Soevereiniteit in de praktijk

Maart 2026

SCHUBERG PHILIS

Management samenvatting

Vorig jaar publiceerden wij de Whitepaper 'Control by Design: het soevereiniteitsspectrum'. Hierin positioneerden wij digitale soevereiniteit als strategische noodzaak. In dit whitepaper beschrijven wij a.d.h.v. een case study hoe deze noodzaak vertaald kan worden naar een tastbare oplossing.

Het document bevat 4 onderwerpen om het proces van strategie tot operatie te realiseren:

1. **Van bewustwording naar actie:** Waar 2025 focuste op bewustwording van de enorme afhankelijkheid van Amerikaanse Big Tech, is 2026 een jaar van transformatie. In het coalitie akkoord zijn diverse maatregelen opgenomen om echt de stap naar Nederlandse / Europese alternatieven te maken. Ook de invoering van Wero als Europees alternatief (European Payments Initiative) voor betalingen is een voorbeeld van de mogelijkheden om daadwerkelijk een hoger niveau van soevereiniteit te behalen.
2. **Van theorie naar praktijk – Case study:** Soevereiniteit bereik je niet door simpelweg voor een bepaald type cloud of platform te kiezen. Het vraagt om expert keuzes op vele verschillende thema's zoals interoperabiliteit, encryptie, leveranciersafhankelijkheid en de governance van datastromen door de gehele stack. Wij hebben deze cyclus doorleeft en delen onze bevindingen in de case study.
3. **Geleerde lessen tijdens de realisatie:** Het nastreven van een hoger niveau van soevereiniteit gaat vaak ten koste van andere aspecten, zoals tijd van idee tot realisatie, niveau van automatisering, security, of gebruiksvriendelijkheid. Dankzij onze jarenlange ervaring met missie kritische dienstverlening in vitale sectoren hebben wij deze schijnbare tegenstrijdigheid weten te doorbreken. Wij delen onze belangrijkste lessen hier zodat Nederland verdere stappen kan zetten naar een hoger niveau van digitale soevereiniteit
4. **Waarde voor besluitnemers:** In tijden van geopolitieke onzekerheid is het cruciaal om grip te hebben op continuïteit, te kunnen versnellen zonder de veiligheid te compromitteren, flexibel te blijven en volledig inzicht te hebben in digitaal verkeer. Eigenaren van maatschappijkritische processen in het publieke domein dragen de verantwoordelijkheid om dit voor Nederland te waarborgen.

Wij streven ernaar om met dit document een hoger niveau van digitale soevereiniteit in maatschappijkritische processen te helpen realiseren.

1

Van bewustwording naar actie

Het jaar 2025 stond in het teken van bewustwording van een nieuwe geopolitieke werkelijkheid. Een werkelijkheid waarin de trans-Atlantische betrekkingen met Amerika bekoeld zijn. De presentatie van de nieuwe nationale veiligheidsstrategie (NSS) bevestigde dat Amerika niet langer wenst op te treden in de geest van de Pax Americana. Hierin trad Amerika op als hoeder van de liberale wereldorde, waarin internationale organisaties en militaire bondgenootschappen krachtige afschrikwekkende middelen waren voor internationale conflicten. Amerika focust (geheel in lijn met de Make America Great Again en America First slogans) op haar eigen invloedssfeer, en schuwt niet om ongekende (militaire en economische) druk uit te oefenen op mede NAVO landen. Momenteel zijn economische maatregelen zoals 10% hogere importtarieven voor Europa al van kracht.

Deze koerswijziging van Amerika vindt plaats in een tijd waarin er na een periode van 80 jaar relatieve vrede en stabiliteit een grootschalige oorlog woedt op Europees grondgebied. Naast de Russische invasie van Oekraïne is er momenteel ook sprake van het 'Davidson window', de periode waarin militaire analisten anticiperen op het verkrijgen van controle van Taiwan door China.

