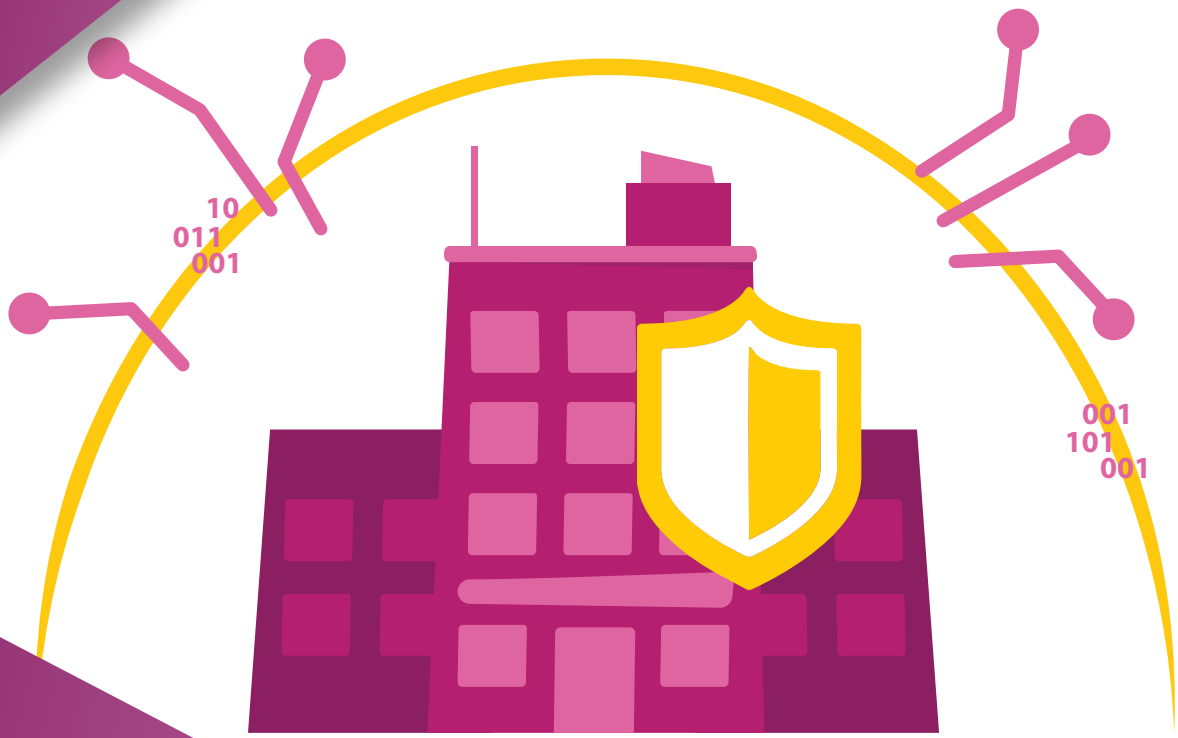
Digitale autonomie in de praktijk: van afhankelijkheid naar regie



Proloog

Het is 2022. Het is de periode kort voorafgaand aan de invasie van Rusland in Oekraïne. In een vergaderzaal in Kyiv, neemt de Oekraïense Minister van Digitale Transformatie, Mykhailo Fedorov, een beslissing die in vredestijd ondenkbaar zou zijn. Alle overheidsdata, van Belastingdienst tot Defensie, van Bevolkingsregisters tot diplomatieke communicatie — moet onmiddellijk naar de cloud. Niet over zes maanden. Niet na een zorgvuldig migratietraject. Nu.

Het Parlement past in recordtempo de wet aan. President Zelensky ondertekent de Wet op Cloud Services op 15 maart 2022[1]. Microsoft zet in de weken rond de invasie de data van vrijwel alle ministeries over naar Azure datacenters verspreid over Europa. De rekening loopt op tot boven de 400 miljoen dollar.

Op 24 februari 2022, enkele uren voor de eerste raketinslagen, detecteert het Threat Intelligence Center van Microsoft een massale golf cyberaanvallen op Oekraïense overheidsinfrastructuur.[2] Door de snelle waarschuwing en de schaalbaarheid van de cloud wordt de aanval geneutraliseerd. Wanneer Russische raketten kort daarna de fysieke overheidsdatacenters treffen, is de schade beperkt tot beton en staal. De data is al weg. De Oekraïense overheid blijft online. En operationeel.

Het is een van de meest indringende lessen uit de digitale geschiedenis van de afgelopen jaren. Niet omdat Oekraïne alles goed deed — de afhankelijkheid van één Amerikaanse techgigant, de CLOUD Act die op de achtergrond meespeelt, de vendor lock-in die zich voor jaren heeft vastgezet — maar omdat het zo ontzettend duidelijk maakt waar de echte kwetsbaarheid zat. Niet in de cloud, maar in de servers op eigen bodem. In de illusie dat fysieke aanwezigheid gelijkstaat aan controle.

Digitale soevereiniteit, zo bleek die februarimaand in 2022, is geen kwestie van waar je data staat. Het is een kwestie van wie erbij kan, of je kunt blijven functioneren als een leverancier wegvalt, en of je de sleutels in eigen hand hebt op het moment dat het er werkelijk toe doet.

We leven in een geopolitiek roerige tijd. De afhankelijkheid van Europese organisaties van internationale technologieplatformen staat volop ter discussie. In boardrooms, in Den Haag, in Brussel. De toon is er één van zorg, soms van urgentie, en te vaak van verlamming. Want de vraag “wat moeten we doen?” blijft zonder bevredigend antwoord zolang digitale soevereiniteit wordt behandeld als een politiek of juridisch vraagstuk in plaats van als wat het werkelijk is: een security en weerbaarheidsuitdaging.

