-cultuur.infonu.nl*

http://www.faqs.org/espionage/Ec-Ep/Enigma.html
*faqs.org*

http://support.microsoft.com/en-us/kb/246071
*support.microsoft.com*

http://mathworld.wolfram.com/RSAEncryption.html
*mathworld.wolfram.com*

http://upload.wikimedia.org/wikipedia/en/7/75/Caesar3.png
*uploads.wikimedia.org*

http://upload.wikimedia.org/wikipedia/commons/3/3c/Four-rotor-enigma.jpg
*uploads.wikimedia.org*



# Van de voorzitter

## De identiteit van Inter-*Actief*

*Door: Rien Heuver*
*Voorzitter bestuur 36*

**In onze wereld van hedendaagse ICT zijn 'anonimiteit' en 'privacy' altijd makkelijk scoren op de bullshitbingokaart. Maar je kunt pas spreken van anonimiteit als je kunt spreken van een identiteit. Maar wat is dan de identiteit van Inter-*Actief*? Hebben wij een identiteit? Wat kenmerkt onze vereniging en wat maakt ons ons? We zeggen wel makkelijk dat het bestuur de vereniging vertegenwoordigt en dat de voorzitter het gezicht van de vereniging is, maar ik voel mij niet de identiteit van Inter-*Actief* en de rest van het bestuur evenmin. Of moeten we stellen dat onze identiteit fluctueert? Dat ieder jaar, met ieder nieuw bestuur, de identiteit van Inter-*Actief* weer onderhevig is aan verandering?**

Een hele serie vragen waarvan de antwoorden niet voor de hand liggen. Maar toch probeer ik in de rest van deze column een antwoord te schetsen; met de nadruk op schetsen want ook ik weet niet precies wie wij zijn.

Laat ik beginnen met iets vatbaars: mijn presentatie op de open dagen. Tijdens deze presentatie vertel ik wat een studievereniging aan de UT nou precies inhoudt en daarna vertel ik over onze vereniging; de vier pijlers van Inter-*Actief*. - Pas op, marketingtermen. -

- De toekomst van de student
- Verbetering van de studie
- Opdoen van ervaring
- Gezelligheid

De gedachten hierachter: Inter-*Actief* werkt met een hele rits bedrijven samen: allemaal potentiële werkgevers voor later. Daarnaast gaan we natuurlijk regelmatig met docenten/modulecoördinatoren in gesprek om de opleiding beetje bij beetje te verbeteren. Met onze uitgebreide lijst van commissies is het opdoen van extracurriculaire ervaring ook een uitgelezen kans en als laatste zijn we hartstikke gezellig met onze overload aan activiteiten en een haast continu geopende verenigingskamer. Maar is dat wat Inter-*Actief* kenmerkt? Is dat onze identiteit?

Veel verenigingen, stichtingen en met name bedrijven hebben iets als een toekomstvisie, een vijfjarenplan of een andere concrete invulling van een strategie. Bij Inter-*Actief* hebben we zoiets niet. Ieder bestuur schrijft zijn eigen beleidsplan en gaat daarmee aan de slag. Maar is dat slecht? Ik denk juist van niet. Ik denk dat dit juist iets is wat Inter-*Actief* eigen is. Doordat ieder bestuur zijn eigen ding kan doen, na bijsturing en goedkeuring van de ALV, hebben we juist een dynamische vereniging die snel kan reageren op veranderingen, van welke aard dan ook. Juist doordat je als kandidaatbestuur niet jezelf hoeft te vinden in een langetermijnstrategie, is het eenvoudiger om je thuis te voelen in de vereniging om die later te kunnen vertegenwoordigen.

Maar goed, doordat we geen vastgestelde visie hebben zou je ook weer kunnen stellen dat we geen identiteit hebben. Ieder bestuur kan weer zo anders zijn van aard dat er wellicht geen consistente lijn zit in het verenigingsbeleid. En stel we zijn zo ingericht dat niets Inter-*Actief* kenmerkt; is dat dan onze identiteit? De afwezigheid van een identiteit maakt wie wij zijn?

Dus nu is aan jou de vraag als lid of alumnus van onze vereniging: wat vind jij dat Inter-*Actief* kenmerkt, het onderscheidt van de rest; wat maakt ons ons? Ik hoor het graag, want ik weet het niet.