Deze, door anti globalisering, ontwrichting van internationale normen en scepticisme ten opzichte van traditionele bondgenoten, gekenmerkte nieuwe wereldorde leidt tot het herzien van voorheen hoogst onwaarschijnlijke, zo niet onmogelijk geachte, scenario's. Het blokkeren van een online dienst en data, het invoeren van torenhoge tarieven op het reguleren van Big Tech dienstverlening, en het afdwingen van opgave van NAVO grondgebied op basis van militaire (on)macht zijn allen voorbeelden waar Nederlandse overheidsinstellingen rekening mee moet houden.

In 2025 zagen wij Nederlandse overheidsinstellingen al de eerste stappen ondernemen om deze afhankelijkheid te doorgronden, en waar mogelijk te verlagen. Zo startten in 2025 bijvoorbeeld de training van GPT-NL en is de Visie – Digitale autonomie en soevereiniteit van de overheid geaccordeerd. Wij onderschrijven met klem de laatste zin in deze visie: *'Nu is het moment om te handelen'*.

Schuberg Philis is in 2025 ook op meerdere punten begonnen met handelen. Zo ondersteunden wij onze klanten bij het analyseren van de weerbaarheid van IT ecosystemen, brachten wij risico's in kaart gerelateerd aan digitale soevereiniteit, en maakten wij architectuur keuzes om de controle en autonomie bij onze klanten in de vitale sectoren te verhogen. Ook is onze jarenlange kennis van het ontwikkelen en beheren van missie kritische dienstverlening toegepast in het opzetten van een autonome cloud. Op basis van deze ervaringen met missie kritische dienstverlening is ons Sovereignty Operating Framework ontwikkeld.

Naast het ondersteunen van onze klanten in het soevereiniteitsvraagstuk realiseren wij ook binnen Schuberg Philis een hoger niveau van soevereiniteit. Dit doen wij o.a. door het uitvoeren van Proof of Concepts om onze sbp.cloud oplossing nog wendbaarder en weerbaarder te maken. Het neerzetten van een adaptieve architectuur is het uitgangspunt.

2

Van theorie naar praktijk – Case study

Context en vraag

Een klant in de vitale infrastructuur vroeg om een cloudomgeving die blijft functioneren wanneer de internetverbinding doelbewust wordt verbroken. De achterliggende bestuursvraag: Hoe kunnen wij de IT-snelheid binnen OT behouden zonder veiligheidsconcessies, met volledige regie over data, sleutels, platform en toegang? Concreet vertaald naar: "Bouw een cloud waar we de internetstekker uit kunnen trekken, terwijl de operatie door moeten blijven gaan."

Deze opdracht raakte aan verschillende aspecten van de uitdagingen rondom soevereiniteit: niet alleen voldoen aan wet- en regelgeving, maar juist handelingsvrijheid borgen bij verstoringen of beleidswijzigingen buiten de eigen invloedssfeer.

Onze aanpak: Plan – Build – Run

Wij maakten gebruik van onze bewezen Plan – Build – Run aanpak. De klant bracht ons een opgesteld High-Level Design waar de cloudomgeving aan diende te voldoen. Dit document vormde een belangrijk startpunt voor de samenwerking richting een daadwerkelijk omgeving die voldeed aan de gestelde eisen.

Plan

Het datacenter is opnieuw ontworpen vanaf het netwerk, via storage en virtualisatie naar platformdiensten (zoals authenticatie, autorisatie en sleutelbeheer). Een cloudomgeving bouwen met een operatie die door moet gaan zonder internetverbinding, beïnvloedt het ontwerp op vele facetten. Zo dient er bijvoorbeeld rekening gehouden te worden met de verschillende type licenties (SaaS – perputual – open source), maar ook met de juridische basis en eigenaarschap van de licenties.

Build

Het datacenter is ingericht conform het design in de Plan fase. Per laag kozen wij voor technologie waarop het team aantoonbare kennis had; waar nodig is gericht geëxperimenteerd met nieuwe of additionele technologische oplossingen. De cloudomgeving is eerst zonder klantdata in onze eigen cloudomgeving (sbp.cloud) opgebouwd. Het beheer en de configuratie van de infrastructuur is volledig geautomatiseerd met gebruik van Infrastructure as Code. Daardoor kan dezelfde omgeving in weken herbouwd worden in het doel-datacenter. Dit resulteert in snelheid in de bouwfase, en portabiliteit in de beheerfase.

