Essay: SaaS of Soeverein

Auteur: Arend Jan Wiersma

Datum: augustus 2023

Op verzoek van het Bureau Forum voor Standaardisatie (BFS) heeft de auteur een essay geschreven over de Cloud. Dit naar aanleiding van de door BFS en anderen geconstateerde ontwikkeling dat overheidsorganisaties steeds meer ICT-systeem inkopen die als SaaS worden aangeboden. De Cloud is ook een van de thema's die in de ICTU Monitor Open Standaarden 2023 aan de orde komen.

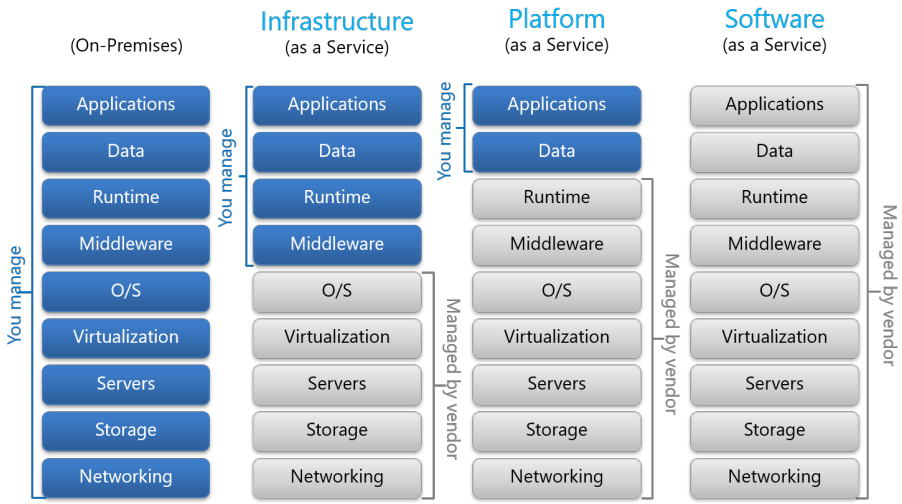
Soms geeft de jaarlijkse Open Standaarden Monitor, naast inzage in het gebruik van open standaarden, nog andere interessante inzichten. Een voorbeeld daarvan die we in dit stuk kort gaan uitlichten is de snelle toename van SaaS (Software-as-a-Service) aanbestedingen die we de afgelopen jaren voorbij hebben zien komen. Vrijwel alle soorten software worden anno 2023 aangeschaft in de vorm van SaaS. De redenen hiervoor lijken duidelijk: over het algemeen geeft SaaS meer gebruiksgemak, eenvoudiger management en lagere kosten. Toch worden er, zeker voor de overheid, misschien ook kritieke concessies gedaan die pas zichtbaar worden op een langere tijdslijn. Hieronder een weging van de voor- en nadelen als relativering van de ogenschijnlijk oneindige lijst met voordelen die momenteel SaaS tot standaardkeuze voor software maakt.

Wat is SaaS?

SaaS, ook wel de cloud of clouddiensten genoemd, is een vorm van on-demand software. Het kenmerkt zich door gebruik van een browser en inloggegevens om toegang te krijgen tot software die ergens op een server op het internet draait. Veelgebruikte SaaS-diensten binnen de overheid en het bedrijfsleven zijn Microsoft Office 365 en Google Workspace. Andere voorbeelden zijn internetbankieren, social media en webwinkels.

Inmiddels is SaaS volledig ingeburgerd en gebruiken we deze vorm van software dagelijks. Toch is dit een relatief nieuwe vorm softwarelevering. Slechts 10-15 jaar geleden werd software voornamelijk geleverd door middel van installatie op de computer van de gebruiker. De programmacode draaide uitsluitend op het apparaat van de gebruiker en was beperkt tot de informatiebronnen die op diezelfde computer aanwezig waren. Met de uitrol van het internet werd deze software geavanceerder en kon het ook externe informatiebronnen gaan raadplegen. Inmiddels is de kwaliteit van het internet zodanig hoog dat we software op afstand kunnen gebruiken zonder deze lokaal te hoeven installeren. Dit levert enorme winst op in kostenefficiëntie en gebruiksgemak. Het is dan ook geen verrassing dat aanbestedingen anno 2023 meer dan 90% de vraag om SaaS betreft.