Op 21 november 1992 zag Rien Heuver zijn eerste daglicht. In Stadskanaal werd hij geboren en daar heeft hij ook zijn peuter- en kleutertijd doorgebracht. De start van zijn carrière, het leren lezen en schrijven, begon met een frisse start in Heerde, waar hij tot het begin van zijn studie aantoe gewoond heeft. Na 6 vrolijke jaren op de Wilhelminaschool was het tijd voor het voortgezet onderwijs. Tweetalig onderwijs, ook wel tto genoemd, moest het worden. Helaas daagden ook de nieuwe opleiding en de extra taal Riens bovenkamer weinig uit, dus was het na evenzoveel jaren als op de basisschool tijd voor iets nieuws. Gelukkig had Rien in de tussentijd zich kostelijk vermaakt met hobby's als muziek maken, tafeltennissen en mountainbiken, maar om ook iets te hebben waar je later echt de kost mee kunt verdienen besloot hij te starten aan de Universiteit Twente bij de opleiding Technische Informatica. Aangezien het lidmaatschapsgeld zich al terugverdiend heeft na de aanschaf van de eerste boeken, was Rien vanaf dag één van de opleidings-Kick-in lid van I.C.T.S.V. Inter-Actief. Echter, het duurde tot het begin van zijn tweede collegejaar eer hij ook actief werd bij de vereniging. Na, op chronologische volgorde, betrokken te zijn geweest bij de SkiCie, de CoLeX, de BHV'ers en de SymCie mag hij zichzelf nu voorzitter van de vereniging noemen voor het collegejaar 2014/2015.

# GEZOCHT

# TALENTEN ALS MARNIX

PASSIE:
UITDAGINGEN &
INNOVATIES

AMBITIE:
ECHT IETS BEREIKEN EN BETEKENEN,
OP TERMIJN MET MIJN EIGEN
BEDRIJF EN PROJECTEN.

BELANGRIJK BUITEN STUDIE/WERK:

1. SPORT
2. VRIENDEN
3. BUITENLUCHT

LEREN:
ECONOMIE/ONDERNEMEN,
PRESENTEREN & MEZELF
BETER UITDRUKKEN.

TALENT: LOGICA, RATIONEEL

BIG DATA OVER 10 JAAR:
MAAKT VEEL MAKKELIJKER
MEDE DANKZIJ GEORDENDE
DATABASES.

FAVORIETE WEBSITE:
STRAVA.COM
VELOVIEWER.COM

HELDEN:
LEONHARD EULER
&
EDSGER WYBE DIJKSTRA

KOFFIE:
ZWART

GEDREVEN INFORMATICA STUDENTEN ALS MARNIX, DIE LEREN WE BIJ MICOMPANY GRAAG BETER KENNEN. OM HET BESTE UIT ELKAAR EN DE BIG DATAVAN ONZE KLANTEN TE HALEN. OM SAMEN DROMEN TE VERWEZENLIJKEN, DOELEN TE BEREIKEN EN DUURZAAM TE GROEIEN.

MEER WETEN OVER MICOMPANY?

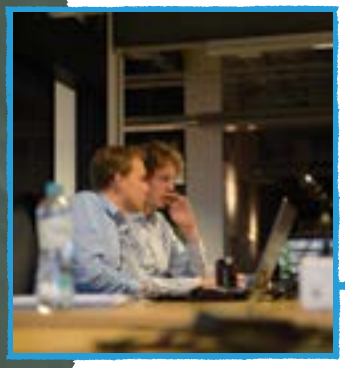
LEES HIERNAAST OVER DE DAG VAN MARNIX
BIJ DÉ BIG DATA SPECIALIST EN CHECK:
MICOMPANY.NL/TALENT

# WELKOM BIJ DÉ BIG DATA SPECIALIST

MICOMPANY IS DÉ SPECIALIST IN COMMERCIAL ANALYTICS. EN ANALYSEERT DE KLANTGEGEVENS VAN TOPONDERNEMINGEN ALS ACHMEA, BOL.COM, KPN EN DE GOEDE DOELEN LOTERIJEN. MICOMPANY ONTDEKT KANSEN UIT PATRONEN IN DE DATABASE (DISCOVERY) EN BOUWT DE ANALYTISCHE COMPETENTIE BIJ BEDRIJVEN (YOUR ANALYTICS). EN CREËERT ZO NIEUWE, DUURZAME GROEI.

## MICOMPANY ZOEKT TALENT

MIcompany is hard op zoek naar talenten die mee willen groeien met het succes van Big Data. Met aanleg voor het ontginnen, koppelen en verrijken van data. En het inrichten van duurzame Business Inteligence-oplossingen waarin de performance van bedrijven kan worden gemonitord.



## WAT KUN JE BIJ ONS LEREN?

Samenwerken aan analytische oplossingen. Complexe databestanden ontsluiten. En inzichten genereren en standaardiseren door het bouwen van rapportages, dashboards en analytische databases.

## DUS HEB JIJ...

- business sense & overtuigingskracht;
- passie voor programmeren;
- affiniteit met commerciële dienstverlening;
- en een technische WO opleiding afgerond, zoals Informatica?

## DAN BIEDEN WIJ JOU:

- een uitdagende functie binnen ons Technology team;
- gespecialiseerde trainingen om je tot Senior Technology Analyst te ontwikkelen;
- coaching door top senior professionals uit het vakgebied;
- inclusief zéér goede arbeidsvoorwaarden bij een jong, informeel, succesvol en hard groeiend bedrijf in het hartje van Amsterdam!

