Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Digitale autonomie, fundament voor digitale weerbaarheid

RDI toezicht op gebruik van clouddiensten

De discussie over digitale soevereiniteit en autonomie wint snel aan belang in Europa. Veel organisaties zoeken naar manieren om minder afhankelijk te zijn van cloudleveranciers buiten de EU of Nederland. Tegelijkertijd is het belangrijk om scherp te blijven op wat het werkelijke doel is, namelijk digitale weerbaarheid.

Digitale weerbaarheid begint bij één principe: De digitale autonomie oftewel grip op afhankelijkheden.

Alleen gebruik maken van Nederlandse of Europese clouddiensten (soevereiniteit) kan bijdragen aan die weerbaarheid, maar is geen doel op zich. Het is één van de mogelijke manieren om cyberbeveiligingsrisico's te beheersen. Waar het om draait is dat je als organisatie zelf in control bent over je digitale afhankelijkheden. Ongeacht welke cloudleverancier je gebruikt, je moet controle hebben over je data, processen en continuïteit: digitale autonomie.

Jasper Nagtegaal, directeur digitale weerbaarheid RDI: "Organisaties die grip hebben op hun afhankelijkheden, zijn weerbaarder, ongeacht waar hun cloud draait. Organisaties die grip missen, blijven kwetsbaar, zelfs in een volledig 'soevereine' omgeving. "

Er zijn veel goede redenen om gebruik te maken van clouddiensten. In dit paper maken we op hoofdlijnen duidelijk wat de RDI verwacht van organisaties die vallen onder de aankomende Cyberbeveiligingswet (Cbw) en gebruik maken van clouddiensten.

Zet digitale weerbaarheid centraal

Met de invoering van de Cyberbeveiligingswet (de Nederlandse implementatie van de NIS2) ligt er meer nadruk op aantoonbare beheersing van risico's in de digitale infrastructuur. Deze wet stelt geen expliciete eisen aan soevereiniteit en dus geen eisen over waar cloudleveranciers zich wel of niet mogen bevinden.

Belangrijk in ons toezicht is dus digitale autonomie:

- Heeft de organisatie zelf regie op welke clouddiensten op welke wijze worden ingezet en met welk doel.
- En op welke wijze worden de risico's beheerd.

Drie thema's uit de Cyberbeveiligingswet zijn extra relevant bij het gebruik van clouddiensten:

1. Risicoanalyse en beveiliging van informatiesystemen.
2. Beveiliging van de toeleverancierskеten.
3. Effectiviteit van beleid en procedures.

1. Risicoanalyse en beveiliging van informatiesystemen

De Cbw verplicht organisaties passende maatregelen te nemen om risico's voor de beveiliging van hun netwerk- en informatiesystemen te beheersen. Het gebruik van clouddiensten is geen eenvoudige keuze. Het biedt voordelen voor de betrouwbaarheid en beschikbaarheid van de digitale infrastructuur, maar het brengt ook afhankelijkheden die je goed inzichtelijk moet hebben en waarvan de risico's moeten worden afgewogen:

- Welke impact heeft wet- en regelgeving die van toepassing is voor de cloudleverancier?
- Wat is de impact van geopolitieke risico's en/of criminele dreigingen?
- Is er risico op *vendor lock-in* (technisch of contractueel)?
- Heb je als gebruiker inzicht in en invloed op de beveiliging van data in de cloud?
- Wat zijn de gevolgen voor jouw continuïteit als de clouddienst niet beschikbaar is?

Toezicht op risicoanalyse en beveiliging van informatiesystemen

De RDI kijkt of organisaties die gebruik maken van de clouddiensten:

- Een duidelijk beveiligingsbeleid hebben vastgelegd waarin in elk geval is opgenomen: verantwoordelijkheden, taken, rollen, architectuur, beveiligingseisen en uitgangspunten, monitoring, logging en toegang.
- Begrijpen hoe cloudleveranciers de beschikbaarheid, integriteit en vertrouwelijkheid beïnvloeden van hun dienstverlening.
- Concrete maatregelen hebben genomen om afhankelijkheid van de cloudleverancier te minimaliseren (zoals multi-cloud of exit-strategieën).
- Doorlopend geïnformeerd blijven over risico's en kwetsbaarheden.
- Maatregelen treffen ter voorkoming van verstoringen en in geval van verstoringen snel weer kunnen herstellen (Business Continuity Management).