En dat is precies waar dit whitepaper over gaat. Niet over het verlaten van de Amerikaanse cloud. Niet over een terugkeer naar servers in eigen kelders. Maar over de vraag die bepaalt wie er werkelijk bij de data kan. Over de architectuur die bepaalt of jouw organisatie blijft functioneren als een leverancier wegvalt — en die verder gaat dan herstel alleen, naar een adaptieve inrichting die omschakelt in plaats van instort. Over de sleutels — letterlijk en figuurlijk — die bepalen of je in control bent.

Voor CISO’s en andere security adviseurs is dit het moment om de handschoen op te pakken. De politieke en bestuurlijke urgentie rond digitale soevereiniteit versterkt de business case voor investeringen in data security en weerbaarheid op een manier die zelden eerder zo helder was. Wie nu de verbinding legt tussen de soevereiniteitsdiscussie en de security agenda, vergroot niet alleen de digitale weerbaarheid van zijn organisatie, maar neemt ook de regie in een debat dat te lang zonder technische stem is gevoerd.

Dit whitepaper beschrijft hoe.

Deze proloog gebruikt publiek beschikbare informatie om een mechanisme te illustreren. Exacte details aantallen, timing en inrichting kunnen per bron en context verschillen.

Dit whitepaper is opgesteld als algemene informatievoorziening en biedt handvatten voor organisaties die meer inzicht willen krijgen in digitale autonomie en soevereiniteit. Met deze whitepaper beoogt de projectgroep Digitale Autonomie van Cyberveilig Nederland bij te dragen aan een gedeeld begrip en handelingsperspectief op hoofdlijnen. Het document is nadrukkelijk niet bedoeld als juridisch, beveiligings- of ander professioneel advies, noch een uitputtende beschrijving van alle toepasselijke wet- en regelgeving of best practices.

In dit whitepaper wordt op meerdere plaatsen de term ‘Europees’ of ‘Europese’ gebruikt als verkorte aanduiding voor de Europese Unie (EU) of EU-gerelateerde onderwerpen, zoals EU wet- en regelgeving en EU-beleid.

Welke maatregelen noodzakelijk, proportioneel en effectief zijn, hangt onder meer af van de sector en wettelijke context, het organisatietype, risicoprofiel, gegevenscategorieën, kritische processen, leveranciersketen en de concrete (technische en organisatorische) inrichting van de organisatie. Het wordt organisaties aangeraden om voor nadere toepassing in de eigen situatie passende expertise in te schakelen. Dit whitepaper helpt met de concretisering van de vraagstelling.

1. Wet van Oekraïne ‘On Cloud Services’ [15 maart 2022], No.2075-IX https://zakon.rada.gov.ua/laws/main/2075-20#Text

2. Defending Ukraine: Early Lessons from the Cyber War

Inhoud

Samenvatting

Er is een groeiende behoefte bij Nederlandse organisaties aan inzicht in afhankelijkheden, risico's en strategische keuzes op het gebied van digitale autonomie en digitale soevereiniteit bij het gebruik van hardware, software en digitale diensten. Cyberveilig Nederland heeft dit whitepaper geschreven om deze organisaties inzicht, overzicht en handvatten te bieden om deze vraagstukken beter te begrijpen en te adresseren.

Digitale autonomie gaat over het vermogen om zelfstandig keuzes te maken in het digitale domein, terwijl digitale soevereiniteit zich richt op juridische en bestuurlijke controle. Beide hebben invloed op de mate van weerbaarheid van een organisatie en bevinden zich op een spectrum, waarbij het aan organisaties is om bewust een positie te kiezen die past bij hun risico's en afhankelijkheden. Concreet zijn in het kader van digitale autonomie en soevereiniteit de volgende drie typen dreigingen relevant:

- Vertrouwelijkheid van data, infrastructuur en diensten;
- Integriteit van data, infrastructuur en diensten;
- Beschikbaarheid van data, infrastructuur en diensten.

Momenteel creëert met name het geopolitieke klimaat onzekerheid over de wijze waarop staten hun invloed in de toekomst hierop zouden kunnen inzetten. Dit betekent echter niet dat dergelijke risico's uitsluitend samenhangen met de jurisdictie(s) waarin een leverancier opereert. Ook de mate waarin organisaties aantoonbare regie hebben over toegang, sleutelbeheer, auditability en continuïteit speelt een belangrijke rol.

Europese wetgeving stuurt daarbij ook niet op volledige onafhankelijkheid, maar op het bewust beheersen van digitale afhankelijkheden door het afdwingen van transparantie, risicobeheersing en ketenregie. Dit maakt dat internationale dienstverlening juridisch mogelijk blijft, terwijl passende beheersmaatregelen de feitelijke controle waarborgen. Daarmee verschuift het debat van "soevereiniteit" naar "aantoonbare controle": welke technische en organisatorische maatregelen maken risico's acceptabel én aantoonbaar beheerst (verifieerbaar)? Er worden steeds meer oplossingen ontwikkeld door grote cloudleveranciers die proberen hieraan tegemoet te komen. Toch vereist digitale autonomie meer dan alleen technologische voorzieningen. Het inrichten van eigen technische, organisatorische en contractuele maatregelen blijft noodzakelijk om regie te behouden.

Daarbij vormen de dreigingen die voortkomen uit onze digitale afhankelijkheden geen nieuwe categorie risico's, maar een nieuwe uitingsvorm van bekende securityvraagstukken. Wat het nu anders maakt is de politieke en bestuurlijke context die het nemen van aanvullende (beheers)maatregelen nodig maakt. Denk hierbij aan encryptie met onafhankelijk sleutelbeheer, een adaptieve (netwerk)architectuur en een onafhankelijke herstelomgeving. Dit pleit dan ook niet tegen internationale leveranciers op zichzelf. Integendeel: internationale technologie kan uitstekend passen binnen deze benadering. Het gaat om de technische en organisatorische beheersmaatregelen. Deze moeten aantoonbaar op orde zijn en organisaties moeten actief sturen op afhankelijkheden.