KIJK VOOR MEER INFORMATIE
ÉN JOUW KANSEN BIJ MICOMPANY OP:

MICOMPANY.NL/TALENT

SUSTAINABLE GROWTH THROUGH ANALYTICS

MI COMPANY

# Identity & Access Management

## De aanval kan ook van binnenuit plaatsvinden...

*Door: Michel Brinkhuis*
*Redacteur I/O Vivat*

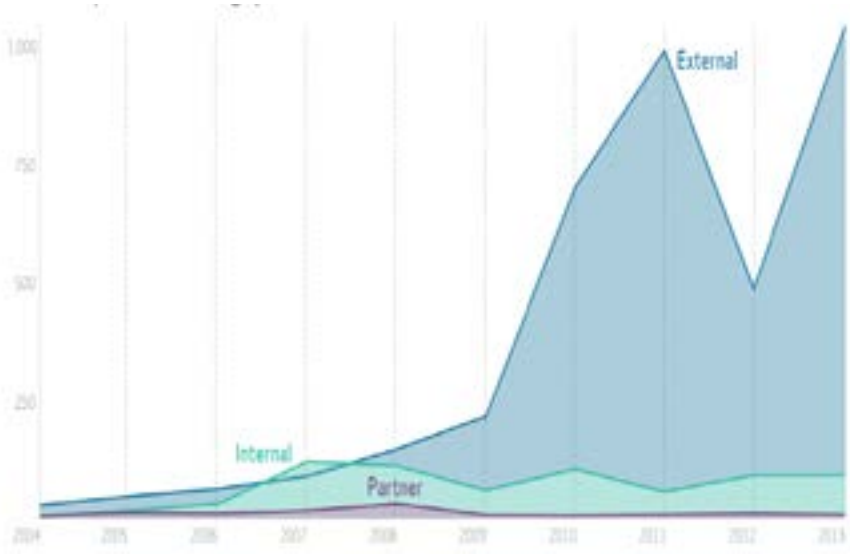
**Het is een bekend gegeven in de wereld van social engineering: al is je beveiliging nog zo goed, de mens is vaak de zwakste schakel. Omdat bijna iedereen toegang heeft tot bedrijfssystemen is het van groot belang voor bedrijven om te zorgen dat dit op een juiste wijze is geregeld. Als multinational met enkele tienduizenden werknemers wil je vermoedelijk niet dat iedere werknemer toegang heeft tot ieder bestand. Het zou namelijk zeer vervelend zijn als bedrijfsgevoelige informatie eenvoudig kan worden ingezien via de computer van een receptionist. Simpelweg omdat die computer zich vaak voor de toegangspoortjes van het bedrijfspand bevindt. Controleren wie er fysiek toegang heeft tot de machine is dan al iets lastiger, dan wanneer iemand eerst door een toegangspoortje moet. Zo'n fysieke drempel opwerpen is echter maar het begin: meestal zijn informatiestromen ook binnen een onderneming gescheiden.**

De procedures die het bedrijfsleven en de overheid hanteren om te bepalen wie toegang heeft tot welke data valt onder de noemer Identity & Access Management (IAM). Kort samengevat gaat dit over de bedrijfsprocessen en ondersteunende technologie om ervoor te zorgen dat de juiste mensen toegang krijgen tot de juiste bestanden en gegevens op het juiste moment.

### Het gaat soms fout

Om het belang van I&AM in te zien is het interessant om een blik op het verleden te werpen. Zijn er voorbeelden van organisaties waarbij het aan een juiste implementatie ontbrak, met de logische gevolgen van dien? Telecomgigant Verizon brengt jaarlijks een 'Data Brach Investigations Report' uit. In hun 2014-editie trekken ze conclusies op basis van meer dan 63.000 beveiligingsincidenten die in meer dan 90 landen hebben plaatsgevonden. Zo'n incident betekent overigens niet dat er door kwaadwillende partijen ook daadwerkelijk data is 'buitgemaakt'. Dat gebeurde in slechts 2% van de gevallen: 1367 keer.

