Overzicht over data in de cloud ontbreekt bij veel organisaties

Leuk, alles bij elkaar opslaan in de cloud, zodat je er altijd en overal bij kan. Toch blijkt het moeilijker dan het lijkt. Veel bedrijven worstelen met het beheer van hun data, die die over een groot aantal services en applicaties zijn verdeeld.

Nieuw onderzoek van Kaspersky Lab, onder andere uitgevoerd in Nederland en België, laat zien dat 35 procent van de bedrijven erkent niet zeker te weten of bepaalde data op hun eigen servers staan of op die van hun cloudproviders. Dit maakt het beveiligen en verantwoorden van data erg moeilijk, brengt de integriteit ervan in gevaar en kan tot ernstige beveiligingsproblemen en hoge kosten leiden.

Cloud computing

Cloudservices bieden bedrijven de mogelijkheid om de meest geavanceerde technologieën te gebruiken ter ondersteuning van hun dagelijkse activiteiten en hun groeiplannen, zónder het hoofd te hoeven breken over onderhoud en kosten. Het is dan ook geen verrassing dat 78 procent van de bedrijven al ten minste één Software-as-a-Service-platform (SaaS) heeft geïmplementeerd. Daarnaast is 75 procent van plan om in de toekomst meer applicaties naar de cloud te verhuizen. Als het gaat om IaaS, is bijna de helft van de grotere ondernemingen (49 procent) en 45 procent van het MKB van plan om de IT-infrastructuur en -processen uit te besteden.

Geen duidelijk plan

Met de verlokkingen van kosten- en andere besparingen is echter voor veel ondernemingen de snelheid waarmee clouddiensten ingevoerd zijn ten koste gegaan van de veiligheid, omdat er voorbij is gegaan aan databeveiligingsstrategieën. Vaak is het onduidelijk wie er nu precies verantwoordelijk is voor de beveiliging van clouddata. Ons onderzoek toont aan dat 70 procent van de bedrijven die SaaS- en cloudserviceproviders gebruiken geen duidelijk plan heeft voor de aanpak van beveiligingsincidenten die hun partners kunnen raken. Een kwart geeft toe de compliance-richtlijnen van de serviceprovider niet eens te hebben gelezen, wat suggereert dat

ze ervan uitgaan dat de provider het wel oplost als er iets misgaat.

De volledige verantwoordelijkheid voor de beveiliging bij de provider leggen, kan echter een riskante strategie zijn. 42 procent van de bedrijven voelt zich niet voldoende beschermd tegen incidenten die met hun cloudserviceprovider te maken hebben, en 24 procent is het afgelopen jaar geconfronteerd met een incident dat invloed heeft gehad op de door een externe partij gehoste IT-infrastructuur.

Beveiliging

Dit gebrek aan planning en verantwoordelijkheid kan ernstige gevolgen hebben: de gemiddelde financiële impact van een beveiligingsincident in de cloud bedraagt 100 duizend dollar (zo'n 85 duizend euro) voor een MKB-onderneming en 1,2 miljoen dollar (zo'n 1 miljoen euro) voor een groter bedrijf. Als gevolg van incidenten waarbij een externe partij was betrokken, zijn vooral de volgende soorten data aangetast: hoogst gevoelige klantinformatie (ervaren door 49 procent van de MKB's en 40 procent van de grotere ondernemingen); elementaire werknemersinformatie (35 procent van het MKB, 36 procent van grotere ondernemingen); en e-mails en interne communicatie (31 procent van het MKB, 35 procent van grotere ondernemingen).

Wildgroei in de cloud

Daarom moeten bedrijven manieren vinden om de wildgroei in de cloud onder controle te krijgen. Ieder datapakket moet optimaal worden beschermd, waar het zich ook bevindt. Om dit voor elkaar te krijgen, moet iedere afwijking binnen de cloudinfrastructuur van de onderneming worden opgespoord. Dat kan alleen worden bereikt door een combinatie van technieken als machine learning en gedragsanalyse. Dit vermogen om onbekende dreigingen te identificeren en zich ertegen te wapenen is essentieel voor de beveiliging van de cloudinfrastructuur.

Daarnaast zorgt zichtbaarheid van het cloud-ecosysteem en de cyberbeveiligingslaag ervoor dat bedrijven duidelijk in beeld hebben waar alle data zich bevinden en of de huidige beveiligingsstatus voldoet aan het beveiligingsbeleid van het bedrijf. Alleen op deze manier kan de cloud volledig in de hand worden gehouden, ongeacht de hoeveelheid en de locatie van de data.