De oplossing bestaat uit bewezen bouwblokken die samen een autonoom, airgapped platform vormen.

- **Identity & Access**
  Eigen IAM (bijv. Keycloak) voor authenticatie en autorisatie. Geen afhankelijkheid van externe SaaS-diensten

- **Gelaagde, veilige toegang op afstand:**
  Vanuit een gevalideerde laptop → VPN naar firewall → BeyondTrust → authenticatie via eigen IAM → bastion → pas daarna toegang tot de geïsoleerde omgeving

- **Cryptografie & sleutelbeheer**
  Eigen PKI met HSM's; streng beheer van rootcertificaten en sleutelmateriaal. Dit voorkomt externe sleutelafhankelijkheden en maakt trust chains auditeerbaar

- **Netwerk en segmentatie**
  Datacenter-grade netwerk met hoge bandbreedte, microsegmentatie en policy enforcement. Niet vertrouwen op publieke-cloud services, maar eigen controle over routing, filtering en egress

- **Compute & platform**
  Combinatie van virtual machines en Kubernetes; uitrol met Infrastructure as Code (o.a. Terraform/Ansible) en CI/CD, beheer via Configuration Management (Ansible) en GitOps (FluxCD). Hiermee blijven workloads portabel en reproduceerbaar

- **Storage & back-up**
  Enterprise storage met onafhankelijke back-ups en herstelprocedures. Geen verplichte verbindingen naar leverancierssystemen. Herstel is aantoonbaar en herhaalbaar

- **Zichtbaarheid & security**
  Volledige zichtbaarheid op verkeer en gedrag van workloads (tot op Kubernetes-podniveau), logging/metrics/tracing onder eigen regie. Afwijkingen worden gelogd en gekoppeld aan OT/SOC-processen

- **Beschikbaarheid en weerbaarheid**
  Multi-datacenter high availability: twee primaire locaties en een derde witness-locatie om split-brain te voorkomen en de "single-source-of-truth" te borgen .

- **Hybride inzet:** mogelijk in lokale datacenters en/of VPS-omgevingen; delen van het platform kunnen gevirtualiseerd worden afhankelijk van de gewenste autonomie

Impact van ontwerpkeuzes op het spectrum van soevereiniteit

- **Autonomie boven afhankelijkheid:** door eigen IAM, PKI, logging en netwerk te beheren, ontstaat feitelijke controle over toegang, sleutels, data en operationele telemetrie. Juridische risico's van extraterritoriale claims of licentievoorwaarden worden zo gemitigeerd
- **Portabiliteit als exit-strategie:** alles is code en draait op bewezen binaries, waardoor herbouw in andere datacenters planbaar is (orde van weken). Dit is de basis voor een geloofwaardige exit- en continuïteitsstrategie
- **Observability = handelingsvrijheid:** volledige zichtbaarheid maakt het mogelijk om te monitoren, blokkeren of extra te controleren zonder derde partijen. Dat vergroot de bestuurbaarheid van risico's en de snelheid van respons bij incidenten
- **IT-snelheid in OT-context:** moderne engineeringpraktijken (CI/CD, IaC, microsegmentatie, geautomatiseerde security) binnen een strikt gecontroleerde, geïsoleerde omgeving. Zo versnelt de vernieuwing zonder dat veiligheid of beschikbaarheid in het geding komt
- **Licentie- en leveranciersrisico's managen:** open source heeft de voorkeur vanwege vrijheid en onafhankelijkheid, maar vereist licentie due-diligence (bijv. wijzigingen bij Red Hat/CentOS). Waar closed source nodig is, toetsen we of airgapped draaien mogelijk is (zonder verplichte externe licentiechecks). Hiermee voorkom je "lock-in via de achterdeur"

Behaalde resultaten

1. **Continuïteit onder eigen regie:** de omgeving blijft functioneren bij internetuitval; kritieke bedrijfsprocessen draaien door in een volledig geïsoleerde modus
2. **Hoge beschikbaarheid:** twee primaire datacenters + witness-locatie voorkomen split-brain en borgen dataconsistentie
3. **Volledige observability:** 100% inzicht in digitaal verkeer, met de mogelijkheid om te loggen, blokkeren en aanscherpen waar nodig, zonder externe afhankelijkheden
4. **Portabiliteit:** dankzij automation-first is herbouw in het doel-datacenter in weken mogelijk; experimenteren gebeurt veilig in sbp.cloud zonder klantdata
5. **IT/OT-convergentie:** snelheid en wendbaarheid van IT vertaald naar OT, met behoud van klassieke veiligheidsprincipes