Verizon heeft hun getallen ook uitgesplitst naar de oorzaken van deze incidenten. In meer dan 11.000 gevallen gaat het om 'insider and privilege misuse'. Daarbij kan worden gedacht aan mensen binnen de organisatie die bestanden benaderen of eventueel zelfs meenemen waar ze misschien helemaal niet bij zouden hoeven kunnen. Onderzoek van het Ponemon Institute dat vorig jaar is uitgevoerd laat zien dat 71% van de geïnterviewde personen (1166 IT-beheerders en 2276 werknemers bij bedrijven in de VS en de EU) zegt dat ze rechten hebben om bij meer bestanden te komen dan dat voor hun functie nodig is. Een voorbeeld van een 'datadiefstal' van binnenuit, puur vanuit de protocollen bekeken, is de verzameling




Figuur 1: Aantal inbraken per gevarencategorie over tijd

documenten die Edward Snowden meenam bij de NSA, waar hij als contractor was gestationeerd. Een ander voorbeeld is een echtpaar in de Verenigde Staten dat brood zag in het verkopen van bedrijfsgeheimen van General Motors, waar de man des huizes werkte, aan Chinese concurrenten. De man kopieerde vele bestanden naar een externe harde schijf, kort nadat hij een vertrekregeling aangeboden had gekregen. De totale waarde van de gekopieerde bedrijfsgeheimen zou veertig miljoen dollar bedragen.

In figuur 1 is te zien dat de grootste dreiging voor bedrijven moet worden gezocht buiten het bedrijf, maar ook intern is er zeker een risico. Daarnaast kunnen aanvallers van buitenaf soms lastig worden herkend, vooral als ze binnenkomen met gestolen gegevens. Zo'n externe aanvaller logt dan dus in op de systemen met de gegevens van een werknemer. Daardoor kan een aanval minder opvallen. Dit type aanval is volgens het onderzoek van Verizon het meest voorkomend in 2013. Het zorgt vaker voor problemen dan bijvoorbeeld spyware of een backdoor, zoal figuur 2 laat zien.

## I&AM implementeren

Grote organisaties implementeren veel van hun IT aan de hand van concepten benoemd in de Information Technolgy infrastructure Library; beter bekend als ITIL. Het is een reeks van best practices en concepten, die duidelijk maken hoe IT-beheerprocessen vormgegeven kunnen worden. Identity & Access Management is hier ook een onderdeel van, toegevoegd in versie 3. Binnen ITIL wordt access management onder meer gekoppeld aan event management (een ander 'process' binnen ITIL). Sommige events kunnen namelijk helpen bij het opsporen van situaties waarbij onterecht toegang tot een apparaat of dataset wordt verkregen. Er zijn twee sub processen benoemd binnen access management: het onderhoudt van de catalogus met alle gebruikersrollen en toegangsprofielen, en het verwerken van gebruikersrechtenverzoeken. (user access requests).

> "71% van de werknemers heeft meer rechten dan vereist"

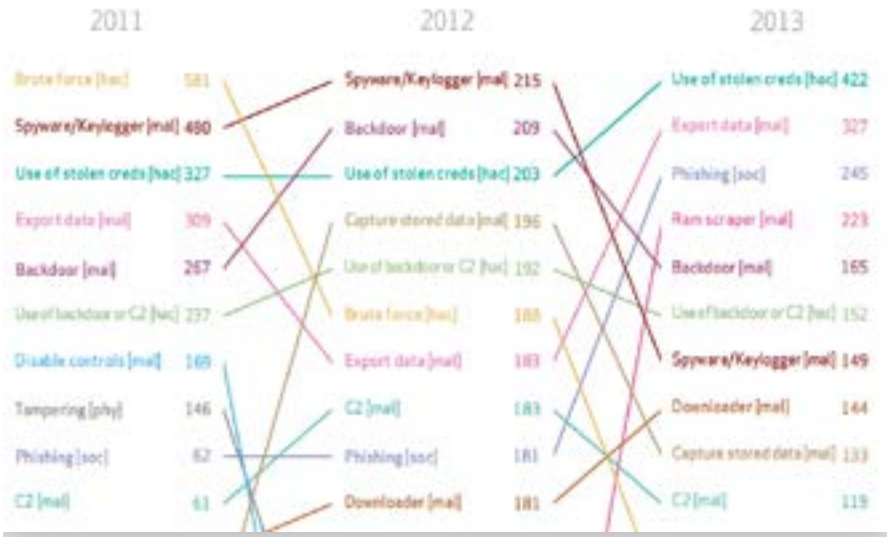
Het eerste subproces gaat in op het überhaupt maken van een onderscheid tussen verschillende rollen van gebruikers binnen de organisatie. Denk daarbij bijvoorbeeld aan het verschillen van een HR-rol en een Sales-rol. Beide medewerkers hoeven geen toegang te hebben tot precies dezelfde informatie: iemand op de HR-afdeling heeft voor zijn functie geen toegang nodig tot specifieke contracten, terwijl een salesmedewerker weinig van doen heeft met de Cv's van kandidaten op een engineering-functie. Het tweede sub proces laat organisaties vervolgens bewust omgaan met het toekennen van de gedefinieerde rollen aan gebruikers. Wanneer krijgt iemand welke toegangsrollen? En misschien wel net zo belangrijk: hoe lang heeft iemand deze rol? Het omvat dus het toekennen, wijzigen en afnemen van toegangsrollen.

