ONLINE TRUST COALITIE
MANIFEST

ONLINE TRUST
COALITIE

Leidschendam, september 2020

Ruim twintig organisaties afkomstig uit overheid, bedrijfsleven en wetenschap hebben zich verenigd in de Online Trust Coalitie. Deze coalitie is een initiatief van het Ministerie van Economische Zaken en Klimaat en het publiek-private samenwerkingsproject Partnering Trust[1].

De Online Trust Coalitie ziet dat cloud- en onlinediensten (in het vervolg clouddiensten) deel uitmaken van vrijwel alle digitale innovaties. Artificial Intelligence (AI) en het Internet of Things (IoT) nemen juist nu een grote vlucht omdat opslag, rekenkracht en slimme algoritmen in de cloud beschikbaar zijn. Clouddiensten zijn essentieel om de huidige maatschappelijke uitdagingen op te lossen. Clouddiensten zijn dan ook een fundament van de in de Nederlandse Digitaliserings Strategie geformuleerde ambities[2].

De Online Trust Coalitie constateert dat het bijzonder moeilijk is voor de afnemer en andere belanghebbenden (denk aan consumenten, burgers, financiers, aandeelhouders, auditors maar ook toezichthouders) om zekerheid te krijgen over de betrouwbaarheid van clouddiensten, op basis van de verantwoordingsinformatie die aanbieders geven. De moeilijkheid voor aanbieders van clouddiensten is dat belanghebbenden vaak verschillende bewijzen vragen om aan te tonen dat aan alle wettelijke- en betrouwbaarheidseisen wordt voldaan.

Dat gebrek aan zekerheid werpt drempels op voor het gebruik van clouddiensten en remt daarmee innovatie. Het zorgt ook voor een ongelijk speelveld: voor kleinere Europese aanbieders en innovatieve nieuwkomers is het moeilijk om hun betrouwbaarheid aan te tonen en zij kunnen daarom soms minder goed concurreren met grote, gevestigde partijen.

Overheid, bedrijfsleven en wetenschap werken samen in de Online Trust Coalitie om hierin verandering te brengen. De urgentie om samen te werken wordt versterkt door de Europese ontwikkelingen. In februari 2020 is door de Europese Commissie een strategie voor data en AI[3]) aangekondigd. Daarin hebben clouddiensten een centrale rol toebedeeld gekregen. Gezien de Nederlandse ambitie om koploper te zijn in Europa op het gebied van digitalisering, en gegeven het feit dat Nederland een sterke positie heeft op dit gebied, ligt een proactieve en intensieve betrokkenheid bij de invulling van deze Europese strategie voor de hand.

Dit manifest gaat in op het doel van de Online Trust Coalitie, de deelnemers, de uitgangspunten en de vraagstukken die de coalitie wil aanpakken.

1 Partnering Trust is een publiek-privaat samenwerkingsprogramma dat wil bereiken dat afnemers en andere belanghebbenden van clouddiensten op een laagdrempelige manier zekerheid kunnen verkrijgen over de betrouwbaarheid ervan. De afgelopen jaren bracht Partnering Trust Europese samenwerking tot stand en ontwikkelde en implementeerde oplossingsrichtingen samen met aanbieders van clouddiensten en auditors. Het programma Partnering Trust is opgenomen in de Roadmap Veilige Hard- en Software van het Ministerie van Economische Zaken en Klimaat.

2 https://www.rijksoverheid.nl/documenten/rapporten/2018/06/01/nederlandse-digitaliseringsstrategie

3 https://ec.europa.eu/commission/presscorner/detail/en/IP_20_273

DOEL VAN DE COALITIE

Het doel van de Online Trust Coalitie (OTC) is het beschikbaar maken van een eenduidige, efficiënte methode waarmee leveranciers van clouddiensten kunnen aantonen dat hun diensten betrouwbaar en veilig zijn. En die helpt bij het invulling geven aan de relevante wet- en regelgeving.

Veiligheid, beschikbaarheid en privacy zijn daarbij belangrijke aandachtspunten, maar niet de enige. Ook zaken als het snel weer kunnen opstarten van een dienst na een incident en transparante toedeling van verantwoordelijkheden wanneer meerdere aanbieders betrokken zijn bij een dienst, spelen een rol.

Niet alleen de afnemer, maar ook andere belanghebbenden hebben zekerheid nodig over de betrouwbaarheid van een clouddienst. Denk aan consumenten, financiers, aandeelhouders, auditors, maar ook toezichthouders[4].

WIE ZIJN AANGESLOTEN BIJ DE COALITIE

OTC is een samenwerkingsverband van leidende nationale en internationale partijen, zowel aanbieders als afnemers van clouddiensten, betrokken overheden en experts, die zich actief bezighouden met cybersecurity, compliance, conformiteit en assurance.

De coalitie heeft een open karakter: wij roepen organisaties op om deel te nemen en met elkaar de digitale economie van Nederland in de internationale context te versterken.