Met deze referentieaanpak realiseerde Schuberg Philis een autonoom, airgapped platform dat soevereiniteit concreet maakt: minder afhankelijkheden, meer handelingsvrijheid en aantoonbare continuïteit – precies de impact die ertoe doet in het publieke domein.

3

Geleerde lessen tijdens de realisatie

De geleerde lessen uit het realiseren van een autonome cloud zijn talrijk. Om deze lessen te ordenen, herhaalbaar te maken, en breder bij onze missie kritische klanten in te kunnen zetten zijn deze opgenomen in ons Sovereignty Operating Framework.

Uit onze ervaringen is een belangrijk inzicht naar voren gekomen: Er is geen one-size-fits-all antwoord op de uitdaging van digitale soevereiniteit.

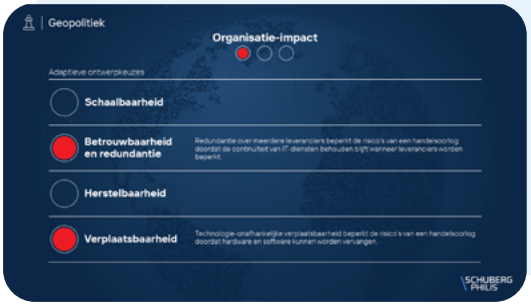
Er zijn vele verschillende scenario's, ieder met een eigen impact en oplossingsrichting. Publieke instituties zijn daarmee verplicht om iets anders na te streven dan oplossing X of Y. Ons Sovereignty Operating Framework begeleidt besluitnemers in het doorleven van de verschillende scenario's, om vervolgens strategische ontwerpkeuzes te kunnen maken. En het beste ontwerp is dat wat blijft werken, juist wanneer de wereld onvoorspelbaar wordt.

Het Sovereignty Operating Framework start met het toetsen van weerbaarheid en wendbaarheid van de architectuur op basis van verschillende scenario's. Deze scenario's zijn uitgewerkt rondom 4 thema's:

- Geopolitiek
- Juridisch
- Natuurrampen
- IT leverancier en sourcing risico's

Verschillende scenario's onder deze 4 thema's zijn uitgewerkt in een kaartspel. Het spel maakt soevereiniteit voor het bestuur, (IT) Management teams en security teams tastbaar. Het behandelt verschillende scenario's, classificeert de impact op de organisatie en vertaalt deze door naar één van de vier pijlers van ontwerpkeuzes, leidend tot een adaptieve architectuur. De vier keuzes voor het realiseren van een wendbare architectuur ontwerpkeuzes hebben betrekking op:

- Schaalbaarheid
- Betrouwbaarheid & Redundantie
- Herstelbaarheid
- Portabiliteit



Een voorbeeld:
Thema: Geopolitiek
Risico scenario: Escalerende handelsoorlog, verbod op verschillende leveranciers, hardware en software
Bedrijfsimpact: Mate van verstoring van de bedrijfsfuncties is afhankelijk van het type organisatie en AS IS architectuur
Wendbare ontwerpkeuzes: Betrouwbaarheid en redundantie & portabiliteit.

Betrouwbaarheid en redundantie kan in het ontwerp meegenomen worden d.m.v. een multi-vendor strategie. Gedacht kan worden aan het overeenkomen van contracten met meerdere derde partijen, uitwijkmogelijkheden, en door het reserveren van extra capaciteit.

Voeg naast deze maatregelen een hoog niveau van portabiliteit toe en het resultaat is een architectuur die eenvoudig switcht naar leveranciers, hardware en software die niet getroffen zijn door het opgelegde verbod. Dit kan bijvoorbeeld door open standaarden af te dwingen, een bewezen exit strategie en termijn op te nemen, en de infrastructuur zoveel mogelijk in te richten middels code.

