

*Cloud computing vraagt om nieuwe,  
passende beveiligingsmaatregelen*

# Security

in de cloud, geen sinecure

---

Cloud computing is sterk in opkomst voor het vervangen of uitbesteden van de ict-infrastructuur. Het maakt de ict-dienstverlening flexibel en schaalbaar, en vaste kosten variabel. Het verhoogt bovendien het niveau van beheer en beschikbaarheid. Voor beveiliging biedt cloud computing echter geen automatische garanties. Dat vraagt om nieuwe maatregelen. Het Cloud Cube-model van het Jericho Forum biedt daarvoor een goede leidraad.

**DOOR CORNE DE KEIZER** CISSP, CISA EN **BART VERHAAR**, SECURITYCONSULTANTS BIJ MOTIV, EN IR **BASTIAAN BAKKER**, BUSINESS-DEVELOPMENTMANAGER BIJ MOTIV

Het zogenoemde cloud computing is het architectuurmodel voor internetgebaseerd computergebruik. De cloud (wolk) is daarbij een metafoor voor het open en ontastbare internet. In de cloud zijn vooral 'software as a service' (SaaS-) en 'security as a service' (SecAas-)providers actief, die applicaties en diensten overnemen van bedrijven.

Een goed voorbeeld van een dienst die bij uitstek geschikt is voor uitbesteding is een e-maildienst. De voordelen hiervan zijn evident: meer beheersgemak door transparantie en flexibiliteit, garanties voor beschikbaarheid en de belofte van kostenbesparing. Bovendien is het

relatief eenvoudig om (delen van) een e-maildienst te migreren naar de cloud.

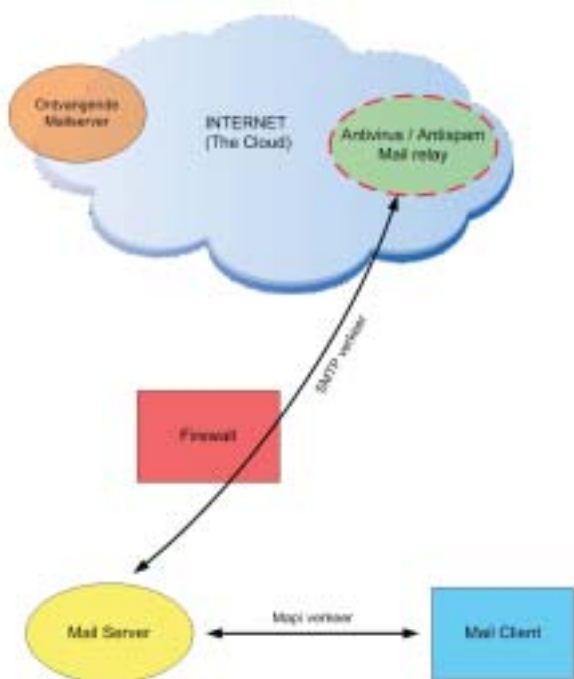
De overstap van een traditionele, intern beheerde ict-omgeving naar cloud computing kan op verschillende manieren gemaakt worden. Het Cloud Cube-model van het Jericho Forum brengt deze helder in kaart. Het maakt ook de risico's inzichtelijk die hieraan verbonden zijn. Het forum geeft bovendien suggesties voor de extra beveiligingsmaatregelen die getroffen kunnen worden. In de volgende drie varianten worden de mogelijkheden voor de migratie van een e-maildienst naar de cloud toegelicht.

## **VARIANT 1 - Security via de cloud**

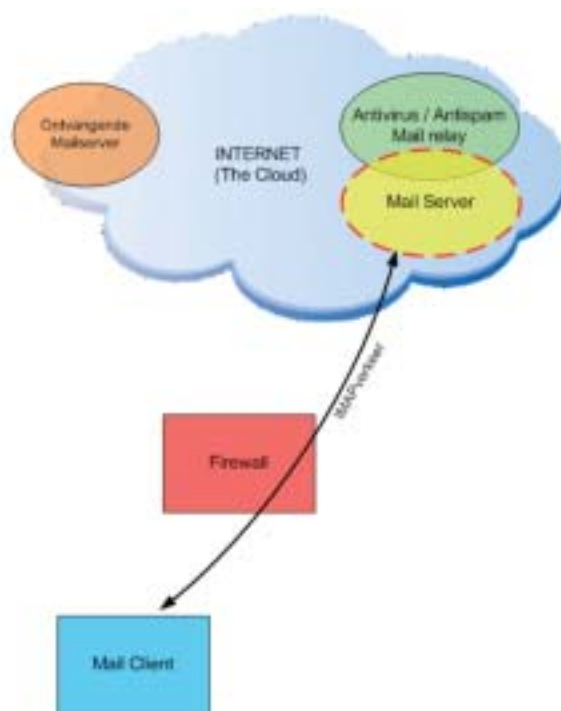
Een veelvoorkomende functie die overgezet wordt naar de cloud, is het uitbesteden van de mail-relayservices. In plaats van zelf security appliances voor e-mailbeveiliging in de DMZ (demilitarized zone) te plaatsen, wordt dit als dienst afgenomen via een SecAas-provider (zie figuur 1).