Een goede risicoanalyse betekent dat een organisatie zijn afhankelijkheden goed in kaart heeft gebracht.

2. Beveiliging van de toeleverancierskеten

Een ander belangrijk element van de Cyberbeveiligingswet is de beveiliging van de toeleverancierskеten. Risico's zitten niet alleen in de eigen organisatie, maar ook (in toenemende mate) in de keten. Cloudleveranciers zijn vaak een essentieel onderdeel van die keten.

Organisaties moeten dus actief sturen op de risico's die ontstaan door afhankelijkheden van leveranciers:

- Weten wie toegang hebben tot kritieke systemen die bij een clouddienst staan.
- Contractueel vastleggen wie wat gaat doen bij incidenten.
- Inzicht hebben in welke onderleveranciers, toegang hebben tot de clouddienst en welke datalocaties worden gebruikt door die onderleveranciers.
- Een plan hebben om van leverancier te kunnen veranderen of te verplaatsen naar een eigen omgeving (exit-scenario's).

Toezicht op beveiliging van de toeleverancierskеten

De RDI beoordeeldt in haar toezicht de volgende punten:

- Of een organisatie daadwerkelijk regie uitoefent op zijn afhankelijkheden in zijn cloudketen.
- Of deze regie aantoonbaar is via contracten, audits, certificeringen en technische maatregelen.

3. Effectiviteit van beleid en procedures

Beleid op papier hebben over de beveiliging van de toeleveringsketen is niet genoeg. Het moet ook werken in de praktijk. Hoe stel je beleid op dat je kan toetsen?

- Stel concrete criteria op voor de selectie van cloudleveranciers en zorg voor periodieke evaluatie van bestaande cloudleveranciers
- Bepaal meetbare indicatoren voor risico's en dreigingen en evalueer deze regelmatig.
- Zorg voor duidelijke escalatieprocedures als er onacceptabele afhankelijkheden ontstaan in de keten.

Toezicht op effectiviteit van beleid en procedures

De RDI toetst het beleid en kijkt of een organisatie kan aantonen dat het beleid ook wordt getest en geoefend in de praktijk, oftewel wordt omgezet in concrete actie. Denk aan:

- Werkende exit-strategieën.
- Werkelijke spreiding van risico's en afhankelijkheden door gebruik te maken van verschillende leveranciers.

Digitale autonomie boven soevereiniteit

Soms lijkt het of veiligheid alleen mogelijk is met volledig nationale cloudoplossingen of cloudoplossingen binnen de Europese gemeenschap.

Maar volledige cloudsoevereiniteit is moeilijk te realiseren. Bovendien is het geen wettelijke norm. Digitale weerbaarheid is dat via de Cyberbeveiligingswet wél.
De RDI kijkt op basis van de Cyberbeveiligingswet: de controle en regie die een organisatie heeft over zijn clouddiensten is daarbij meer doorslaggevend dan de herkomst van de cloudleverancier. Zo kan een niet-Europese leverancier acceptabel zijn voor de wet, mits de risico's beheerst zijn. En kan een Nederlandse leverancier of oplossing in eigen beheer onacceptabel zijn, als die controle ontbreekt.

Soevereiniteit zonder daadwerkelijk grip op afhankelijkheden volstaat dus niet.

Focus daarom bij gebruik van clouddiensten op:

1. Risicoanalyse - Begrijp en documenteer je afhankelijkheden van de clouddienst
2. Ketenbeheer - Beheers afhankelijkheden van leveranciers via exit-strategieën en contracten en houdt zicht op de naleving van deze contracten
3. Beleidseffectiviteit - Zorg dat maatregelen ook echt werken

Dit is een uitgave van
Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Emmasingel 1 Groningen
088 - 041 60 00
info@rdi.nl
www.rdi.nl

April 2026

#wijzijnRDI