Aantoonbare regie, dat is waar digitale autonomie in de praktijk om draait.

Inleiding en aanleiding

Wij migreren steeds meer van onze on-premise IT-functies naar cloud-gebaseerde alternatieven bij Amerikaanse bedrijven. Is dat nog wel verstandig? Moeten we daarmee stoppen?

Wij kopen hardware en/of software van een leverancier buiten de EU die in de huidige geopolitiek wordt gezien als een hoog-risico jurisdictie, is dat riskant? Moeten we iets anders doen, of ergens rekening mee houden?

Dit zijn enkele voorbeelden van de vele vragen die organisaties in Nederland stellen aan hun cybersecurityleveranciers. Het laat een groeiende behoefte zien van organisaties die zoeken naar inzicht in hun afhankelijkheden en de risico's die hun strategische keuzes binnen het digitale domein mede bepalen. De (strategische) afhankelijkheden, geopolitieke ontwikkelingen en Europese wet- en regelgeving leiden tot een toename van deze vragen. Onderwerpen zoals dataverwerking, ketenafhankelijkheden en risico's bij uitbesteding zijn geen vraagstuk voor de toekomst, maar het is iets waar organisaties nu mee worstelen.

Vanuit de cybersecuritysector is onder coördinatie van Cyberveilig Nederland daarom een projectgroep gestart om organisaties te helpen bij bovenstaande vraagstukken. Deelnemende organisaties van de projectgroep zijn: Atos, Cisco, DataExpert, Defion, Fox-IT, Northwave, Schubergphilis, Sentyron en Tesorion.

Allereerst zal de theorie toegelicht worden zodat het duidelijk is wat we bedoelen met bepaalde terminologie. In het kader van digitale autonomie zijn drie dreigingen relevant die nader worden toegelicht. Bij de inrichting en inkoop van digitale diensten worden echter ook frequent juridische bezwaren opgeworpen. Daarom is het van belang om ook het juridisch perspectief te schetsen. Vervolgens zal er invulling gegeven worden aan soevereine cloud en wordt er invulling gegeven aan wat de te nemen stappen zijn. In de bijlage is een stappenplan opgenomen die organisaties kunnen gebruiken bij het nemen van maatregelen die digitale soevereiniteit en autonomie in de praktijk borgen.

Digitale weerbaarheid, soevereiniteit en autonomie

In dit hoofdstuk ordenen en beschrijven we beknopt de begrippen digitale weerbaarheid, digitale autonomie en digitale soevereiniteit en hoe zij zich tot elkaar verhouden.

DIGITALE WEERBAARHEID is het vermogen om inbreuken op de vertrouwelijkheid en integriteit van informatie, en de continuïteit van bedrijfsprocessen te voorkomen, herkennen, op te vangen en te herstellen en daarbij zo goed mogelijk te blijven functioneren. Het bewerkstelligen van digitale weerbaarheid vergt een breed palet aan waarborgen. Raamwerken als ISO27001, NEN7510 en IEC62443 voorzien in concrete meetbare maatregelen die organisaties met een risico-gebaseerde aanpak kunnen implementeren. Daarnaast hebben digitale autonomie en digitale soevereiniteit ook invloed op de mate van weerbaarheid van een organisatie.

Digitale autonomie en digitale soevereiniteit worden vaak in één adem genoemd, maar ze vertegenwoordigen twee verschillende – elkaar versterkende – perspectieven. Zie hiervoor ook de Visie Digitale autonomie en soevereiniteit van de Overheid [3] ,een document dat weliswaar voor de overheid is geschreven, maar dat ook relevant is voor bedrijven.

DIGITALE SOEVEREINITEIT richt zich op juridische en bestuurlijke controle. Het sleutelwoord is hier zeggenschap: wie bepaalt uiteindelijk de spelregels over data, systemen en infrastructuur? In essentie gaat dit over jurisdictie: onder welke wetgeving vallen systemen en informatie? We lichten dit nader toe in hoofdstuk 3. Daarmee heeft digitale soevereiniteit invloed op continuïteitsvraagstukken én vertrouwelijkheidsvraagstukken, zoals we toelichten in hoofdstuk 4.

DIGITALE AUTONOMIE gaat over het vermogen om zelfstandig keuzes te maken in het digitale domein, oftewel handelingsvrijheid. De ruimte om te beslissen, te veranderen en te sturen zonder dat externe partijen die vrijheid (zouden kunnen) beperken. De visie Digitale Autonomie en Soevereiniteit stelt dat die vrijheid bestaat uit drie aspecten:

1. technologische keuzevrijheid;
2. kennisautonomie;
3. mitigatie van strategische afhankelijkheden.

In de praktijk heeft digitale autonomie, handelingsvrijheid, grote invloed op continuïteitsvraagstukken, zoals we toelichten in hoofdstuk 4.

NIET ZWART-WIT, MAAR EEN SPECTRUM

Geen van deze begrippen zijn overigens absoluut, maar bevinden zich op een spectrum van minder naar meer weerbaarheid. Volledige digitale weerbaarheid, soevereiniteit en autonomie zijn dan ook niet per se een doel op zich. Het is aan organisaties om bewust de juiste positie te kiezen op deze schaal, passend bij de gevoeligheid van de data, het risicoprofiel en strategische afhankelijkheid. Zo kan het hebben van **minder** autonomie en **minder** soevereiniteit dóór afhankelijkheid van de cloud in bepaalde omstandigheden ook juist leiden tot **meer** weerbaarheid. Denk aan hoe een cloud migratie juist essentieel kan zijn bij het in stand houden en beveiligen van kritieke systemen en -data. Digitale soevereiniteit en autonomie gaan dan ook over bewuste regie en niet zo zeer over het terughoudend gebruikmaken van (cloud)technologie.

[3] https://open.overheid.nl/documenten/c49a2705-3f3d-44be-8a7d-2cecd2183604/file

Wat is de dreiging?

