Checklist Clouddienstverlening

(publieke SaaS-applicaties)

Colofon

Opgesteld door: Fleur van Leusden

Versiebeheer

Versie: [versienummer]
Datum: [datum versie]

Versie	Datum	Auteur(s)	Opmerkingen
0.1			

Wat is cloud?

Cloud is een verzamelterm voor verschillende typen dienstverlening waar men gebruik maakt van een infrastructuur die niet door de eigen organisatie beheerd wordt. Voor medewerkers is het belangrijkste te weten dat in elk geval alle applicaties waarvoor je via het internet ergens naartoe moet navigeren en vervolgens moet inloggen (niet zijnde van SSC ICT) cloudapplicaties zijn waarvoor deze checklist bedoeld is.

Doel en doelgroep

Het doel van deze checklist is om voor de organisatie te inventariseren en inzichtelijk te maken hoe de meest voorkomende informatiebeveiligingsrisico's omtrent publieke cloudoplossingen worden behandeld voor een specifieke applicatie. Door deze checklist in te vullen krijgen de teams die een wens hebben voor gebruik van een clouddienst, inzicht in de risico's en wat moet worden geregeld. De checklist is bedoeld om ingevuld te worden door de (potentiële) eigenaar van de clouddienst. Deze kan na het invullen overleggen met de CISO of er nadere acties nodig zijn en zo ja, welke. De CISO kan, indien noodzakelijk, op basis van de checklist een risico-inventarisatie maken en eventueel aanvullend advies geven.

Het is de bedoeling dat de checklist gebruikt wordt als hulpmiddel. De checklist zal daarom niet altijd in te vullen zijn zonder nader onderzoek te doen of informatie op te vragen bij de dienstverlener of elders.

De nadruk van de checklist ligt op publieke cloud, omdat hier voor de organisatie de meeste beveiligingsrisico's spelen.

Woordenlijst

Woord	Betekenis
Clouddienstverlening	Een ICT-dienst waarbij gebruik gemaakt wordt van infrastructuur buiten de organisatie. Er zijn meerdere soorten clouddiensten. Voorbeelden zijn Platform as a Service (PaaS) en Software as a Service (SaaS).
Departementaal Vertrouwelijk	Departementaal Vertrouwelijk is alle informatie die bij openbaarmaking risico's oplevert voor burgers, bedrijven of de eigen organisatie.
EER (Europese Economische Ruimte)	Landen die lid zijn van de Europese Economische Gemeenschap.
Eigenaar	Degene binnen de organisatie die verantwoordelijk is voor een applicatie. Deze rol is verantwoordelijk voor het budget, correct en veilig gebruik en eventueel gerelateerde projecten.
Openbaar (informatie)	Openbaar is alle informatie die bij openbaarmaking geen risico oplevert voor burgers, bedrijven, de organisatie of de Nederlandse Staat en diens belangen.
Publieke Cloud	Clouddienst die openbaar en dus voor iedereen te gebruiken is. Voorbeelden zijn S3, Azure, maar ook Facebook, Mentimeter en Gmail.
SLA (service level agreement)	Afspraken over de mate waarin een applicatie beschikbaar moet zijn. Hoeveel procent van de tijd mag een applicatie offline zijn (bijvoorbeeld door storing of onderhoud)?

Tips

Bij het invullen is de kans groot dat niet alle vragen meteen beantwoord kunnen worden. Clouddienstverleners hebben informatie soms centraal beschikbaar gesteld voor klanten of geïnteresseerden, en dan met name certificeringen, concept verwerkingsovereenkomsten etc. Het loont de moeite hiernaar te zoeken online.

Om te voorkomen dat er niet-werkende links in deze checklist komen te staan, staan hier geen verwijzingen. Maar je kunt ervan op aan dat bij de meeste dienstverleners de hier gevraagde informatie online vindbaar is of anders is op te vragen.