In variant 1 is de mail-relayservice verplaatst van een interne dienst naar een externe beveiligingsdienst. Het voordeel hiervan is dat de SecAas-provider een hoge beschikbaarheid kan waarborgen, altijd up-to-date virusscanners heeft en innovatieve reputatiefilters gebruikt voor spamfiltering. Bovendien wordt deze dienst geleverd tegen een vaste prijs per gebruiker. Deze variant wordt in het Cloud Cube-model van Jericho Outsourced Per(EO) genoemd (zie kader).

Beveiliging is relatief eenvoudig uit te besteden. Helemaal risicovrij is het echter niet. Zo is het transport van e-mailberichten tussen de SecAas-provider en het interne netwerk niet meer controleerbaar. In theorie betekent dit dat hackers nieuwe kwaadaardige code toe kunnen voegen (een zogenoemde 'man in the middle'-aanval). Het is geen groot risico, maar creëert wel een nieuwe kwetsbaarheid die in een traditionele omgeving niet bestaat. Een goede oplossing daarvoor zijn nieuwe technieken, zoals data loss prevention (DLP).



Figuur 1: E-mailbeveiliging via een SecAas-aanbieder



Figuur 2: E-mail volledig via de cloud

Dat vraagt echter wel om maatwerk per klantomgeving. Een DLP-oplossing treft verschillende beveiligingsmaatregelen binnen een complete ict-infrastructuur, inclusief e-mailbeveiliging.

### VARIANT 2 - Hosted e-mail via de cloud

De tweede variant gaat een stap verder dan de eerste. In deze variant wordt de volledige serveromgeving voor e-mail uitbesteed aan een SaaS-provider. Daar maken ook de beveiligingsmaatregelen, zoals virus- en spamfilters, deel van uit. Alleen de e-mailclients zijn nog lokaal geïnstalleerd, wat vaak wenselijk is omdat gebruikers dan ook offline kunnen blijven werken (zie figuur 2). Deze variant wordt in het Cloud Cube-model van Jericho Outsourced D-p(EO) genoemd (zie kader en figuur 2).

Door de mail-relayservices en de mail-servers te verhuizen ontstaan er veel nieuwe risico's. Zo worden de eisen voor identificatie van de gebruiker cruciaal. Alleen sterke authenticatie voorkomt dat de e-mailbox van een gebruiker kan worden overgenomen door password guessing of password cracking. Sterke authenticatie is daarom een kritische voorwaarde voor de migratie naar de cloud. Het is ook essentieel dat de ge-

## 'Beveiliging is relatief eenvoudig uit te besteden, maar helemaal risicoloos is het niet'

bruikersadministratie op twee plaatsen wordt bijgehouden. Ten eerste moet dit gebeuren op het interne netwerk, ten tweede bij de SaaS-provider. Daarnaast is de beveiliging van het IMAP-protocol, het standaardprotocol tussen de e-mailclient en -server, vaak complex. Net als het geval is bij variant 1, is ook voor variant 2 de keuze van de partner aan wie de diensten worden uitbesteed, erg belangrijk. Het is altijd een goed advies om kennis te nemen van de exacte beveiligingsmaatregelen en te controleren of de SaaS-provider beschikt over een ISO 27001-certificering.

### VARIANT 3: Cloud computing pur sang

De derde variant is de overstap naar pure cloud computing. Dit betekent dat de volledige functionaliteit via internet te benaderen is via een standaardwebbrowser en open protocollen. In deze variant levert de SaaS-provider de mail-relayservices, de e-mailservices en een webinterface. Het is weliswaar niet langer noodzakelijk om een lokale e-mailcli-

ent te gebruiken, maar wel aan te raden om offline werken mogelijk te houden. In deze variant loggen gebruikers in via een pc met internetverbinding en webbrowser. Deze variant wordt in het Cloud Cube-model van Jericho Outsourced D-



Figuur 3: E-mail volledig via de cloud

p(EO) genoemd (zie kader).

Deze variant brengt ook nieuwe risico's met zich mee, want de eindgebruiker moet altijd online zijn. Ook bij tele- of thuiswerken is een optimaal beveiligde verbinding noodzakelijk. Sterke authenticatie van gebruikers is daarom ook in deze variant essentieel. De SaaS-provider moet niet alleen voldoen aan de huidige beveiligingseisen, maar ook aan toekomstige. Wanneer wet- en re-

gelgeving bijvoorbeeld nieuwe bewaartermijnen voor e-mail voorschrijft, moet de SaaS-provider daar snel op kunnen inspelen. Dat vraagt om een groot vertrouwen in de SaaS-provider. Als dat er echter is, resulteert dat in een mooie, innovatieve oplossing.