Concreet zijn in het kader van digitale autonomie en soevereiniteit de volgende drie typen dreigingen relevant:

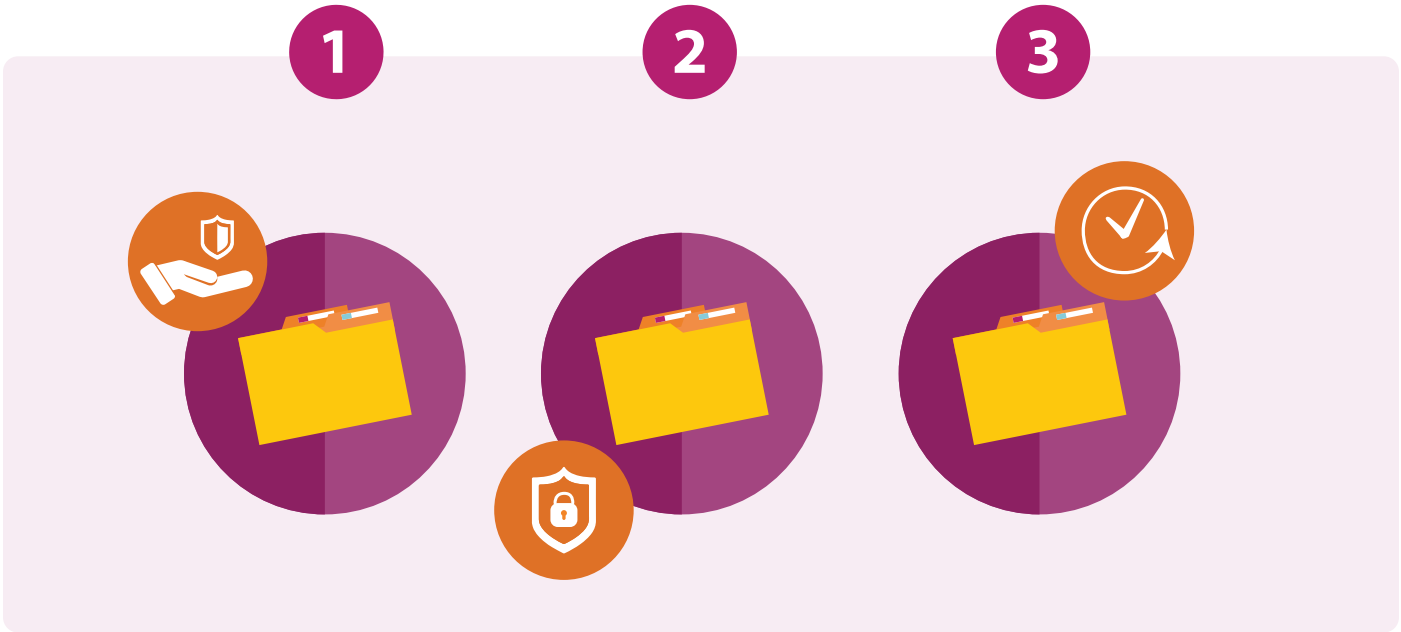
1. **VERTROUWELIJKHEID VAN DATA, INFRASTRUCTUUR EN DIENSTEN.**
Een cloudleverancier kan onder omstandigheden worden verplicht om buitenlandse autoriteiten toegang te verlenen tot gegevens waartoe hij toegang heeft.

2. **INTEGRITEIT VAN DATA, INFRASTRUCTUUR EN DIENSTEN.**
Digitale inmenging door een cloudleverancier of autoriteit kan de integriteit van informatie aantasten, wanneer data onvolledig of incorrect worden opgeslagen of gewijzigd bij gebruikt.

3. **BESCHIKBAARHEID VAN DATA, INFRASTRUCTUUR EN DIENSTEN.**
Een cloudleverancier kan (al dan niet onder druk) dienstverlening beperken of staken. Dit kan onmiddellijke consequenties hebben, maar ook gevolgen die zich later manifesteren zoals on-premise software van een leverancier waar geen updates meer op geleverd worden.

Deze dreigingen worden in de praktijk vaak als groter ervaren bij afhankelijkheid van internationale cloudleveranciers, onder meer door verschillen in wet- en regelgeving, de betrokkenheid van meerdere jurisdicties en de beperkte invloed die individuele organisaties daarop kunnen uitoefenen. Bovendien zorgt het geopolitieke klimaat voor onzekerheid over op welke wijze landen hun invloed in de toekomst zouden kunnen inzetten.

Genoemde drie kernaspecten van informatiebeveiliging: vertrouwelijkheid, integriteit en beschikbaarheid, zijn niet abstract. Ze worden zichtbaar in situaties waarin Europese overheden, publieke diensten of vitale infrastructuren afhankelijk blijken van internationale technologie. Onderstaande scenario's illustreren hoe deze dreigingen in de praktijk tot uiting kunnen komen en welke risico's deze met zich meebrengen. Deze scenario's zijn illustratief en focussen bewust op situaties met internationale afhankelijkheden, omdat daar de spanning tussen afhankelijkheid en controle vaak het meest zichtbaar wordt. Zij laten zien hoe deze dreigingen in de praktijk kunnen voorkomen en welke risico's daaruit kunnen voortvloeien.



Scenario's

De scenario's in dit hoofdstuk zijn illustratief en beschrijven mogelijke mechanismen. Zij zijn niet bedoeld als feitelijke beschrijving van specifieke gebeurtenissen of handelingen van concrete leveranciers.

