De CLOUD Act en NIS2 Soevereiniteitscheck

Tien vragen die elke organisatie met gevoelige data zichzelf moet stellen

Veel van het dagelijkse netwerkverkeer van Nederlandse organisaties loopt via clouddiensten die onder de Amerikaanse CLOUD Act vallen, vaak zonder dat iemand het doorheeft. Met de Cyberbeveiligingswet, de Nederlandse uitwerking van NIS2, die naar verwachting in 2026 van kracht wordt, wordt dat ook een compliancevraag. Loop deze checklist in vijf minuten door en ontdek je blinde vlekken.

1 Inzicht in je datastromen

- [ ] Weet je welke clouddiensten dagelijks data van je organisatie verwerken?
- [ ] Weet je in welke landen die data fysiek staat?
- [ ] Heb je een actueel overzicht van al je SaaS-leveranciers, ook de kleine?

2 Jurisdictie en CLOUD Act

- [ ] Weet je welk deel van je dataverkeer onder Amerikaanse jurisdictie valt?
- [ ] Gebruik je Microsoft 365, Google Workspace of vergelijkbare diensten voor gevoelige gegevens?
- [ ] Heb je in beeld welke data buitenlandse autoriteiten in theorie kunnen opvragen?

3 NIS2 en compliance

- [ ] Weet je of je organisatie onder NIS2 valt, direct of via je keten?
- [ ] Heb je je leverancierskеten in beeld? Een groeiend deel van de incidenten loopt via toeleveranciers en dienstverleners.
- [ ] Kun je bij een audit aantonen waar je data naartoe gaat?

4 Regie en alternatieven

- [ ] Heb je EU-soevereine alternatieven overwogen voor je belangrijkste diensten?

De uitkomst

Drie keer of vaker **nee** of **weet ik niet**? Dan zit er een blinde vlek op precies de plek waar het risico zit. Het goede nieuws is dat dit meetbaar is.

Je hebt dit nu op gevoel ingevuld. Wil je weten hoe het echt zit?

Een checklist op gevoel is een eerste indicatie, geen meting. SoevereinProbe meet binnen twee weken hoeveel van je data daadwerkelijk onder de CLOUD Act valt, met exacte cijfers in plaats van aannames. Dat is precies het verschil tussen denken dat het goed zit en het weten.

Vraag de scan aan

www.soevereinprobe.nl

Bron: ENISA Threat Landscape 2025. ENISA noemt geen los percentage voor de keten, maar wel als een van de snelst groeiende routes voor incidenten.