WWW.MINDYOURSTEP.INFO

Werken in de Cloud

is het eigenlijk wel zo veilig?

De vraag

De term ‘werken in de Cloud’ zien we tegenwoordig vaak voorbij komen. Maar wat betekent dat? Cloud Computing is het (veelal) via het internet op aanvraag gebruik kunnen maken van hardware, software en gegevens via een derde partij. Het zorgt ervoor dat de gewenste dienstverlening of gegevens plaats-onafhankelijk, snel en gemakkelijk beschikbaar zijn. De term ‘Cloud’ ofwel ‘Wolk’ is eigenlijk een beetje misleidend. Uiteraard hangen je gegevens niet zomaar ‘ergens’ in de lucht, maar worden ze opgeslagen op een Cloudserver. Hoe veilig is ‘werken in de Cloud’ eigenlijk?

De uitdaging

De Cloud heeft veel voordelen. Eén daarvan is dat je als organisatie de ICT-infrastructuur kunt verschuiven naar ‘huren op maat’. Er zijn dus geen grote investeringen in eigen servers, onderhoud en bemensing nodig en je betaalt naar gebruik. Daarnaast is het mogelijk om gegevens te delen met andere (interne) gebruikers. Werken in de Cloud is daarom een handig hulpmiddel om samen te werken. Hier is bijvoorbeeld bij overheden veel vraag naar. Zij werken veelvuldig in ketens samen met publieke en private partijen. Tot slot willen we steeds meer en meer tijd- en plaats-onafhankelijk werken. Bij Cloud Computing kun je eenvoudig, snel en flexibel gebruik maken van ICT-diensten en is je data altijd beschikbaar.

Ondanks de voordelen zijn veel mensen nog terughoudend als het gaat om werken in de Cloud. Ze zijn bang dat hun gegevens voor het oprapen liggen voor internetcriminelen. Toch doen we het privé bijna allemaal al; zo zetten we bijvoorbeeld onze vakantiefoto’s op Google Drive, maken we een back-up van ons financieel overzicht op Dropbox en bewaren we een kopie van ons paspoort op de Apple iCloud Drive.

De oplossing

De voordelen van de Cloud zijn duidelijk en kwantificeerbaar in tijd en geld, de risico’s zijn echter veelal kwalitatief van aard en minder zichtbaar. Om veilig te kunnen werken in de Cloud is het dus belangrijk om je goed voor te bereiden en in ieder geval rekening te houden met de volgende zaken:

- De Cloud bestaat in verschillende varianten; de publieke-, private-, community- en hybride Cloud. Iedere vorm heeft zijn eigen kenmerken en daarbij horende voor- en nadelen. Door je te verdiepen in de verschillende vormen kun je bewust een keuze maken voor een oplossing die het beste past bij de structuur van je organisatie en de gegevens die je wilt opslaan.
- De goedkoopste vorm is de publieke Cloud. Je weet dan niet altijd waar de gebruikte hardware zich bevind, de servers kunnen dus ook in het buitenland gestationeerd zijn en de gegevens kunnen vrij stromen tussen verschillende landen. Lokale (privacy)wetgeving kan bijvoorbeeld invloed hebben op de privacy van je gegevens. Duidelijke afspraken met de leverancier zijn dus gewenst als je data privacygevoelige informatie bevat! Dit kan bijvoorbeeld door middel van een verwerkersovereenkomst of een Service Level Agreement.
- De ene leverancier is de andere niet. Als je eenmaal gekozen hebt voor een vorm van Cloud dienstverlening, heb je vervolgens de keuze uit verschillende leveranciers. ‘Welk beleid voert de leverancier en aan welke officiële informatie-beveiligingsnormen voldoet de partij?’ Vragen die je jezelf kunt stellen alvorens een keuze te maken.
- Bekijk voordat je gaat werken in de Cloud welke data privacy- of organisatiegevoelige informatie bevat en welke niet. Rangschik je data (dataclassificatie) en bepaal of en onder welke condities de gegevens veilig staan in de Cloud. Gebruik die kennis vervolgens om je Cloud optimaal in te richten en structuur aan te brengen.
- Leg in de afspraken met de leverancier vast wie eigenaar is en blijft van de gegevens. Door de controle en zeggenschap af te kaderen voorkom je dat de gegevens zonder toestemming gebruikt worden door de Cloud-leverancier.
- Tot slot, weten jij en je collega’s welke mogelijkheden de Cloud precies biedt? En wat daar de voordelen, maar ook de risico’s van zijn? Als je alles uit de Cloud wilt halen is het raadzaam om een webinar of training te organiseren, via de leverancier of een andere externe partij. Zo is iedereen up-to-date en goed voorbereid op veilig werken in de Cloud!

Kortom; zorg dat je op de hoogte blijft van nieuwe wetgeving en technologische ontwikkelingen. Verdieping, aandacht en een set goede afspraken met de leverancier en ook binnen je eigen organisatie zorgen ervoor dat de risico’s niet de boventoon gaan voeren.

Meer weten?

Bezoek onze website www.mindyourstep.info voor meer tips en tricks op privacy- en informatieveiligheidsvlak.
Of neem direct contact op met Marijn Berndes via marijn@soulmade.nl of door te bellen naar 0162-430345.