Aanmelden kan via *info@onlinetrustcoalitie.nl.*

4 Denk bij toezichthouders aan partijen als de Agentschap Telecom, ACM, AFM, Belastingdienst, De Nederlandsche Bank enz.

UITGANGSPUNTEN

De OTC hanteert de volgende uitgangspunten:

- Clouddiensten zijn essentiële bouwstenen voor digitale innovaties en leveren daarmee een bijdrage aan oplossingen voor maatschappelijke uitdagingen. Innovaties als Artificial Intelligence (AI) en Internet of Things (IoT) zijn vrijwel alleen mogelijk door gebruik te maken van clouddiensten.
- Clouddiensten omvatten conform de gangbare definitie van het National Institute of Standards and Technology[5] zowel infrastructuur-, platform- als software-as-a-service (Iaas, Paas, SaaS).
- Bij clouddiensten zijn meestal verschillende dienstverleners betrokken die elk delen van de dienst leveren. Afnemers en gebruikers van clouddiensten kunnen ook zelf weer aanbieders zijn, bijvoorbeeld als (cloud)diensten worden geaggregeerd ten behoeve van nieuwe diensten.
- De afnemers van online en clouddiensten vragen zekerheden en de aanbieders willen die bieden. Afnemers hebben een verantwoordelijkheid voor juist en veilig gebruik van een online dienst.
- Naast afnemers van clouddiensten zijn er andere belanghebbenden met betrekking tot zulke zekerheden: denk aan aandeelhouders, auditors, toezichthouders – en in zekere zin de gehele samenleving.
- Over de betrouwbaarheid van de clouddienst moet zekerheid worden geboden. Veel bestaande certificeringen hebben echter niet de kwaliteit van de dienst, maar de kwaliteit van de organisatie van aanbieders als scope.
- Een belangrijk aspect van het bieden en kunnen beoordelen van zulke zekerheid betreft de verantwoordingsinformatie. Uniformiteit en standaardisatie van die informatie zijn daartoe noodzakelijk.
- De aanbieder van een clouddienst moet de afnemer zekerheid bieden over de betrouwbaarheid van de dienst. Vervolgens kan die afnemer zelf aanbieder zijn van een clouddienst: in die rol moet die aanbieder zijn afnemers ook weer zekerheid bieden. De visie van het OTC is daarom dat zekerheden hergebruikt moeten kunnen worden in de keten.
- De OTC sluit aan op de ontwikkelingen binnen de EU rond certificering. De OTC draagt bij aan deze ontwikkelingen door samenwerking en draagvlak te organiseren, zowel binnen Nederland als andere Europese lidstaten. De OTC geeft richting aan Europese ontwikkelingen vanuit de eigen uitgangspunten en doelstellingen. Zij beoogt invulling te geven aan die ontwikkelingen vanuit de Nederlandse situatie.

5 *https://csrc.nist.gov/publications/detail/sp/800-145/final*

VRAAGSTUKKEN

Met de volgende vraagstukken wil de OTC aan de slag om een breed vertrouwen in de digitale economie en in clouddiensten te versterken:

Risico's inschatten en standaardiseren van risicoprofielen

- Eén van de problemen die de OTC wil oplossen, is dat op dit moment afnemers onafhankelijk van elkaar risico's inschatten. Daardoor hebben zij ieder hun eigen wensen en eisen op het gebied van zekerheden over cybersecurity, beschikbaarheid, privacy et cetera. Daar komt bij dat afnemers vaak niet goed weten welke risico's zij lopen, welke assets zij willen beschermen, welke vragen ze moeten stellen en wat hun wettelijke verplichtingen zijn. Het is voor hen onduidelijk welke vormen van zekerheid bij hun specifieke risico's passen. Want afnemers en andere belanghebbenden verschillen van elkaar als het gaat om de bereidheid risico's te accepteren en het vaststellen van de doeltreffendheid van risicobeheersingsmaatregelen.
- Het is voor aanbieders van clouddiensten moeilijk om aan meer dan één eisenpakket invulling te geven. Dat kan botsen. Er is daarom behoefte aan standaardisatie van risicoprofielen, vanuit de gedachte dat deze profielen risk-based zijn.

Verdelen van aansprakelijkheid

Er is sprake van contractuele machtsongelijkheid. In het digitale speelveld van grote en kleine aanbieders en afnemers ontstaan mogelijkheden om aansprakelijkheid af te schuiven. Er is daarom behoefte aan een gestandaardiseerde oplossing voor een rechtvaardige verdeling van de verantwoordelijkheden en bijbehorende aansprakelijkheden.

Right to audit

Sommige wetgeving geeft afnemers het recht of de plicht te auditen bij de aanbieder. Maar ook dwingen afnemers soms contractueel het recht af te mogen auditen. Er moeten oplossingen worden ontwikkeld voor een efficiënte en kosteneffectieve invulling van die rechten en plichten, zodat herhaalde, vrijwel identieke auditactiviteiten bij de aanbieder overbodig worden.