Checklist

Algemene informatie

Naam applicatie	
Naam dienstverlener (bedrijf)	
Type clouddienst (SaaS, IaaS, PaaS etc.)	
Naam (potentieel) eigenaar (intern)	
Voornamelijk in gebruik bij team	
Datum/periode verwachte start ingebruikname	

Type informatie, AVG en schade

1. Wat is het niveau van vertrouwelijkheid van de informatie die wij willen verwerken en opslaan in de applicatie?[1]

☐ Openbaar
☐ Departementaal vertrouwelijk

Toelichting:

Informatie met een andere rubricering dan ‘openbaar’ of ‘departementaal vertrouwelijk’ mag niet in een publieke cloudoplossing worden opgeslagen of verwerkt.

Hoger dan dit is informatie die bij openbaarmaking risico’s oplevert voor de Nederlandse Staat en (diplomatieke) dienstbelangen.

[1] Wat ‘openbaar’ en ‘departementaal vertrouwelijk’ inhoudt staat uitgelegd in de verklarende woordenlijst boven in dit document.

2. Bevat de informatie persoonsgegevens en zo ja, welke soort?

Persoonsgegevens: alle informatie die (in theorie) te herleiden is naar de identiteit van een natuurlijk, levend, persoon. Voorbeelden: IP-adressen, namen, adressen, e-mailadressen (ook zakelijk), kentekenbewijzen etc.

Bijzondere persoonsgegevens: medische informatie, strafrechtelijke informatie, politieke voorkeur, ras/afkomst en religie.

☐ Persoonsgegevens
☐ Bijzondere persoonsgegevens
☐ Nee

Toelichting:

Bijzondere persoonsgegevens mogen niet zonder meer in een publieke cloudoplossing worden verwerkt of opgeslagen. Hiervoor dienen vooraf een DPIA en een risicoanalyse te worden opgesteld en het gebruik dient te worden gemeld bij het Rijk.[2]

3. Gaat de applicatie grote hoeveelheden persoonsgegevens opslaan?

☐ Ja
☐ Nee

Toelichting:

Bij grote hoeveelheden persoonsgegevens dient vooraf een DPIA te worden opgesteld. Wat precies ‘grote hoeveelheden’ zijn is niet expliciet vastgelegd in de AVG. Ga ervan uit dat als het over meer dan honderd betrokkenen gaat, je kunt spreken van ‘grote hoeveelheden’.

[2] Cloudbrief

4. Waar wordt de informatie opgeslagen?

☐ Binnen de EER
☐ Buiten de EER

Toelichting:

Bij het opslaan van persoonsgegevens buiten de EER dien je contact op te nemen met de Privacy Officer voor advies.

Niet openbare informatie, ook als het geen persoonsgegevens betreft, mag niet worden opgeslagen in Rusland, China, Iran of Noord-Korea.

5. Is een verwerkingsovereenkomst opgesteld en/of heeft de dienstverlener een model verwerkingsovereenkomst online staan?

☐ Niet van toepassing
☐ Nee
☐ Ja, is beschikbaar
☐ Ja, ARBIT-modelovereenkomst mogelijk

Toelichting:

Bij het opslaan van persoonsgegevens in een cloudoplossing is een verwerkingsovereenkomst een vereiste. De ARBIT heeft hierbij de voorkeur, omdat dit model van de Nederlandse overheid is.

6. Als de informatie uit deze applicatie gemanipuleerd zou worden, niet langer beschikbaar zou zijn op een belangrijk moment of openbaar zou worden gemaakt, waar heeft dat dan impact op? Selecteer alle antwoorden die van toepassing zijn.