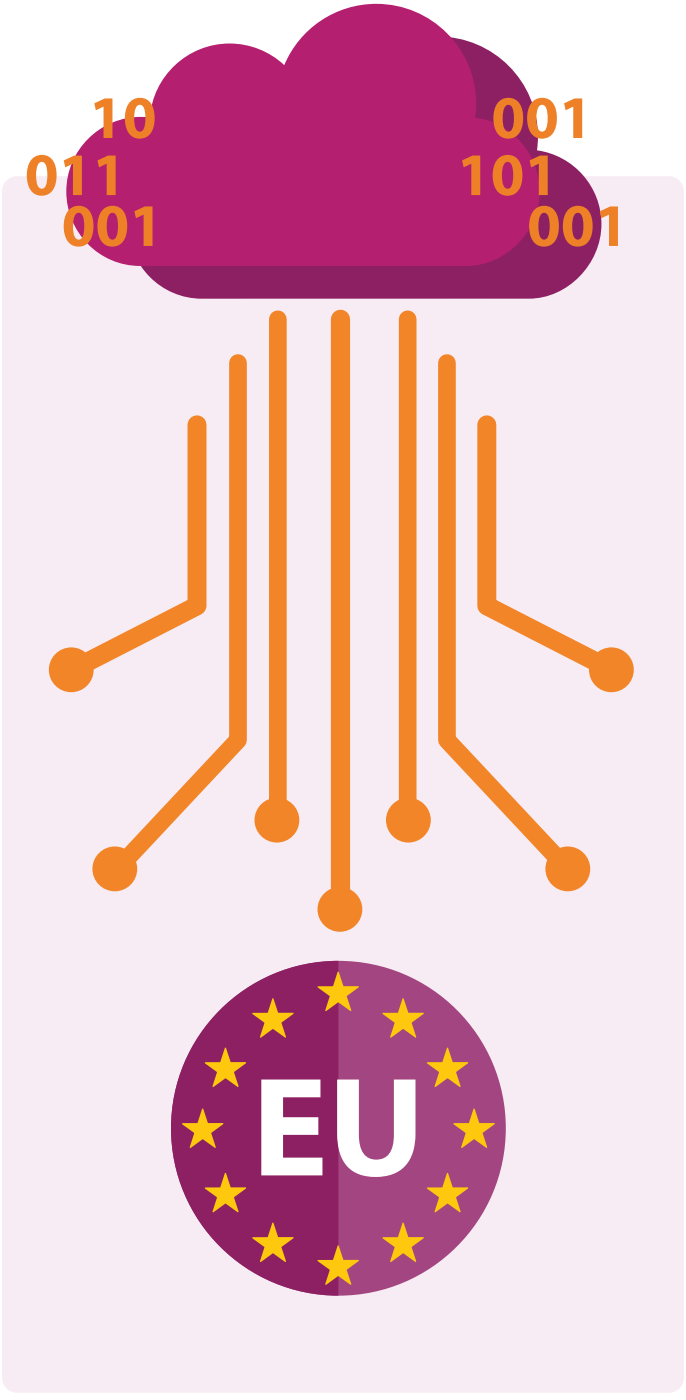
SCENARIO 1: TOEGANG TOT EUROPESE PERSOONSGEGEVENS VIA EEN AMERIKAANSE CLOUDLEVERANCIER

SITUATIE: Een Europese organisatie draait een groot deel van haar data analyse platform op een cloudomgeving van een internationale cloudleverancier. De data bevat onder andere persoonsgegevens en bedrijfsgevoelige informatie.

TRIGGER: Een Amerikaanse opsporingsautoriteit voert een onderzoek uit naar een organisatie die voorkomt in de Europese datasets. Deze vraagt via een juridisch proces gegevens op, gericht op specifieke accounts of datasets bij de cloudleverancier die onder de Stored Communications Act (SCA) valt.

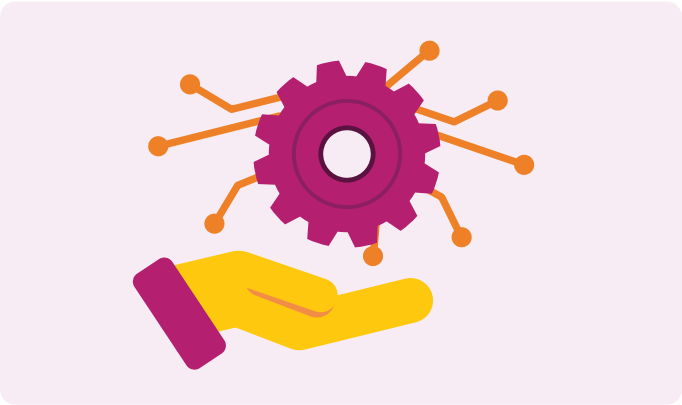
MECHANISME VAN DE DREIGING: Op basis van de CLOUD Act in combinatie met de SCA kan een Amerikaanse cloudleverancier die onder Amerikaanse jurisdictie valt, op grond van een geldig juridisch proces worden verplicht om inhoud en/of (meta)data[4] te bewaren en te verstrekken die onder zijn possession, custody or control vallen, ongeacht waar die data fysiek is opgeslagen. Het juridisch proces kan bovendien gepaard gaan met een (tijdelijk) geheimhoudings- of uitstelbevel waardoor de cloudleverancier de klant niet (direct) hierover mag informeren.

MANIFESTATIE: De cloudleverancier ontvangt een juridisch verzoek dat (tijdelijk) onder geheimhouding kan vallen. Zonder medeweten van de Europese organisatie worden bepaalde gegevens en bijbehorende informatie uit geselecteerde accounts verzameld en doorgegeven aan de bevoegde autoriteit. Een cloudleverancier kan zo'n bevel overigens onder voorwaarden wel laten toetsen of aanvechten op grond van een comity-afweging bij een conflict met buitenlands recht (zoals de AVG). In dat geval moet een Amerikaanse rechter de verschillende belangen tegen elkaar afwegen.