## De grote spelers

Gartner heeft in januari van dit jaar een 'magic quadrant' gepubliceerd met grote spelers in de wereld van 'Identity Governance & Administration'; hieronder valt I&AM. Leider in dit gebied is SailPoint, welke wordt gevolgd door IBM en EMC. Deze laatste is bij velen waarschijnlijk wel bekend van de RSA-tokens. SailPoint is een relatief jong bedrijf: gestart in 2005, en moet opboksen tegen grote jongens als IBM en Oracle. I&AM is echter een sector die volop in beweging is. Ontwikkelingen als 'Bring your own device' en de opkomst van het Internet of Things vragen oplossingen die daarop inspelen. Grote spelers moeten zich daarop aanpassen, maar de dynamiek creëert dus ook kansen voor nieuwe bedrijven. Eén daarvan is bijvoorbeeld Exabeam.

## Toekomst

Het is voor een bedrijf lastig om zich te wapenen tegen een datadiefstal. Vooral als het van binnenuit gebeurd: bijvoorbeeld omdat iemand kan inloggen met andermans account, en daar misbruik van maakt. Daarnaast zijn er enorm veel potentiële aanvalsmethoden te bedenken. Zoveel, dat het niet mogelijk om voor iedere potentiële dreiging je systeem voor de volle honderd procent dicht te timmeren.




Figuur 2: Populariteit van aanvallen per type over tijd

Een opkomend onderdeel binnen I&AM software is gedragsanalyse, waarin Exabeam actief is. Daarbij wordt er het gedrag van iedere gebruiker continue bijgehouden. Op basis daarvan kan een patroon worden vastgesteld dat 'normaal gedrag' representeert. Vervolgens kan iedere sessie van een gebruiker worden vergeleken met dat patroon. Wijkt het af? Dan is dat een potentiële dreiging. Bijvoorbeeld omdat het account van een gebruiker zich ineens heel anders gedraagt dan in de maanden ervoor. Dat kan erop wijzen dat iemand anders gebruik maakt van het account. Hierbij gaat het dus niet zozeer om voorspelbaar gedrag, waarbij een bepaalde actie van een gebruiker een bepaalde 'trigger' raakt waardoor systeembeheerders op de hoogte kunnen worden gesteld, maar op een systeem dat op basis van al het gebruikersgedrag afwijkingen kan detecteren. Afwijkingen die je misschien zelf niet zo snel zou bedenken, en die dus lastig in triggers te vangen zijn.

> "Het is niet mogelijk je systeem voor elke dreiging dicht te timmeren"

## Internet of Things

Een analyst van Gartner ziet dat met de opkomst van het Internet of Things ook de 'Identity of Things' belangrijk wordt. Hij stelt dat I&AM voorheen ging over de relatie van een persoon met een bedrijfsproces. Echter, met de komst van 'things' als derde speler ontstaat er een heel scala aan nieuwe potentiële relaties tussen personen, 'things' en bedrijfsprocessen. Dat nieuwe stelsel beheren vraagt om een vernieuwde aanpak van I&AM. Hoe? Daar is nog niet veel duidelijk over, Gartner ziet de ontwikkeling aankomen. De oplossing moet worden geformuleerd door de industrie. Alles bij elkaar: I&AM lijkt een saai en formeel gebeuren, maar met ontwikkelingen op het gebied van cybercrime en nieuwe interacties tussen technologie en mens is het een volop bloeiend vakgebied.


Figuur 3: No entry

## Bronnen

Exabeam unveils user behavior platform - ExaBeam - *http://www.exabeam.com/news/exabeam-unveils-user-behavior-intelligence-platform-delivers-future-of-cyberattack-detection-and-response/*

Data Breach Investigations Report - Verizon - *http://www.verizonenterprise.com/DBIR/2014/*

Data breach from the inside out - PepperLaw - *http://www.pepperlaw.com/pdfs/LudolphR_SSR_10_2014_data-breachfrom-inside-out.pdf*

Gartner IGA Magic Quadrant - SailPoint - *https://www.sailpoint.com/gartner-magic-quadrant-iga-2014*

Identity of Things - Gartner - *http://blogs.gartner.com/earl-perkins/2014/08/04/the-identity-of-things-for-the-internet-of-things/*

//Column

# Samen elke dag een beetje beter

## Over ons onderwijs



*Door: Klaas Sikkel*
*Docent bij Technische Informatica en Business & IT*

**In het financieel dagblad (was ik nooit lees, maar gelukkig is er Facebook) stond onlangs een artikel over goed onderwijs [1]. Jaap Versfelt was ooit consultant bij McKinsey. Van gezinsleden hoorde hij veel verhalen over onderwijs. Soms kregen ze goed les van leuke leraren, soms ook erg slecht. Door de bank genomen is het onderwijs in Nederland redelijk goed, maar zeker niet geweldig. Jaap vroeg zich af of dat niet beter kon. Hij is gaan onderzoeken wat de kwaliteit van onderwijs bepaalt (kort samengevat: de leraar) en heeft de stichting Leerkracht opgezet die geïnteresseerde scholen helpt hun onderwijs te verbeteren.**

Beter onderwijs is niet maakbaar door het top-down op te leggen. Een interventie van bovenaf kan nuttig zijn als je van zwak naar redelijk onderwijs wilt komen. Maar goed onderwijs upgraden tot excellent onderwijs kan je niet afdwingen. Wat wel kan, aldus Jaap, is een cultuur creëren van samen elke dag een beetje beter.

