Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# 5 adviezen voor veilige inkoop van clouddiensten

Factsheet FS-2020-06 | versie 1.0 | 16 oktober 2020

Vele organisaties overwegen, of zijn al bezig met de inkoop van clouddiensten. Clouddiensten kunnen een grote functionele aanvulling vormen voor organisaties, mits er afgewogen maatregelen zijn genomen voor de inkoop van clouddiensten. Organisaties blijken in de praktijk clouddiensten regelmatig niet veilig in te kopen, wat leidt tot onbeheerste risico's. Veel van deze risico's zijn na het inkopen nog wel te mitigeren. Voor een aantal maatregelen geldt echter dat deze alleen effectief zijn als ze vooraf getroffen worden. Het NCSC adviseert om geen clouddienst in te kopen zonder vooraf vijf maatregelen te treffen: (1) risicoanalyse, (2) configuratie en monitoring, (3) exitstrategie, (4) functioneel beheer en (5) audittoegang.

## Achtergrond

Publieke clouddiensten zijn populair, bij particulieren maar in toenemende mate ook bij organisaties. Grote clouddienstverleners zoals Microsoft en Amazon bieden cloudvarianten aan voor steeds meer veelgebruikte toepassingen. Deze diensten bieden een grotere schaalbaarheid. Ook kan het gebruik van een clouddienst kostenbesparend zijn. Dit maakt dat veel organisaties overwegen, of zelfs al bezig zijn om functionaliteit van onpremise-omgevingen naar de cloud te verplaatsen.

Onder 'publieke clouddiensten' verstaan we in deze factsheet zowel IaaS als PaaS en SaaS. Voorbeelden zijn Amazon EC2 (IaaS), Microsoft Windows Azure (PaaS) en Microsoft Office 365 (SaaS). De genoemde adviezen gelden voor alle soorten clouddiensten.

## Wat is er aan de hand?

Clouddiensten bieden vele aantrekkelijke functionaliteiten in vergelijking met onpremise-omgevingen. Om zo veilig mogelijk gebruik te maken van deze diensten is een afgewogen inkoop essentieel. Organisaties blijken clouddiensten nog onveilig in te kopen. Als medewerkers zich bijvoorbeeld niet bewust zijn van de gevoeligheid van de gegevens waar ze mee werken, bestaat het risico dat onbedoeld gevoelige gegevens in cloudomgevingen staan. Als daarbij voor veilig cloudgebruik geen aanvullende maatregelen worden getroffen, dan loopt de organisatie een verhoogd risico op beveiligingsincidenten zoals datalekken of overtredingen van wetgeving.

Ook komt het regelmatig voor dat medewerkers niet precies nagaan welke taken een clouddienstverlener wel en niet vervult. Zo vergeten ze verantwoordelijkheden als backup, monitoring en autorisatiebeheer te beleggen, wat later tot grote problemen kan leiden.

## Doelgroep

Werknemers die betrokken zijn bij cloudinkoop

## Aan deze factsheet hebben bijgedragen:

- CIO Rijk
- Conclusion
- DNB
- NBV van de AIVD
- Schuberg Philis
- Strategisch Leveranciersmanagement Microsoft Google AWS Rijk

Deze situatie ontstaat omdat organisaties bestaande regels niet naleven, niet omdat er geen regels zijn. Er bestaan meerdere richtlijnen, normen en afwegingskaders[1] over uitbestedingsrisico's voor clouddiensten. In de praktijk blijken organisaties deze regelmatig niet of onvolledig toe te passen. Dit heeft verschillende oorzaken. Het implementeren van allerlei maatregelen maakt de uitbesteding bijvoorbeeld duurder. Daarnaast is er specifieke kennis van clouddiensten nodig om veilig clouddiensten in te kopen en te gebruiken.

## Wat kan er gebeuren?

Wanneer een organisatie functionaliteit (bijvoorbeeld opslag of verwerking) onvoldoende veilig uitbesteedt aan clouddienstverleners, dan leidt dit tot risico's. Sommige van deze risico's zijn te mitigeren door naderhand alsnog passende maatregelen te treffen. Voor een aantal maatregelen geldt echter dat deze alleen effectief zijn als ze vooraf getroffen worden.