4. denk aan logbestanden, toegangsgegevens en communicatiepatronen

SCENARIO 2: IDENTITEITSDIENST VAN EEN EUROPESE OVERHEID DRAAIT OP EEN INTERNATIONALE IT-DIENSTVERLENER



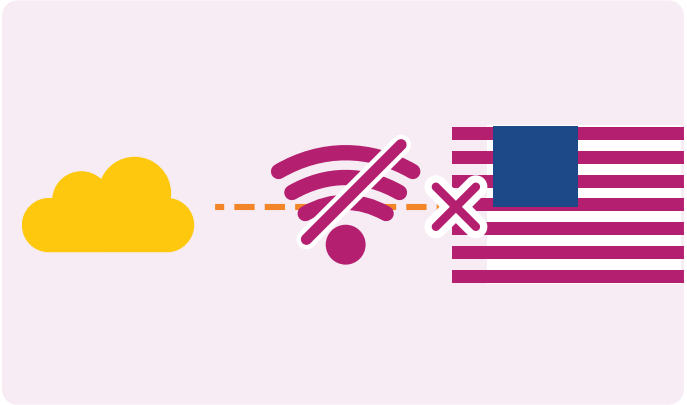
SITUATIE: Een nationale digitale identiteitsdienst, gebruikt door miljoenen burgers voor onder meer belastingaangifte, zorgportalen en gemeentelijke diensten, draait op een extern platform van een niet Europese IT dienstverlener. De leverancier beheert onder andere de authenticatie servers, PKI-componenten, logging en monitoringdiensten en (een deel van) het incidentresponsproces. De overheid heeft beperkte inzage in de onderliggende infrastructuur en is afhankelijk van de leverancier voor herstel bij storingen.

TRIGGER: In het land waar de leverancier onder valt, worden nieuwe export , sanctie- of compliance-regels gesteld (bijvoorbeeld rond cryptografische technologie). Hierdoor moeten onderdelen van de dienstverlening worden herzien, (opnieuw) worden gecertificeerd of tijdelijk worden uitgeschakeld.

MECHANISME VAN DE DREIGING: Door wettelijke of beleidsmatige eisen kan de leverancier bepaalde beveiligingsfuncties stopzetten, updates uitstellen of de dienstverlening beperken totdat aan de vereiste regels en certificeringen is voldaan. Het kan zijn dat de leverancier hierover slechts beperkt kan communiceren vanwege wettelijke restricties.

MANIFESTATIE: Binnen korte tijd vallen authenticatie servers uit, kunnen burgers niet meer inloggen bij overheidsdiensten of worden certificaten ongeldig verklaard of niet vernieuwd. Daardoor ontstaat een kettingreactie in systemen die afhankelijk zijn van de controle van identiteiten. De overheid kan de dienst niet zelfstandig herstellen als cruciale onderdelen buiten haar beheer vallen.

SCENARIO 3: ONDERBREKING VAN DIENSTVERLENING ONDER DRUK VAN DE AMERIKAANSE OVERHEID



SITUATIE: Een internationale organisatie die in Nederland zetelt maakt gebruik van een grote Amerikaanse cloudleverancier voor opslag en verwerking van gevoelige onderzoeksdata. Denk hierbij aan getuigenverklaringen, bewijsstukken, interne analyses en communicatie tussen medewerkers. Deze data is noodzakelijk voor de werkwijze van de internationale organisatie en wordt operationeel in Europa verwerkt en opgeslagen. De cloudleverancier valt wel onder Amerikaanse wet- en regelgeving.

TRIGGER: De internationale organisatie start een onderzoek naar mogelijke oorlogsmisdaden waarbij ook Amerikaanse militairen vanwege het conflictgebied in beeld komen. De politieke druk in Washington loopt op.

MECHANISME VAN DE DREIGING:
De dreiging is hier eigenlijk tweeledig:

Datatoegang: Op basis van de CLOUD Act/SCA kan de cloudleverancier, via een juridisch proces, verplicht worden om data te bewaren en/of te verstrekken die onder zijn possession, custody or control valt, ongeacht waar die data fysiek is opgeslagen.

Dienstcontinuïteit: Geopolitieke druk kan ertoe leiden dat diensten worden beperkt, support wordt opgeschort, accounts worden geblokkeerd of andere maatregelen worden genomen. Voor zover sprake is van een juridisch verzoek tot datatoegang, kan bovendien (tijdelijk) sprake zijn van uitgestelde melding richting de klant binnen voornoemd SCA-kader.

MANIFESTATIE: De cloudleverancier ontvangt een juridisch verzoek en/of interne instructies die niet direct publiek of volledig transparant zijn. Voor de internationale organisatie betekent dit in de praktijk dat bepaalde gegevens of accounts niet meer beschikbaar zijn, dat back-ups minder goed werken of dat belangrijke beheertaken vertraging oplopen. Hierdoor wordt het moeilijker om toegang te krijgen tot belangrijke informatie en kunnen onderzoeken vertraging oplopen of zelfs stilvallen. Dit heeft direct gevolgen voor de zelfstandige werking van de organisatie.

MOGELIJKE IMPACT: RODE DRAAD

De dreigingen uit de bovenstaande scenario's kunnen gevolgen hebben voor de drie belangrijkste aspecten van informatiebeveiliging: vertrouwelijkheid, integriteit en beschikbaarheid.

Vertrouwelijkheid: onbevoegden kunnen toegang krijgen tot gevoelige gegevens, zoals persoonsgegevens of staatsinformatie. Dit kan leiden tot privacyproblemen en risico's op spionage, bijvoorbeeld op het gebied van beleid, defensie of diplomatie.

Integriteit: gegevens, instellingen of toegangsrechten kunnen bewust of onbedoeld worden gewijzigd, waardoor informatie niet langer betrouwbaar is.

Beschikbaarheid: systemen of diensten kunnen uitvallen, waardoor belangrijke processen en publieke diensten, zoals zorg, uitkeringen of onderwijs, niet meer beschikbaar zijn.