In de methode van de stichting Leerkracht helpen leraren elkaar vooruit door drie kerninterventies: (1) doelen noteren op een verbeterbord, (2) samen lessen ontwerpen en (3) elkaars lessen bezoeken en feedback geven.

**Kunnen we hier iets van leren voor het hoger onderwijs, in de context van TOM aan de UT?**
In mijn beleving is het informatica-onderwijs bij ons best goed maar zeker niet excellent. Er zijn redenen waarom het onderwijs eigenlijk ook niet optimaal kán zijn: de werkdruk is hoog en over het algemeen vindt men onderzoek belangrijker dan onderwijs. Er wel iets in de academische cultuur in Nederland, maar dat gaat héél er langzaam.

Zouden interventies zoals die van Leerkracht daar verandering in kunnen brengen? Docenten zijn moeilijk aan te sturen. Je moet dan een kritische massa van docenten motiveren om het zélf te willen. En ze daar de ruimte voor geven. Maar met te weinig resources voor te veel ambities zie ik het voorlopig niet gebeuren (als men het überhaupt al zou willen).

**Zijn er andere manieren waarop we wel samen elke dag een beetje beter kunnen worden?**
Jazeker. Elementen daarvan zie ik ook op verschillende plekken om me heen. Docenten die met elkaar overleggen wat er in een module beter kan. Studentassistenten die, al dan niet daartoe uitgenodigd, hun ervaringen terugkoppelen aan docenten. Last but not least: Studenten die door middel van enquêtes, evaluatiebijeenkomsten of anderszins laten weten wat goed en wat minder goed is aangekomen. Bij serieuze klachten kan Inter-actief een bemiddelende rol spelen.

Dat dit werkt komt niet omdat het in procedures en reglementen is vastgelegd. Dat dit werkt komt omdat er bij Informatica een cultuur is waarin inbreng van studenten door het opleidingsbestuur en de meeste docenten op prijs gesteld wordt.

Ook dit loopt goed maar niet optimaal. Soms is de respons op enquêtes behoorlijk lauw. In december was ik bij een evaluatiegesprek waar een bescheiden 3 % van de studenten is op komen dagen. Wellicht is vaak ook niet duidelijk –en misschien is daarom de animo laag– wat de docenten er uiteindelijk mee doen.

Ik zie goede mogelijkheden om hier meer en beter gebruik van te maken. Stap bij de docent binnen als je wat op je lever hebt! (maar liefst niet allemaal tegelijk). Vul enquêtes in! (met name de open vragen). Ga naar evaluatiegesprekken! En als je denkt dat de docent er niks mee doet: stuur Inter-actief erop af!

Zo kunnen we samen het onderwijs beter maken. Elke dag een beetje.

Klaas Sikkel heeft Informatica (specialisatie Software Engineering) gestudeerd aan de Vrije Universiteit. Hij is aan de UT gepromoveerd in de Theoretische Informatica. Bij het onderzoeksinstituut GMD In Sankt Augustin (Duitsland) heeft gewerkt in de onderzoeksgroep voor Computer Supported Cooperative Work. In 1997 is Klaas aan de UT komen werken bij de vakgroep Informatiesystemen (inmiddels opgegaan in Services, Cybersecurity and Safety). Sinds 2013 is hij als docent betrokken bij de invoering van het Twents Onderwijsmodel bij Informatica en BIT.

In 2015 won Klaas de onderwijsprijs van Inter-*Actief*. Klaas houdt van fietsen en van klassieke muziek.

## Bronnen

[1] Thieu Vaessen: Alles staat of valt met de docent. Financieel dagblad, 7 maart 2015.
*http://www.stichting-leerkracht.nl/wp-content/uploads/2014/12/FD-artikel.pdf*

//Advertorial

kpn consulting

# De kleine lettertjes van de cloud

## Wie de voorwaarden van zijn cloudleverancier klakkeloos accepteert, is verloren

**Bij het overstappen op de cloud is een professionele aanpak onmisbaar. De eerste stap, zegt Simon van den Doel, is de cloudleverancier vragen om de voorwaarden. Vervolgens formuleert hij zeven vragen aan de hand waarvan de klant deze voorwaarden kan doorgronden. Een cloudvoorwaarden-abc.**

Wie nog niet in de cloud zit is hopeloos ouderwets. En wie de voorwaarden van zijn cloudleverancier(s) klakkeloos accepteert, is hopeloos verloren. Want wat nou als een cloudleverancier in rook opgaat, vastzit aan de Amerikaanse wet of z'n datacenters in Verweggistan heeft staan?