De meeste clouddienstverleners bieden mogelijkheden voor nauwkeurig autorisatie- en toegangsbeheer. Als inkopende organisaties hier onvoldoende gebruik van maken, dan kan het gemakkelijk gebeuren dat vele medewerkers volledige toegang hebben tot alle gegevens. Dit kan grote gevolgen hebben, bijvoorbeeld voor het vermogen van de organisatie om aan relevante wet- en regelgeving te voldoen. Als door gebrekkige toepassing van logging en monitoring vervolgens achteraf niet te achterhalen is wie welke gegevens heeft geraadpleegd, dan valt er slechts te concluderen dat u geen idee heeft wat er in de tussentijd met uw gegevens is gebeurd.

Veel clouddiensten zijn makkelijk in gebruik te nemen, maar lang niet altijd gemakkelijk te verlaten. De dienstverlener heeft er immers belang bij u als klant te behouden. Dit risico staat bekend als 'vendor lock-in'. Als u vooraf de mogelijkheid om eenvoudig te vertrekken niet contractueel heeft vastgelegd, dan kunt u daar naderhand geen aanspraak meer op maken. Een migratietraject kan dan zeer complex of duur uitvallen.

Wanneer organisaties clouddiensten inkopen, dan maken ze vaak geen afspraken over de toepassing van standaarden en toegang tot auditinformatie met de dienstverlener. Naderhand valt dat bijna niet meer af te spreken. Hierdoor ontstaat het risico dat organisaties geen inzicht hebben in het beveiligingsniveau van de clouddienstverlener. Mogelijk voldoet de organisatie daardoor ook niet aan wet- en regelgeving (zoals de Algemene Verordening Gegevensbescherming) en is ze niet in staat risico's te beheersen.

## Wat adviseert het NCSC?

Het NCSC adviseert om risico's van cloudinkoop te mitigeren door *vooraf* onderstaande maatregelen te treffen. Met deze maatregelen mitigeert u risico's die na het sluiten van de overeenkomst nauwelijks nog te mitigeren zijn.

De genoemde maatregelen zijn voornamelijk organisatorisch, bestuurlijk en juridisch van aard. Juist bij deze aspecten maakt het veel verschil of u er vooraf aandacht aan schenkt. In de selectiefase kunt u nagaan welke leverancier u in staat stelt om deze maatregelen passend te implementeren, en in de onderhandeling over het contract kunt u bepaalde voorzieningen juridisch vastleggen. Na het sluiten van de overeenkomst is het vaak moeilijk of onmogelijk om deze maatregelen nog toe te passen. Voor technische maatregelen geldt dit minder. Hoewel ook daarbij vroege toepassing leidt tot een hoger beveiligingsniveau, kunt u technische aspecten bij overhaaste inkoop vaak achteraf nog wel herstellen.

Deze opsomming van maatregelen is niet volledig. Ten eerste zijn er veel andere maatregelen die u kunt treffen voor een veilige clouduitbesteding. Ten tweede kunnen er in uw organisatie aanvullende belangen en beveiligingsbehoeften spelen bij het uitbesteden van functionaliteit aan een clouddienstverlener. Het NCSC adviseert om op basis van risicomanagement en wet- en regelgeving gebruik te maken van bestaande normen en richtlijnen voor cloudinkoop. Zo blijft u in staat om de

[1] Meerdere organisaties hebben richtlijnen en afwegingskaders opgesteld, bijvoorbeeld CISPE, ENISA, SANS, CSA, DHPA en de Rijksoverheid. Voorbeelden van veelgebruikte normenkaders zijn ISO 27010, CSA, SOC2, C5 en G-CLOUD.

risico's van clouduitbesteding effectief te beheersen, ook na de initiële inkoop.

Het NCSC heeft een cloudervaringsdocument gepubliceerd, waarin staat beschreven hoe het NCSC zelf omgaat met het waarborgen van zijn organisatiebelangen bij clouduitbesteding.[2]

## Handelingsperspectief: te treffen maatregelen

### Maak iemand binnen uw organisatie verantwoordelijk voor de in te kopen clouddienst en laat deze verantwoordelijke een risicoanalyse uitvoeren

Voer een risicoanalyse per clouddienst uit op het gebied van privacy, compliance, security en financiering. Uitbesteding naar clouddienstverleners brengt zowel voordelen als nieuwe risico's met zich mee.