## SAMENVATTING

Het Cloud Cube-model is een praktische leidraad voor de besluitvorming

rond de strategie en toepassing van cloud computing. Daarbij worden zowel technische als organisatorische aspecten overwogen, op een hoog abstractieniveau. Met behulp van een ingevuld model is in een oogopslag te zien welke basiskeuzes er zijn voor flexibiliteit en verantwoordelijkheid bij het opzetten van de clouddienst. 

## Het Cloud Cube-model van het Jericho Forum

Het Jericho Forum is onderdeel van The Open Group, een consortium met een ideële visie op toegang tot informatie op basis van open standaarden. Het Jericho Forum onderzoekt en adviseert over richtlijnen voor ict-beveiliging in een open netwerkgeving. Cloud computing, en de implementatie en consequenties daarvan, behoort ook tot het gedachtegoed van het Jericho Forum. Dit heeft geresulteerd in het Cloud Cube-model, dat in meerdere dimensies de verschillende verschijningsvormen van cloud computing weergeeft. Deze worden door het forum cloud formaties genoemd.

Het Cloud Cube-model wordt weergegeven in de vorm van een kubus en kent in totaal vier dimensies. Iedere dimensie heeft twee mogelijkheden, waardoor het model goed leesbaar en toepasbaar is. De eerste drie dimensies zijn terug te vinden op de assen van de kubus. Dit zijn de dimensies internal versus external (intern of extern geplaatst), proprietary versus open (gesloten of open licenties) en perimeterised versus de-perimeterised (begrensde of onbegrensde toegang). Omdat een kubus slechts drie dimensies kent, heeft het Jericho Forum

ervoor gekozen de vierde dimensie, insourced versus outsourced (intern beheerd of uitbesteed) met kleuren weer te geven.

Om de dimensies te benoemen en te bepalen waar een clouddienst zich bevindt, wordt het model van links naar rechts gelezen. Een clouddienst is daarvoor:

- intern (I) of extern (E), én
- proprietary (P) of open (O), én
- perimeterised (Per) of de-perimeterised (D-p), én
- insourced of outsourced.

Iedere dimensie beantwoordt specifieke vragen en wordt hieronder toegelicht.

### Dimensie internal (I) versus external (E)

De primaire vraag bij deze dimensie is: waar bevindt de data zich fysiek? De dimensie is internal wanneer de data zich binnen de fysieke grenzen van de organisatie bevindt. In alle andere gevallen is de dimensie external.

### Dimensie proprietary (P) versus open (O)

De P/O-dimensie geeft antwoord op de vraag: wie is eigenaar van de toegepaste technologie, services, interfaces, et cetera? Dit geeft inzicht in de mate van flexibiliteit van de gekozen clouddienst en de uitwisselbaarheid met andere (cloud)diensten. Het geeft ook een indicatie over mogelijke beperkingen bij het uitwisselen en delen van applicaties en data.

### Dimensie perimeterised (Per) versus de-perimeterised (D-p)

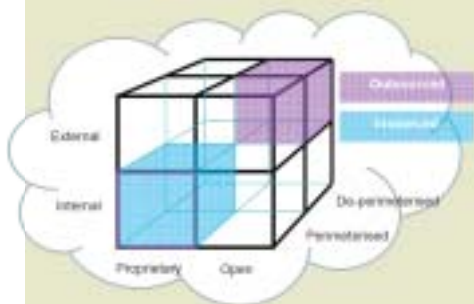
Wat is de 'architectural mindset' bij het ontwerp van de dienst? Deze vraag

wordt beantwoord in de dimensie Per/D-p. Wordt er gewerkt binnen de traditionele IT-perimeter, of daarbuiten? De traditionele IT-perimeter is een netwerk dat afgedekt is met firewalls, en beperkt een organisatie in het zakendoen en samenwerken met andere organisaties. De-perimeterisation is een onderwerp dat door het Jericho Forum veelvuldig besproken wordt. Het gedachtegoed van het Jericho Forum is gebaseerd op elf richtlijnen voor informatiebeveiliging. Deze elf beginselen gaan uitgebreid in op het onderwerp De-perimeterisation.

In het Cloud Cube-model kan gewerkt worden in vier verschillende cloud formaties (I/P,I/O,E/P,E/O), in combinatie met een van de architectural mindsets (Perimeterised of De-perimeterised). Volgens het Jericho Forum is de optimale combinatie te vinden in een E/O/D-p omgeving.

### Dimensie insourced versus outsourced

Tot nu toe zijn er acht mogelijke cloud formaties gedefinieerd: Per(IP,IO,EP,EO) en D-p(IP,IO,EP,EO). Het forum voegt hier een vierde dimensie aan toe. Deze dimensie beantwoordt de vraag: Wie is verantwoordelijk voor het draaien van de clouds? Op het moment dat de dienst wordt geleverd door een derde partij is de dimensie 'outsourced'. Als de verantwoordelijkheid voor de dienst ligt bij de interne ict-afdeling is de dimensie 'insourced'. Het draait primair om wie er verantwoordelijk is voor het leveren van de dienst. Dit is voornamelijk een organisatorisch, niet een technisch besluit.



Figuur 4: Het Cloud Cube-model van het Jericho Forum