Een andere geleerde les in het uitvoeren van soevereiniteit in de praktijk, is de nuance in het ‘open source tenzij’ uitgangspunt. Er is een uitgesproken voorkeur voor open source in het realiseren van digitale soevereiniteit, vanwege de vrijheid en onafhankelijkheid. Tegelijk is licentie-due diligence cruciaal: sommige “open” projecten wijzigden licenties of voorwaarden, wat alsnog afhankelijkheid of lock-in veroorzaakte (bijv. wijzigingen rond CentOS/Red Hat en Terraform). Dit vraagt om kritische evaluatie en, waar nodig, herijking van technologie (bijv. overstappen naar Debian).

Een hoog niveau van soevereiniteit realiseren kan ook met inzet van closed source. Enkele belangrijke afwegingen voor het gebruik van closed source: toetsen of de software volledig geïsoleerd kan draaien (airgapped), zonder verplichte externe licentiechecks of verbindingen.

Het inzetten van closed source kan als het ecosysteem autonoom kan blijven functioneren, er transparantie is over de gebruikte binaries en de afhankelijkheden beheersbaar blijven.

4

Waarde voor besluitnemers

Nederlandse publieke instanties zijn aan zet om de vereiste verhoging van digitale soevereiniteit te realiseren. Om deze transitie succesvol te doorlopen, moeten besluitnemers de strategische afwegingen maken welke risico's en maatschappelijke impact onacceptabel zijn. Daartegenover staat dat besluitnemers ook rekening moeten houden welke kosten maatschappelijk aanvaardbaar zijn.

Wat dit betekent voor bestuurders

- **Maak expliciete soevereiniteitskeuzes:** welke data, workloads en platformonderdelen móeten onder eigen regie? Leg dit vast in scenario's en stuur op handelingsvrijheid, niet alleen op compliance
- **Investeer in control-by-design:** eigen sleutelbeheer, identity, observability en portabiliteit zijn geen add-ons, maar basisfuncties van een soeverein platform
- **Vraag naar exit en herhaalbaarheid:** eis "alles als code", onafhankelijke back-ups en een aantoonbare herbouwstrategie. Dit maakt soevereiniteit tastbaar en auditeerbaar

De doelstelling van publieke instituties moet zijn: Realiseer een adaptieve architectuur die weerbaar en wendbaar is in een chaotische geopolitieke wereld. Nu is het moment om te handelen.

Addendum

Bronnen en referenties

Dit whitepaper is gebaseerd op een combinatie van eigen onderzoek, wet- en regelgeving, expertinterviews en doorlopende marktobservaties. Belangrijke bronnen zijn onder meer:

Juridische en regelgevende kaders:

- U.S. CLOUD Act (2018)
- U.S. Patriot Act (2001)
- FISA Sectie 702
- Richtlijn (EU) 2022/2555 (NIS2-richtlijn)
- Digital Operational Resilience Act (DORA)

Markt- en sectorontwikkelingen:

- Wero – Europees Digitaal Betaalsysteem
- EuroStack – Realiseer Europese digitale autonomie d.m.v. Europese Industrieel Beleid

Publieke rapporten en expertanalyses:

- National Security Strategy 2025
- Aan de slag – Coalitieakkoord 2026-2030
- Persberichten en regulatoire roadmaps van de Europese Commissie
- EuroStack Industry Initiative – A proposed framework for a "Buy European" regulation of strategic digital procurement

Input van experts en praktijkinzichten:

- Interne workshops en interviews met klanten en partners van Schuberg Philis in de sectoren financiën, energie en publieke infrastructuur
- Ronde tafels over soevereiniteit en cybersecurity, gehouden in 2024 en 2025

Ervaring en methodologie van Schuberg Philis:

- Sovereignty Operating Framework (SOF)
- Control by Design: The sovereignty spectrum – whitepaper juni 2025
- Inzichten uit missie-kritieke projecten onder EU- en sectorspecifieke compliancekaders

Deze bronnen zijn gebruikt om bevindingen te onderbouwen, analyses te verrijken en de methodologie van het Sovereignty Operating Framework zoals toegepast in dit paper, vorm te geven.

Soevereiniteit in de praktijk

SCHUBERG PHILIS