Certificeren en harmoniseren

Het moet helder zijn welke zekerheid een afnemer kan ontlenen aan de verschillende keurmerken, standaarden en verklaringen. Welke zekerheid past bij welk risico? Hierbij gaat het ook om de manieren waarop de informatie over de zekerheden, de verantwoordingsinformatie, beschikbaar is voor afnemers en andere belanghebbenden.

Best practices

Een verkenning naar bestaande en werkbare best practices is nodig, met voorbeelden van hoe bepaalde standaarden in de praktijk werken. Deze bieden mogelijk kansen te worden omarmd in een certificeringssystematiek. Denk aan Zeker-OnLine, Data Pro Code, maar ook NEN-CEN-ISO en andere systematieken.

IT-werkelijkheid

Wanneer de beoordeling van de betrouwbaarheid van clouddiensten vanuit het perspectief van de afnemer als uitgangspunt wordt genomen, dan heeft dat gevolgen voor de IT-auditmethodiek. Het is belangrijk na te gaan welke gevolgen dat heeft voor de werkzaamheden en de vaardigheden van de IT-auditor.

Toezichthouders

Toezichthouders zullen nooit blindelings varen op keurmerken of certificeringen. Maar hun werk kan wel effectiever en gemakkelijker worden gemaakt. Hoe zorgen we ervoor dat ook toezichthouders kunnen steunen op zekerheden? Dit vraagstuk is veelomvattend en wordt in Europa gaandeweg op de agenda gezet. Het gaat dan bijvoorbeeld om accreditering van auditors, governance op audits, deskundigheid en opleiding van auditors, en de wijze van toezicht en handhaven.

RICHTING OPLOSSINGEN

Mijlpaal 1:

Werkgroep ten behoeve van Europese input – april 2020: Doel van de werkgroep is het volgen en waar nodig ondersteunen van de Nederlandse inbreng in Europese initiatieven op het gebied van certificering, zoals de Europese vertegenwoordiging van het Ministerie van Economische Zaken en Klimaat, de ENISA Ad Hoc Working Group on cloud services, de European Cyber Security Certification Group (ECCG), Stakeholder Cybersecurity Certification Group (SCCG), de European Data Protection Board en het GAIA-X initiatief.

Mijlpaal 2:

Manifest Online Trust Coalitie – september 2020: Beschrijving van de vraagstukken die de coalitie wil adresseren. Wat is de scope, wat zijn de uitgangspunten, wat zijn de mijlpalen en wat is het tijdpad?

Mijlpaal 3:

Whitepaper – november 2020: Hoe kunnen we de vraagstukken die in het manifest worden genoemd adresseren, wat is nodig en wat is de rol van de deelnemers in de coalitie?

Mijlpaal 4:

Actieplan Online Trust Coalitie – maart 2021: Het whitepaper uit mijlpaal 3 vormt de basis voor een actieplan dat de genoemde vraagstukken en oplossingsrichtingen realiseert.

DEELNEMERS COALITIE:

De Online Trust Coalitie is een publiek-private samenwerking. Het is een initiatief van het Ministerie van Economische Zaken en Klimaat, waarbij het coalitiebureau met een brede marktvertegenwoordiging, gecoördineerd wordt door ECP| Platform voor de InformatieSamenleving. Het onafhankelijk en neutraal platform waar overheid, bedrijfsleven, maatschappelijke organisaties, wetenschap en onderwijs samenwerken en kennis uitwisselen over de impact op en verantwoorde toepassing van nieuwe technologieën in de Nederlandse samenleving.

Ministerie van Economische Zaken en Klimaat	Jos de Groot
ECP | Platform voor de InformatieSamenleving	Arie van Bellen
Agentschap Telecom	Jasper Nagtegaal
Bureau ICT-toetsing	Ivo Kerkkamp
CIO Platform Nederland	Ronald Verbeek
Cyberveilig Nederland	Petra Oldegarm
DHPA	Ruud Alaerds
ECP | Platform voor de InformatieSamenleving	Michiel Steltman
Erasmus Universiteit	Egon Berghout
Exact	Alexander Rahusen
EY	Marc Welters
Google	Erwin Angelier
ISP Connect	Simon Besteman
KIWA	Ronald Westerveen
Mazars	Jan Matto
Mendix	Frank Baalbergen
Microsoft	Martin Vliem
NCSC	Hans de Vries
NEN	Jolien van Zetten
NLdigital	Julliette van Balen
NOREA	Irene Vettewinkel
PvIB, GEU	Evert van Zanten
TNO	Berry Vetjens
Wolters Kluwer TAA NL	Peter van Ass
Zeker-OnLine	Bert Tuinsma

MANIFEST

WILT U CONTACT OF MEER INFORMATIE?
info@onlinetrustcoalitie.nl
www.onlinetrustcoalitie.nl