☐ Niemand
☐ Burgers
☐ Bedrijven
☐ Onze eigen organisatie
☐ Het ministerie
☐ De Staat
☐ Diplomatieke betrekkingen
☐ De democratie
☐ Anders, namelijk:

7. Wat geldt voor de mate waarin de informatie beschikbaar moet zijn?

☐ Als de informatie niet beschikbaar is, zelfs voor korte duur, is dit problematisch
☐ Als de informatie niet beschikbaar is voor meer dan een week is dit problematisch
☐ Als de informatie niet beschikbaar is, zelfs voor korte duur, is dit alleen problematisch op kritieke momenten
☐ Als de informatie niet beschikbaar is voor meer dan een week is dit alleen problematisch op kritieke momenten
☐ Het is niet erg als de informatie voor langer dan een week niet beschikbaar is

Toelichting:

8a. In hoeverre kan de dienstverlener voldoen aan de gewenste beschikbaarheid?

☐ Hierover zijn geen afspraken gemaakt of te maken
☐ Door middel van een SLA, maar verder geen consequenties als de SLA niet wordt gehaald
☐ Door middel van een SLA, met alleen financiële consequenties als de SLA niet wordt gehaald
☐ Door middel van een SLA, met contractuele consequenties als de SLA niet wordt gehaald
☐ Anders, namelijk:

Toelichting:

Met ‘contractuele consequenties’ word bedoeld dat de organisatie het contract met de leverancier bijvoorbeeld per direct mag opzeggen bij niet halen van het SLA.

8b. Is het mogelijk om onderhoudswerkzaamheden te verplaatsen voor of na voor onze organisatie kritieke momenten?

☐ Niet van toepassing
☐ Nee
☐ Ja

Toelichting:

Exitstrategie

9. Als de dienstverlener niet voldoende kan leveren wat wij nodig hebben, de beschikbaarheid tegenvalt of men de prijzen verhoogt, zijn er dan andere dienstverleners waarop wij kunnen overstappen?

☐ Ja, namelijk:
☐ Nee

10. (Alleen als de vorige vraag met ‘ja’ is beantwoord:) Schat in hoeveel tijd het onze organisatie kost om over te stappen op een alternatieve dienstverlener.

☐ Minder dan een week
☐ Minder dan een maand
☐ Maximaal zes maanden
☐ Maximaal een jaar
☐ Langer dan een jaar

Certificering en audits

11. Heeft de dienstverlener een of meer van de volgende certificeringen/auditrapportages (die kunnen worden ingezien)?

☐ ISO27001/2
☐ SOC 2
☐ Anders, namelijk:

Toelichting:

12. In hoeverre staat de dienstverlener externe audits toe?

☐ Niet
☐ Alleen door dienstverlener zelf gecontracteerde auditors
☐ Wij mogen zelf audits uitvoeren of auditors inschakelen

Toelichting:

13. Indien de dienstverlener zelf auditors toestaat, kunnen wij de rapportages hiervan dan (op verzoek) inzien?

☐ Ja
☐ Nee

Toelichting:

Toegangsbeveiliging

14. Op welke manier zijn wij voornemens toegang tot de applicatie te verkrijgen? Selecteer alleen meerdere vakjes als al deze opties naast elkaar zullen worden toegepast.

☐ Single Sign On via bestaande infrastructuur die wij al gebruiken
☐ Multi-factor authenticatie via SMS
☐ Multi-factor authenticatie via een app
☐ Multi-factor authenticatie via een hardware token (geen code, maar bijvoorbeeld Yubikey)
☐ Wachtwoord
☐ VPN
☐ Allowlisting (op basis van IP)
☐ Anders, namelijk:

Toelichting:

15. Is het mogelijk inzage te krijgen in logging gegevens betreffende wie, wanneer is ingelogd?

☐ Ja
☐ Nee

Toelichting:

16. Zijn alle accounts op naam, ook van beheerders van onze kant?

☐ Ja
☐ Nee

Toelichting:

17. Is het mogelijk inzage te krijgen in logging over wie wanneer iets gewijzigd heeft in de applicatie (van de kant van onze organisatie)?