De risicoanalyse stelt u in staat om te besluiten welke gegevens u naar de clouddienst wilt migreren. Hanteer hierbij het uitgangspunt dat de clouddienstverlener de gegevens in kan zien. Er bestaan meerdere afwegingskaders die u helpen te besluiten welke gegevens u naar een clouddienst wilt migreren. Betrek ook professionals met kennis over clouddienstverlening, zoals securityarchitecten, bij de risicoanalyse.

Uitbesteding aan een clouddienstverlener brengt ook risico's met zich mee rond privacy en compliance. Veel organisaties kiezen voor uitbesteden vanwege het gemak, maar bij incidenten zullen toezichthouders en het publiek ook uw organisatie daarop aankijken. Moderne wet- en regelgeving stelt vaak dat u minstens ten dele verantwoordelijk blijft voor gegevensverwerkingen die u uitbesteedt.

Meer informatie over het uitvoeren van een risicoanalyse vindt u in de NCSC-factsheet 'Risico's beheersen: de waarde van informatie als uitgangspunt'.[3] Het NCSC kan organisaties uit zijn doelgroepen assisteren bij het uitvoeren van risicoanalyses.

Stel bij het uitvoeren van de risicoanalyse ook een cloudassessment op. Hierin legt u vast waar een clouddienst die u inkoopt aan moet voldoen. Toets regelmatig, bijvoorbeeld jaarlijks, of de clouddiensten die u inkoopt nog aan dit assessment voldoen. Dit is nodig omdat de aard van de clouddienst of uw gebruik ervan met de tijd kan veranderen.

### Maak een duidelijke verdeling in verantwoordelijkheden op het gebied van configuratie tussen de clouddienstverlener en uw organisatie en richt monitoring in

Beveiligingsincidenten in cloudomgevingen ontstaan vaak door misconfiguratie aan de gebruikerszijde. Wanneer functioneel beheerders dataopslag bijvoorbeeld onvoldoende afschermen, kunnen datalekken ontstaan. Vanwege het open karakter van veel clouddiensten, kan opgeslagen informatie dan zelfs voor elke internetgebruiker toegankelijk zijn. Zorg daarom voor passende configuratieprocessen van de betreffende dienst, voor u data naar clouddiensten migreert.

Een uitbestedende organisatie is in eerste instantie zelf verantwoordelijk voor een veilige configuratie. Beschrijf daarom in het configuratieproces wie configuraties beheert en hoe u misconfiguraties zult detecteren. Clouddienstverleners bieden regelmatig scantools aan om de veiligheid van uw configuratie te controleren. Daarnaast kunt u met een clouddienstverlener in het contract afspreken dat u een derde partij met een penetratietest de configuratie wilt laten controleren. Met zo'n penetratietest kunt u misconfiguraties opsporen, nog voor u uw data naar de clouddienst heeft gemigreerd.

### Bepaal uw exitstrategie en leg deze contractueel vast

Ooit kunt u besluiten dat u niet langer van een clouddienst gebruik wilt maken. Op dat moment wilt u dat het mogelijk is te migreren, liefst met beperkte aanvullende kosten. Maak daarom in de dienstverleningsovereenkomst afspraken over de mogelijkheden om uw data weg te migreren. Is het specifieke formaat van de gegevens voor u van belang, leg dit dan ook in de overeenkomst vast.

Organisaties kiezen er regelmatig voor om hun eigen applicaties diepgaand te integreren met de clouddiensten

[2] Zie https://www.ncsc.nl/actueel/nieuws/2020/juni/11/clouddiensten.

[3] Zie https://www.ncsc.nl/documenten/publicaties/2020/juli/21/factsheet-risicobeheersing.

die ze gebruiken. Maak vooraf de keuze of u applicaties wilt integreren. Een risico kan zijn dat migratie naar een andere clouddienst moeilijk of onmogelijk wordt. Vormt dit voor uw organisatie een groot risico? Kies dan voor software die zoveel mogelijk platformonafhankelijk werkt.