Waar data precies zijn opgeslagen, is niet voor ieder bedrijf even relevant. Wél moet iedere organisatie weten wat een cloudleverancier met zijn data doet. Anders hebben ze geen enkel houvast om risico's in te schatten en af te dekken. Daarom is het van belang dat cloudleveranciers openheid geven over de voorwaarden. Waar worden data opgeslagen en welke rechtsregels zijn daarop van toepassing? Hoe staat het met het beveiligingsniveau van data? En hoe zijn data nog bereikbaar als de cloudleverancier failliet gaat of het datacenter waar de cloudleverancier de data heeft neergezet, afbrandt?

De cloud niet gebruiken alleen om de kleine lettertjes zou zonde zijn. Maar bedrijven moeten wel beseffen dat ze niet zomaar even overstappen op de cloud. Een professionele aanpak is onmisbaar. Bij de keuze voor een nieuwe server bijvoorbeeld gaan bedrijven immers ook niet over één nacht ijs. Een belangrijke eerste stap is de cloudleverancier om inzage vragen in de voorwaarden. En daarbij vooral letten op de volgende zaken.Wat is functioneel programmeren eigenlijk en waarom wil je het, of waarom wil je het niet?

### Is er een Disaster Recovery Plan?

93 Procent van de bedrijven met een significant dataverlies is binnen vijf jaar failliet (Gartner). 90 Procent van alle bedrijven die te maken krijgen met een ramp zonder een Business Continuity Plan of Disaster Recovery Plan (DRP) achter de hand te hebben, gaat binnen 18 maanden failliet (PWC). Bij zo'n ramp valt te denken aan het defect raken van een server, per ongeluk verwijderen van cruciale data, vernietigen van het gebouw, een stroomstoring, een aanval van een hacker. Het is dus raadzaam om goed bij de cloudleverancier te checken wat hij geregeld heeft voor het geval zich een ramp voordoet. Waarbij bedrijven zich niet moeten laten afschepen met enkel een percentage dat weergeeft hoe snel de dienst weer in de lucht is na een eventuele calamiteit. Bedrijven doen er goed aan te vragen naar het datacenter- of uitwijkbeleid. Is er sprake van een active-active-uitwijk en nemen datacenters het real time van elkaar over? Of is er tijd nodig voordat het ene datacenter het van het andere kan overnemen? Hoeveel data gaan verloren en hoe is de recovery echt ingericht?

### Hoe is High availability georganiseerd?

High availability betekent dat klanten dankzij spiegeltechnieken (mirroring) kunnen rekenen op een zo hoog mogelijke beschikbaarheid. Als een component uitvalt, wordt het overgenomen door een andere machine. Cloudleveranciers geven meestal een percentage van de beschikbaarheid tijdens een bepaalde tijdspanne. Wat precies beschikbaar moet zijn en wat geteld wordt als onbeschikbaarheid, is vastgelegd in een Service Level Agreement (SLA). Stel: er is een SLA van 99,9 procent beschikbaarheid in de maand afgesproken, dan betekent dat, als er verder geen andere afspraken zijn gemaakt, dat er maximaal 0,1 procent van de tijd in de maand hinder mag zijn van ongeplande niet-beschikbaarheid. Bij 99,99 procent is dat 0,01 procent en bij 99,999 procent is dat 0,001 procent. En ga zo maar door. Maar interessanter dan zo'n percentage is de vraag hoe tolerant de omgeving is voor verstoringen. Belangrijk om te checken bij de cloudleverancier is dus wat er met data gebeurt als een server crasht.

### Welk recht is van toepassing op de data?

Vaak is in de voorwaarden van een cloudleverancier alleen terug te vinden waar de onderneming is gevestigd. Maar heeft een bedrijf bijvoorbeeld

gekozen voor een cloudleverancier in Lutjebroek, dan wil dat nog niet zeggen dat de data automatisch onder de Nederlandse wetgeving vallen. Bedrijven moeten zich dus goed laten voorlichten over de wetgeving, zodat zij weten welke garanties zij voor welke data kunnen afdwingen. Een bedrijf is en blijft zelf verantwoordelijk voor de compliance, dus moet het ook controleren of alle leveranciers voldoende garanties kunnen geven. Belangrijk dus om te checken welk recht van toepassing is op welke data, bij welke IaaS-provider de data staan, in welk land en onder welk recht de beheerders vallen. Dát data in een Amerikaanse cloud staan, hoeft geen probleem te zijn. Zolang het maar bekend is en het een bewuste keuze is. En natuurlijk moet dit passen bij het gevoerde compliancebeleid van de organisatie.

