

Geen angst maar inzicht:

Beveiliging van de cloud

Het lijkt erop dat de complete IT-wereld enthousiast is over de cloud. Duidelijk is wel dat cloud computing de bedrijfs-IT positief kan veranderen. De cloud bevrijdt een organisatie van de verantwoordelijkheid van het directe beheer van (grote gedeeltes van) de IT-infrastructuur. Tegelijkertijd profiteren bedrijven van verbeterde efficiëntie en flexibiliteit door de IT-infrastructuur te verplaatsen naar een gedeelde resource. Toch staan we slechts aan het begin van een brede inzet van cloud computing. De reden? Twijfels over de geschiktheid van de cloud voor het veilig opslaan van gevoelige data.

DOOR GARETH WILLIAMS, CEO VAN INTERROUTE

Er is veel aandacht voor de vrijheid die de cloud biedt. Het is daarom niet vreemd dat velen denken dat er geen fysieke apparatuur nodig is voor cloud



computing. Het beeld bestaat dat alles zich bevindt in een vrij toegankelijke internetomgeving. Zo bezien is het dan ook logisch dat er grote twijfels bestaan over de geschiktheid van de cloud voor het veilig opslaan van gevoelige en vertrouwelijke data. Zelfs met SaaS en IaaS moeten de software, applicaties en fysieke infrastructuur ergens staan. Ook toegang tot data vereist een fysiek leveringsplatform. Deze componenten bepalen hoe veilig de cloud echt is.

ONNODIGE RISICO'S

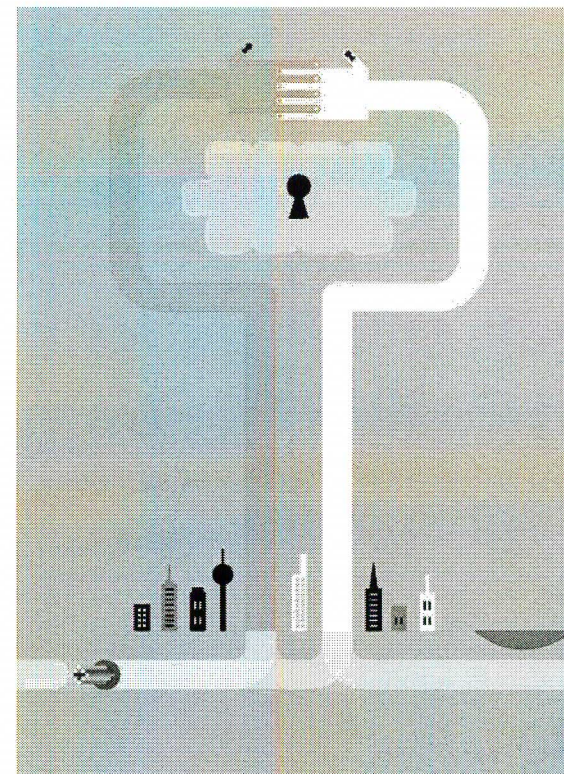
Drie van de vier bedrijven denkt dat de cloud onveilig is. Ze zien cloudbeveiliging dan ook als hun grootste uitdaging. Toegegeven: het delen van resources vanuit een grote hoeveelheid, niet-gedifferentieerde servers en switches brengt risico's met zich mee. Toch doen bedrijven er goed aan zich eerst te richten op de verbinding met de cloud. Iedere cloud die gebruikmaakt van het

publieke internet stelt data bloot aan onnodige risico's. CIO's en CTO's hebben dan ook gelijk als ze voorzichtig zijn voor clouds met zeer onvoorspelbare internettoegang die niet wordt ondersteund door SLAs.

De private cloud vormt een alternatief voor de publieke cloud. Deze is gescheiden van het publieke internet en biedt hetzelfde beschermingsniveau als private netwerken, maar de flexibiliteit van een internettoegangsmodel. Sommigen vragen zich af of de private cloud eigenlijk wel cloud genoemd mag worden vanwege het feit dat er geen gebruik wordt gemaakt van vrij toegankelijke, gedeelde resources. Dat is niet helemaal terecht, want ook dit model gebruikt resources in een pool en levert on-demand diensten. Door een gedeelte van een IP-netwerk te isoleren en veilig te scheiden van het internet, kunnen bedrijven profiteren van gegarandeerde beschikbaarheid en prestaties van hun computing resources. Een sterk verbeterde veiligheid met de flexibiliteit van de publieke cloud zijn dan ook de grootste voordelen van private clouds. Veel bedrijven creëren deze vanuit hun eigen infrastructuur die zij goed (laten) beheren en beveiligen. In het geval dat databeveiliging niet alleen belangrijk maar ook cruciaal is, is de private cloud dan ook de beste optie.