Wanneer zulke verstoringen langdurig of grootschalig zijn, kunnen zij leiden tot maatschappelijke problemen en ontwrichting. De kern van deze scenario's is dat het risico niet alleen afhangt van het land waarin een leverancier gevestigd is. Belangrijker is in hoeverre een organisatie haar afhankelijkheden begrijpt, kan beïnvloeden en zo nodig kan bijsturen. Digitale soevereiniteit en autonomie kunnen daarbij helpen, maar bieden geen garantie voor de vertrouwelijkheid, integriteit en beschikbaarheid van data, systemen en diensten.

In de praktijk draait digitale autonomie vooral om goede beheersmaatregelen, zoals technische beveiliging, duidelijke contractuele afspraken en goed bestuur, afgestemd op de risico's die een organisatie bereid is te accepteren.

De scenario's laten de risico's zien. Het volgende hoofdstuk beschrijft de juridische regels en de ruimte die daarbinnen bestaat. Op basis daarvan wordt duidelijk welke maatregelen nodig zijn om internationale dienstverlening verantwoord in te zetten.

Digitale autonomie: het juridisch perspectief

Het voorgaande deel van dit whitepaper richtte zich primair op cyberdreigingen. Bij de inrichting en inkoop van digitale diensten worden echter ook frequent juridische bezwaren opgeworpen. Hierbij wordt veelal verwezen naar de autonomie- en soevereiniteitseisen in Europese wet- en regelgeving. Dat is begrijpelijk, nu geopolitiek, ketenrisico's en toezicht het ingewikkelder maken om blind te vertrouwen op technologie die niet volledig in eigen beheer is. Tegelijkertijd leiden deze termen vaak tot eisen die absoluter klinken dan wat daadwerkelijk vereist is onder bestaande wet- en regelgeving. Digitale autonomie binnen de Europese Unie ziet dan ook niet toe op volledige onafhankelijkheid, maar op het bewust beheersen van digitale afhankelijkheden en risico's. Europese wetgeving richt zich daarbij niet op het uitsluiten van internationale technologie, maar steeds meer op het afdwingen van transparantie, risicobeheersing en ketenregie.

In dit hoofdstuk worden de belangrijkste juridische kaders kort toegelicht, en wat ten aanzien van digitale autonomie van organisaties wordt verlangd bij het gebruik van (internationale) digitale diensten.[5]

Een veelgehoorde eis is: "data moet binnen de EU blijven". Die wens kan een nuttige vuistregel zijn, maar juridisch is het vaak een middel in plaats van een doel. Het doel is dat je weet wie er bij de data kan, onder welke voorwaarden, en hoe je dat controleert. Locatie kan hierbij helpen, maar garandeert niet automatisch dat toegang, logging, sleutelbeheer of exit goed geregeld zijn. Daarom is het nuttig om onderscheid te maken tussen:

- data-residentie (waar de data gehost is);
- toegangs- en jurisdictierisico (wie er, juridisch én technisch, bij kan);
- exit/portability (hoe snel en gecontroleerd je kunt migreren bij veranderende risico's of voorwaarden).

Met andere woorden: digitale autonomie gaat in de praktijk niet zozeer over harde juridische vereisten, maar meer over een set beheersmaatregelen om te toetsen, auditen en contractueel af te dwingen.

NIS2 (RICHTLIJN (EU) 2022/2555)

NIS2 is een belangrijk Europees kader voor cybersecurity. De richtlijn richt zich niet op de herkomst van technologie, maar op het beheersen van cyberrisico's. Organisaties die onder de NIS2 of de nationale implementatie daarvan vallen, moeten passende beveiligingsmaatregelen nemen, verantwoordelijkheden duidelijk beleggen, incidenten melden en risico's bij leveranciers en andere ketenpartners beheersen, in kaart brengen, beoordelen en monitoren. Daarbij moeten zij kunnen aantonen welke risico's zij accepteren, hoe zij risico's beperken en hoe zij controleren dat dit goed gebeurt.

DATAVERORDENING (VERORDENING (EU) 2023/2854, OOK WEL "DATA ACT")

Waar NIS2 zich richt op cybersecurity, gaat de Dataverordening (Data Act) onder meer over de controle die organisaties hebben over hun data en hun afhankelijkheid van leveranciers. De verordening moet het makkelijker maken om van cloudleverancier of datadienstverlener te wisselen en data tussen systemen uit te wisselen. Hierdoor krijgen organisaties meer grip op hun data en kunnen zij hun afhankelijkheden van één leverancier verminderen. Daarnaast verplicht de Data Act aanbieders van dataverwerkingsdiensten om zich te verzetten tegen onrechtmatige verzoeken van buitenlandse overheden om toegang te krijgen tot niet-persoonsgegevens die in de EU zijn opgeslagen. Hoewel dit geen volledige bescherming biedt, zorgt het wel voor extra juridische waarborgen en meer transparantie. De Data Act draagt zo bij aan digitale autonomie door organisaties meer mogelijkheden te geven om hun data te beheren, te verplaatsen en van leverancier te veranderen.

[5] Dit is een niet-uitputtende lijst van relevante wet- en regelgeving. Denk ook aan DORA, CER-Richtlijn, EU Cybersecurity Act, etc. In dit Whitepaper hebben wij getracht de naar onze mening veel voorkomende juridische bezwaren te bespreken.

ALGEMENE VERORDENING GEGEVENSBESCHERMING (OOK WEL "AVG" OF "GDPR")

De AVG stelt dat persoonsgegevens alleen aan derde landen (buiten de EER) mogen worden doorgegeven wanneer aan de voorwaarden voor internationale doorgifte is voldaan, bijvoorbeeld op basis van een adequaatheidsbesluit, passende waarborgen of een toepasselijke uitzondering. Met andere woorden: het beschermingsniveau voor betrokkenen mag niet worden ondermijnd door de doorgifte van gegevens aan derde landen.