## Wat te doen bij faillissement?

Over de gevolgen van een faillissement van een cloudleverancier of van de IaaS-provider – waar hij zijn dienstverlening onderbrengt – is in de kleine lettertjes meestal niets terug te vinden. Voordat bedrijven met een cloudleverancier in zee gaan, is het belangrijk om dit wél te checken. Bij bedrijfskritische processen moet de continuïteit goed geregeld zijn – technisch en juridisch. Zolang er geen wettelijke regels zijn en er geen goede contractuele afspraken zijn gemaakt, zijn afnemers volledig afhankelijk van de curator. Bedrijven moeten beseffen dat dit gebied van cloudcomputing nog erg onvolwassen is. En dat er dus bijzonder kritisch gekeken moet worden naar dit stukje service. Goed advies over de juridische consequenties, inclusief verzekering tegen dataverlies, is dan ook onmisbaar.

## Hoe ziet het securitybeleid eruit?

Neem geen genoegen met een zinnetje in de voorwaarden zoals 'bij ons zijn je data veilig'. Maar zaag de cloudleverancier door over hoe dan wel. Vraag om bewijzen zoals:

- Hoe ziet jullie securitybeleid eruit?
- Stimuleren jullie de vindingrijkheid van medewerkers, met bijvoorbeeld hackersclubs?
- Hoe worden medewerkers gescreend?
- Hoe is de fysieke beveiliging van data geregeld?
- Hoe worden medewerkers getraind in security?
- Hoe zit het met audits en normeringen?

> "Neem geen genoegen met een zinnetje in de voorwaarden zoals 'bij ons zijn je data veilig'."

## Cloud-exitstrategie geregeld?

Net als elke dienst, kan ook een clouddienst opgezegd worden. Dat betekent dat een cloudleverancier de data terug moet geven aan de rechtmatige eigenaar. Check van tevoren dus goed hoe de rollen en verantwoordelijkheden beschreven zijn bij het opzeggen en welke ondersteuning de cloudleverancier daarbij geeft. Wat staat er bijvoorbeeld beschreven over hoe, wanneer en in welke vorm de data teruggegeven worden? Volwassen cloudleveranciers bieden bijvoorbeeld API's, waarmee hun klanten data zelf eenvoudig kunnen benaderen, migreren of synchroniseren met on-premise-systemen of met andere clouddiensten. Voor klanten betekent dat dat ze minder afhankelijk zijn van een cloudprovider en ze eenvoudig van cloud naar cloud kunnen overstappen.

## Hoe waarborgt de cloudleverancier de privacy?

Bedrijven die in zee gaan met een cloudleverancier, blijven natuurlijk zelf eindverantwoordelijk voor de naleving van de Wet Bescherming Persoonsgegevens (Wbp). Des te belangrijker om goed na te gaan hoe een cloudleverancier omgaat met de privacy. Uit onderzoek blijkt dat 74 procent van de cloudleveranciers niet geschikt is voor Europese bedrijven om data op te slaan. Ze voldoen niet aan de Europese privacyrichtlijn. Volgens deze richtlijn is het verboden persoonsgegevens te exporteren naar een land buiten de Europese Unie als dat land een ontoereikend beschermingsniveau biedt, bijvoorbeeld de Verenigde Staten. Om transport van persoonsgegevens naar de VS toch mogelijk te maken heeft het Amerikaanse Departement van Handel in overleg met de Europese Commissie het Safe Harbor Framework opgericht. Amerikaanse organisaties die zich bij dit framework hebben aangesloten, worden gezien als organisaties die voldoen aan de Europese beveiligingsstandaard. Maar dat is onvoldoende. Bedrijven die een clouddienst afnemen bij zo'n partij, moeten goed checken of de partij zich er ook aan houdt, en of de andere voorwaarden van de Wbp worden gerespecteerd.

## Warboel van verantwoordelijkheden?

Afnemers – die steeds vaker niet meer van een ICT-afdeling komen, maar vanuit allerlei organisatieonderdelen en afdelingen – moeten zich bewust worden van de warboel aan dienstverleners achter hun cloudoplossing. Zo maken SaaS-leveranciers vaak gebruik van één of zelfs meer IaaS- en/of PaaS-leveranciers om hun clouddienst aan te bieden. Er ontstaat een keten van verantwoordelijkheden die impact heeft op de clouddienst. Als de SaaS-provider failliet gaat, hoe zit het dan met de rechten van de klant ten opzichte van de achterliggende leveranciers? En matcht het privacybeleid van de achterliggende leveranciers wel met de privacyeisen die de klant stelt aan zijn in de cloud geplaatste data? Kortom: een correcte, juridisch dichtgetimmerde, inrichting van het IaaS-platform door de SaaS-provider zou topprioriteit moeten hebben. En de afnemer mag daar veeleisend in zijn. Het gaat immers om zijn data.