Figuur 1. Illustratie van de verschuiving van verantwoordelijkheden bij het gebruik van SaaS



Voordelen

De kracht van SaaS komt voort uit het overdragen van een grote mate van verantwoordelijkheid naar de leverancier, zie Figuur 1. De leverancier dient er voor te zorgen dat de dienst draait en toegankelijk is. De afnemer hoeft enkel een computer met internet en een browser te verzorgen en kan aan de slag. Dit was pre-SaaS niet het geval. Organisaties moesten zelf zorgen voor het aanschaffen, distribueren, installeren, updaten, ondersteunen en beveiligen van de software. Dit veelal op individuele computers en eigen server-hardware op de locatie van gebruik of later een datacenter (on-premises hosting is voor sommige bedrijven en ministeries nog steeds relevant, maar de trend wijst duidelijk in de richting van uitbesteding.) Enkele algemene voordelen van SaaS zijn:

- lagere kosten;
- minder onderhoud;
- snellere updates;
- meer mogelijkheden om te koppelen met andere systemen;
- eenvoudiger en beter te controleren toegangsmanagement;
- betere aansluiting bij de verwachtingen en vaardigheden van de eindgebruiker.

Voor IT-afdelingen is SaaS over het algemeen heel prettig. Hele organisaties zijn op deze manier te managen met een centraal configuratie paneel en storingen kunnen doorgezet worden naar de leverancier.

Nadelen

Vrijwel alle positieve aspecten die SaaS zo aantrekkelijk maken hebben een tegenhanger die niet genegeerd moeten worden. Vrijwel alle nadelen komen voort uit datgene dat ook de voordelen creëert, namelijk: alle data bevind zich op een computer van een derde en deze heeft volledige controle over de beschikbaarheid, integriteit en vertrouwelijkheid daarvan. Dit zijn de drie kernaspecten van informatiebeveiliging. Voor een Mkb'er is dit niet zo relevant, maar met het recente besluit van de overheid om gebruik van commerciële clouddiensten voor de Rijksoverheid mogelijk te maken wordt het een nationale aangelegenheid en staat er plotseling veel meer op het spel. Dit zal niet direct vandaag of morgen aan de orde zijn, maar het is duidelijk dat er een nieuwe koers is ingezet en het valt daarom te verwachten dat in de komende jaren steeds meer aspecten van de digitale infrastructuur van de overheid richting de cloud gaan verhuizen.

De overdracht van verantwoordelijkheid zoals weergegeven in Figuur 1 kan binnen de context van een nationale overheid gezien worden als een overdracht van soevereiniteit. Het geeft minder tot geen zorgen maar ook minder tot geen controle. Wanneer door overheden clouddiensten worden afgenomen, maken deze zich volstrekt afhankelijk van commerciële partijen die veelal opereren op een ander continent en onder een ander rechtssysteem. Gezamenlijk zijn de ministeries, provincies en gemeenten van cruciaal belang voor het functioneren van de grote delen van de samenleving.

Migraties naar de cloud zijn complexe projecten en worden niet aangegaan voor een paar jaar, maar voor 5 tot 10 jaar en langer. Eenmaal uitgevoerd ontstaat een lock-in van data, koppelingen en gewenning van eindgebruikers die lastig om te keren is. Daarom is het ook van belang om naar de langere termijn te kijken waar het gaat om risico's en de implicaties daarvan op het gebruik van clouddiensten.

Geopolitiek

Door vergaande digitalisering van de samenleving is er een relatief nieuw maar belangrijk risico: geopolitiek. Een recent voorbeeld is de situatie van Rusland. In een tijdsbestek van enkele maanden is Rusland in vergaande mate afgesloten van diverse westerse clouddiensten en andere voorzieningen. Zij het door directe afsluiting of door het blokkeren van betaalmethodes die hier voor nodig zijn. Indien de Russische overheid gebruik zou hebben gemaakt van bijvoorbeeld Office 365 of Google Workspace voor interne planning en communicatie, zouden we kunnen verwachten dat de beschikbaarheid, integriteit en vertrouwelijkheid van deze diensten ernstig aangetast zouden zijn en zou leiden tot ontwrichting.