BEVEILIGING: TERUG NAAR DE BASIS

Het lijkt een eenvoudige vergelijking, maar voor data in de cloud geldt hetzelfde als voor andere data: slecht beheer resulteert in slechtere beveiliging. De cloud op zich vergroot de kwetsbaarheid van data niet. Beveiliging blijft afhankelijk van de manier waarop een bedrijf de toegang tot data controleert. In tegenstelling tot het publieke inter-



Door beveiligingsangsten blijven bedrijven twijfelen aan de cloud

net zouden beveiligingsmaatregelen als DDoS-bescherming, firewalls en inbraakdetectietechnologieën en inbraakpreventietechnologieën standaard moeten zijn in private clouds. Er zijn tools om te monitoren of de nieuwste beveiligingsmaatregelen zijn toegepast. Door data te classificeren en vervolgens de juiste beschermingslagen aan te brengen, zorgen bedrijven ervoor dat hun data is beschermd.

ZELF BOUWEN OF AANSCHAFFEN?

Het feit dat private clouds zijn gebouwd op een dedicated infrastructuur om zo een beter beheer en beveiliging te garanderen, zorgt ervoor dat dit de duurdere optie is. Het vereist investeringen om de infrastructuur aan te schaffen en een datacenter om te bouwen tot een

private cloud. Dit geldt ook voor de centralisatie van computer- en storage-systemen. Verder geldt dat deze clouds over het algemeen niet de voordelen van cloud computing bieden: open toegang voor eindgebruikers, en de efficiëntie en de mogelijkheid om snel data en resources te distribueren via een 'eigen privé-internet'. Om over deze mogelijkheden te beschikken, is het zaak een leverancier te zoeken die de benodigde privacy biedt, maar ook de flexibiliteit van internetoplossingen. Door gebruik te maken van een privaat IP-netwerk van een leverancier is via het netwerk toegang tot gedeelde bedrijfsresources mogelijk en is data toch veilig afgescheiden van het internet. Private clouds die op deze manier – dus als een service – zijn opgezet, bieden een veilige, gecontroleerde cloudomgeving met een gegarandeerd

hogere beschikbaarheid, betere disaster-recovery-mogelijkheden en flexibele en schaalbare capaciteit. Bovendien zijn bedrijven beter beschermd dan met een zelfgebouwde private cloud en profiteren ze toch van de flexibiliteit van een internetmodel.

HYBRIDE CLOUD

De hybride cloud bevindt zich tussen de publieke en private cloud en de traditionele manier van IT-beheer in. De hybride cloud is een optie als een bedrijf recent heeft geïnvesteerd in de fysieke infrastructuur of als een applicatie niet geschikt is voor de cloud. Met een hybride cloud is het mogelijk om bepaalde data in de private of publieke cloud op te slaan. Dit is een veelvoorkomende situatie, aangezien veel bedrijven overstappen van het traditionele kosten- en arbeidsintensieve model van ict-infrastructuurbeheer naar de flexibelere, kosteneffectievere en directe leveringsmogelijkheden van de cloud.

Clouddiensten zijn nog volop in ontwikkeling. Tot het moment dat de verwarring en de beveiligingsangsten zijn verdwenen, zullen er bedrijven zijn die twijfelen aan de cloud. Toch zijn de voordelen – flexibiliteit, betalen voor gebruik en betere prestaties – niet te negeren. Welke organisatie staat niet voor de uitdaging om de IT-infrastructuur te migreren, te veranderen en opnieuw in te delen om te voldoen aan veranderende zakelijke behoeften? Zou er een CIO zijn die geen interesse heeft in de mogelijkheid om IT-kosten schaalbaar af te stemmen op volume en gebruik? Ook de centralisatie van fysieke technologie en het vergroten van de efficiëntie door onderhoud en ondersteuning uit te besteden, lijkt logisch. Bedrijven moeten niet alleen beveiligingsniveaus in stand houden, maar juist verbeteren. Ook het verbeteren van de interne en externe toegang en transparantie staan hoog op de agenda. Managers realiseren zich al lang dat de productiviteit toeneemt wanneer medewerkers overal toegang hebben tot informatie. Tot nog toe moesten ze echter kiezen tussen beveiliging en efficiëntie. Het geheim om hier niet tussen te hoeven kiezen, is inzicht in hoe de cloud wordt benaderd. Dan is het mogelijk om voor de hele organisatie of binnen de ondersteunde divisies of applicaties het cloud-leveringsplatform te kiezen dat past bij de beveiligingsseisen. 