Er bestaan standaarden en dienstverleners die uw organisatie helpen bij het overstappen van clouddienstverlener. SWIPO (Switching Providers and Porting Data)[4] is bijvoorbeeld een Europees initiatief dat gedragscodes heeft ontwikkeld die helpen bij eenvoudiger overstappen tussen clouddienstverleners. Clouddienstverleners kunnen zich committeren aan deze gedragscodes, om zo te laten zien dat zij hun klanten in staat stellen hun gegevens eenvoudig te migreren.

### Stem uw functioneel beheer af op de clouddienst, en tref hiermee passende maatregelen voor authenticatie en autorisatie

Hoewel het gebruik van een clouddienst beveiligingsvoordelen kan hebben, maakt het ook nieuwe vormen van misbruik mogelijk. Gebruikt u bijvoorbeeld geen streng toegangsbeleid in een cloudomgeving, dan kan dat leiden tot datalekken. Elke medewerker heeft dan bijvoorbeeld toegang tot alle informatie en functionaliteit.

Pas fijnmazig toegangsbeheer toe wanneer u de clouddienst in gebruik neemt, in de vorm van RBAC- of ABAC-gebaseerd identiteits- en toegangsbeheer.[5] Stel beleid op dat beschrijft wie toegang heeft tot welke gegevens en functionaliteiten in de clouddienst. Beperk in dit beleid de toegang die een account standaard heeft tot het minimum, en ken naar behoefte tijdelijk verhoogde rechten toe. Vraag uw functioneel beheerders om dit beleid toe te passen en erop te monitoren.

U kunt het voorgaande advies op verschillende manieren concretiseren. Zo kunt u bijvoorbeeld standaard gebruikmaken van tweefactorauthenticatie op alle accounts. Ook kunt u toegang tot gegevens en functionaliteit alleen toekennen op basis van noodzaak. Dit heet ook wel het principe van *least privilege*. Wilt u toegang bieden op basis van uw eigen middelen voor identiteits- en toegangsbeheer? Regel dit dan vooraf in het contract. Uw functioneel beheerders kunnen deze maatregelen toepassen en monitoren, eventueel met behulp van speciale software om dit in cloudomgevingen te doen. Clouddienstverleners bieden bijvoorbeeld verschillende geautomatiseerde tools die instellingen toetsen tegen het beveiligingsbeleid.

### Maak afspraken zodat u effectieve auditinformatie over uw clouddienstverlener kunt verkrijgen

Spreek met uw clouddienstverlener af op welke manier u met behulp van audits inzicht kunt krijgen in de kwaliteit van de geboden dienstverlening. In vrijwel alle gevallen is zelfstandige audittoegang beperkt of niet mogelijk. U bent in dat geval afhankelijk van audits door derde partijen. De rapporten van deze partijen kunnen een bepaalde mate van zekerheid geven, het zogenaamde *assurance level*.

Als u dat contractueel vastlegt, is het vaak wel mogelijk om input te geven wanneer uw clouddienstverlener een audit laat uitvoeren door een derde partij. Zo kunt u de vragen die voor uw organisatie centraal staan, specifiek laten beantwoorden. Zorg dat u in staat bent om deze vragen aan te leveren, en om de resulterende rapportages ook te verwerken, bijvoorbeeld in een gespecialiseerd proces.

Voor u deze gesprekken voert, zult u moeten weten welke normen en standaarden voor uw organisatie van belang zijn. Over populaire standaarden of verklaringen zoals DPA, SOC2 of ISO 27017 kunt u vaak afspraken maken met een clouddienstverlener. Hetzelfde geldt voor de locatie waar uw gegevens verwerkt of opgeslagen worden. Voor organisaties uit de Rijksoverheid zijn er verschillende raamovereenkomsten met clouddienstverleners gesloten. Zulke raamovereenkomsten kunnen uw organisatie helpen bij het sluiten van een overeenkomst met zo'n dienstverlener.

[4] Zie https://swipo.eu/.

[5] RBAC staat voor Role-based access control, ABAC staat voor Attribute-based access control.

**Uitgave**
Nationaal Cyber Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

**Meer informatie**
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

oktober 2020