Nederland bevindt zich uiteraard in een totaal andere en onvergelijkbare positie, maar het is duidelijk geworden dat de fysieke locatie van data en clouddiensten anno 2023 een kwestie van nationale soevereiniteit is geworden. Wanneer we deze constatering combineren met de observatie dat cloud-migraties voor lange duur worden aangegaan en moeilijk omkeerbaar zijn, is het van belang om terughoudend te zijn met het opslaan van overheidsdata buiten landsgrenzen en eigen jurisdictie. Hoe onwaarschijnlijk deze risico's nu wellicht lijken, met een rationele en kritische blik richting de lange termijn lijkt het onverantwoord om de soevereiniteit van een land zodanig uit handen te geven.

Men meent deze risico's te kunnen wegnemen met wetten, verordeningen, richtlijnen, contracten en inkoopvoorwaarden. Denk aan het Data Privacy Framework (voorheen Privacy Shield). Dit biedt een papieren zekerheid die niet overeenstemt met de praktische realiteit. Een realiteit waarin alle controle over kritieke data en de toegang daartoe wordt overgedragen aan een derde die:

- toegang tot dienst kan blokkeren (beschikbaarheid)
- de data kan manipuleren (integriteit)
- de data bedoeld of onbedoeld kan lekken en/of inzien (vertrouwelijkheid)

De wetten en contracten functioneren tot het moment dat er een situatie ontstaat waardoor het niet meer functioneert. Op dat moment is de praktische realiteit doorslaggevend en heeft de afnemer geen enkele controle.

Het is mogelijk om dit deels te mitigeren door middel van frequente back-ups en gebruik van open source en open standaarden. Dit kan echter alleen de impact van niet-beschikbaarheid (deels) oplossen. Een directe afsluiting van toegang zou zelfs bij aanwezigheid van back-ups voor een langdurige onderbreking zorgen. In het geval van uitgebreide/complexe diensten als Office 365 kan het maanden duren voordat voor alle componenten een werkend alternatief is gevonden. In dit geval is alsnog de vertrouwelijkheid en mogelijk de integriteit van de data blijvend aangetast.

SaaS én Soeverein?

Uiteindelijk zal er een middenweg gevonden moeten worden waarbij men kan profiteren van de voordelen van SaaS, maar ook verantwoord omgaat met de nadelen. De meest doeltreffende strategie is om overheidsdata enkel binnen eigen landsgrenzen op de slaan in eigen datacenters of bij Nederlandse entiteiten die kunnen opereren zonder invloeden van andere rechtssystemen.

Indien er toch voor SaaS leveranciers buiten Nederland wordt gekozen, dan is het goed voorkeur te geven aan doorlopende integrale back-ups, het gebruik van open source en open standaarden en waar mogelijk end-to-end versleuteling. De data zijn cruciaal en back-ups zorgen voor de mogelijkheid tot herstel en migratie wanneer problemen optreden. Open source geeft extra inzage in hetgeen achter de schermen gebeurt en maakt migraties naar alternatieven een stuk eenvoudiger aangezien de broncode beschikbaar is. Open standaarden maken het mogelijk om de data eventueel over te hevelen naar andere leveranciers of systemen die ondersteuning bieden voor dezelfde open standaarden.

De wereld digitaliseert en dit proces is nog lang niet ten einde. Het wereldwijde en publieke internet is daarmee een belangrijk geopolitiek speelveld geworden. Het is niet waarschijnlijk dat Nederland te maken zal krijgen met geopolitieke situaties zoals hierboven beschreven. Maar als de prijs is dat de overheid potentieel maanden niet kan functioneren en gegevens over het functioneren van de overheid en haar burgers buiten onze nationale macht komen te liggen, moeten we ons misschien afvragen of de voordelen opwegen tegen de mogelijk onomkeerbare nadelen.