☐ Ja
☐ Nee

Toelichting:

18. Hoe lang worden logginggegevens bewaard?

Antwoord:

19. Kunnen wij periodiek een overzicht krijgen van alle door ons gebruikte accounts?

☐ Ja
☐ Nee

Toelichting:

20. Hoe borgt de eigenaar dat accounts van ex-medewerkers of medewerkers die geen toegang meer nodig hebben op tijd worden ingetrokken?

☐ Automatisch d.m.v. een script gekoppeld aan personeelssysteem of andere relevante systemen
☐ Handmatig door zelf op te letten, periodieke controle waar een tweede persoon toezicht op houdt
☐ Anders, namelijk:

21. Is er een toegangsmatrix opgesteld?

Voorbeeld:

Rol	Inzage	Aanmaken	Wijzigen	Verwijderen	Beheer
Business Analist	X				
Developer	X	X	X	X	
Test engineer	X	X	X	X	
Functioneel Beheerder	X	X	X	X	X

☐ Ja

☐ Nee

Toelichting/tabel(len) toegangsmatrix:

22. Welke rol binnen onze organisatie zal het functioneel beheer van de applicatie uitvoeren?

Antwoord:

Incidentmanagment

23. In hoeverre is vastgelegd dat en hoe de leverancier ons dient te informeren in het geval van een (mogelijk) beveiligingsincident?

☐ Niet vastgelegd

☐ Contractueel vastgelegd met randvoorwaarden

☐ Contractueel vastgelegd zonder randvoorwaarden

Met randvoorwaarden wordt bijvoorbeeld bedoeld binnen hoeveel uur en via welke lijn/welk communicatiemiddel de leverancier contact met ons opneemt.

Toelichting:

Back-ups

24. Wat gebeurt er wanneer alle informatie in de applicatie (door een fout/storing/malware) gewist blijkt (op het meest ongunstige moment)?

☐ Dat is niet erg, de informatie is niet belangrijk voor onze organisatie om zijn taken uit te voeren
☐ Hiervoor is een terugvalmogelijkheid geregeld op eigen netwerk/papier/anders
☐ Dan zijn wij als organisatie niet langer in staat diens primaire taken uit te voeren
☐ Anders, namelijk:

Toelichting:

Als het antwoord 'Dan zijn wij als organisatie niet langer in staat diens primaire taken uit te voeren' is, is het advies een risicoanalyse te laten uitvoeren.

Verbanden

25. Met welke andere applicaties op andere netwerken wisselt deze cloudapplicatie geautomatiseerd informatie uit?

Denk aan applicaties als Slack, Azure AD of Outlook.

Antwoord:

26. Mag de leverancier conform diens voorwaarden informatie van onze organisatie gebruiken voor eigen/andere doeleinden? Zo ja, waarvoor?

Antwoord:

27. Bevat de applicatie zelflerende algoritmes of vergelijkbare technologie (Artificial Intelligence) waarbij de informatie van onze organisatie kan worden gebruikt om het algoritme te trainen?

☐ Ja
☐ Nee

Toelichting:

Risicoanalyse

28. Is er sprake van een of meer van de volgende situaties?

☐ De leverancier is de afgelopen 12 maanden in het nieuws geweest als slachtoffer van een of meerdere succesvolle aanvallen waarbij informatiebeveiliging in het geding is geweest.
☐ De beveiligingsmaatregelen passen niet bij de gevoeligheid of beschikbaarheidseisen van de informatie (bijvoorbeeld alleen een wachtwoord als toegangsbeveiliging voor gevoelige informatie).
☐ In het geval dat de leverancier onbetrouwbaar blijkt is er geen redelijk alternatief (vendor lock-in), terwijl onbeschikbaarheid van de applicatie ertoe kan leiden dat de primaire taken van de organisatie niet langer kunnen worden vervuld.
☐ Geen van deze beschrijvingen is van toepassing.

Toelichting:

Indien een of meerdere situaties van toepassing zijn dient met de CISO te worden overlegd of een risicoanalyse noodzakelijk is.

=======EINDE CHECKLIST=====