- De Europese Commissie heeft voor een aantal landen adequaatheidsbesluiten vastgesteld. Dit houdt in dat deze landen een passend niveau van gegevensbescherming worden verondersteld te bieden. Voor doorgiften tussen de EU en de Verenigde Staten geldt het EU-US Data Privacy Framework.[6] Amerikaanse organisaties die zich hebben laten certificeren bij het U.S. Department of Commerce worden geacht een passend beschermingsniveau te bieden, waardoor doorgifte naar deze partijen onder de AVG is toegestaan. Dit neemt echter niet alle zorgen weg over mogelijke toegang door buitenlandse autoriteiten. Daarom treffen organisaties vaak aanvullende maatregelen om feitelijke controle over data te versterken.

- Passende waarborgen zijn mogelijk wanneer zo'n adequaatheidsbesluit er niet is. Zo heeft de Europese Commissie Standaardcontractbepalingen (Standard Contractual Clauses, "SCC's") gepubliceerd.[7] Deze kunnen worden gebruikt wanneer een adequaatheidsbesluit ontbreekt. In dergelijke gevallen moet worden beoordeeld of aanvullende technische en organisatorische maatregelen noodzakelijk zijn om een daadwerkelijk gelijkwaardig beschermingsniveau te borgen.

De AVG verbiedt internationale doorgifte van gegevens niet, maar vereist wel een goede risicoanalyse en passende contractuele, technische en organisatorische maatregelen. Ook schrijft de AVG onder bepaalde voorwaarden voor dat organisaties hier contractuele afspraken over moeten maken.

BEPERKINGEN CLOUD ACT

In discussies over digitale soevereiniteit wordt vaak verwezen naar de CLOUD Act. Deze Amerikaanse wet kan bepaalde Amerikaanse dienstverleners verplichten om gegevens te verstrekken, ook wanneer die buiten de Verenigde Staten zijn opgeslagen. Het is daarbij belangrijk om te weten dat de CLOUD Act geen onbeperkte toegang tot gegevens geeft. Verzoeken moeten verlopen via wettelijke procedures en zijn gericht op specifieke accounts of datasets. De CLOUD Act creëert daarmee op zichzelf geen generieke,massale of automatische toegang tot gegevens. Daarnaast kunnen Amerikaanse dienstverleners op grond van een comity-afweging een verzoek aanvechten wanneer dit in strijd is met de wetgeving van een ander land, zoals de AVG. In dat geval moet een Amerikaanse rechter de verschillende belangen tegen elkaar afwegen. Een dienstverlener kan bovendien alleen worden verplicht gegevens te verstrekken waarover hij daadwerkelijk beschikt of waartoe hij toegang heeft. Als diensten zo zijn ingericht dat de leverancier geen toegang heeft tot de leesbare gegevens van klanten, kan dit de toegang tot de leesbare inhoud op grond van de CLOUD Act in de praktijk beperken, al kan verstrekking van versleutelde gegevens of metadata afhankelijk van de feitelijke inrichting nog steeds aan de orde zijn. Technische maatregelen zoals end-to-end encryptie, klantbeheerde encryptiesleutels (Hold Your Own Key) en zero-access-architecturen kunnen hierbij een belangrijke rol spelen.

Hoewel de CLOUD Act vooral betrekking heeft op toegang tot gegevens, kunnen de bredere juridische en geopolitieke omstandigheden ook gevolgen hebben voor de beschikbaarheid van diensten. Bijvoorbeeld wanneer sancties, nalevingseisen of interne risicobeoordelingen leiden tot beperkingen of opschorting van dienstverlening.

Voor zover bekend worden verzoeken op basis van de CLOUD Act momenteel maar beperkt toegepast. Daarbij kunnen ook de leveranciers zelf belang hebben bij het aanvechten van dergelijke verzoeken, bijvoorbeeld vanwege reputatie, kosten of precedentwerking. Ondanks deze juridische waarborgen blijft er in de praktijk enige onzekerheid bestaan. Daarom is het verstandig om aanvullende technische en organisatorische maatregelen te nemen om de risico's verder te beperken.

6. Vastgesteld door de Europese Commissie bij Uitvoeringsbesluit (EU) 2023/1795

7. Zie ook: EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

SAMENVATTEND: JURIDISCHE KADERS MAKEN INTERNATIONALE DIENSTVERLENING MOGELIJK, MAAR BORGING ZIT IN BEHEERSMAATREGELEN

Deze regels laten zien dat internationale digitale dienstverlening juridisch mogelijk is, zolang organisaties duidelijk inzicht hebben in hun afhankelijkheden en passende maatregelen nemen, bijvoorbeeld via governance, contracten en risicobeheersing.

Tegelijkertijd is er een belangrijk verschil tussen wat juridisch is toegestaan en wat in de praktijk goed beheerst wordt. Wet- en regelgeving kan voorwaarden stellen, maar garandeert niet automatisch de beveiliging en beschikbaarheid van systemen en gegevens. Dat vraagt om effectieve technische en organisatorische maatregelen.

Daardoor verschuift de discussie van ‘soevereiniteit’ naar ‘aantoonbare controle’: welke maatregelen zorgen ervoor dat risico’s acceptabel zijn en aantoonbaar worden beheerst? Een internationale leverancier kan, wanneer de afspraken en inrichting goed zijn geregeld, soms zelfs betere beveiliging bieden dan een kleinere Europese aanbieder.

Dit whitepaper laat zien hoe organisaties binnen de geldende juridische kaders veilig en aantoonbaar beheerst kunnen blijven werken, ook als volledige digitale autonomie in de huidige geopolitieke situatie niet altijd haalbaar is.

De wetgeving geeft het kader, maar de invulling vindt plaats in de praktijk. In reactie op deze ontwikkeling hebben hyperscalers (grote internationale cloudleveranciers met wereldwijde infrastructuur en schaalvoordelen, zoals Microsoft, Google en Amazon) “soevereine” varianten van hun diensten ontwikkeld. In het volgende hoofdstuk kijken we hoe deze oplossingen bijdragen aan digitale autonomie, en waar hun beperkingen liggen.

Soevereine cloud: bouwstenen, maar geen eindoplossing

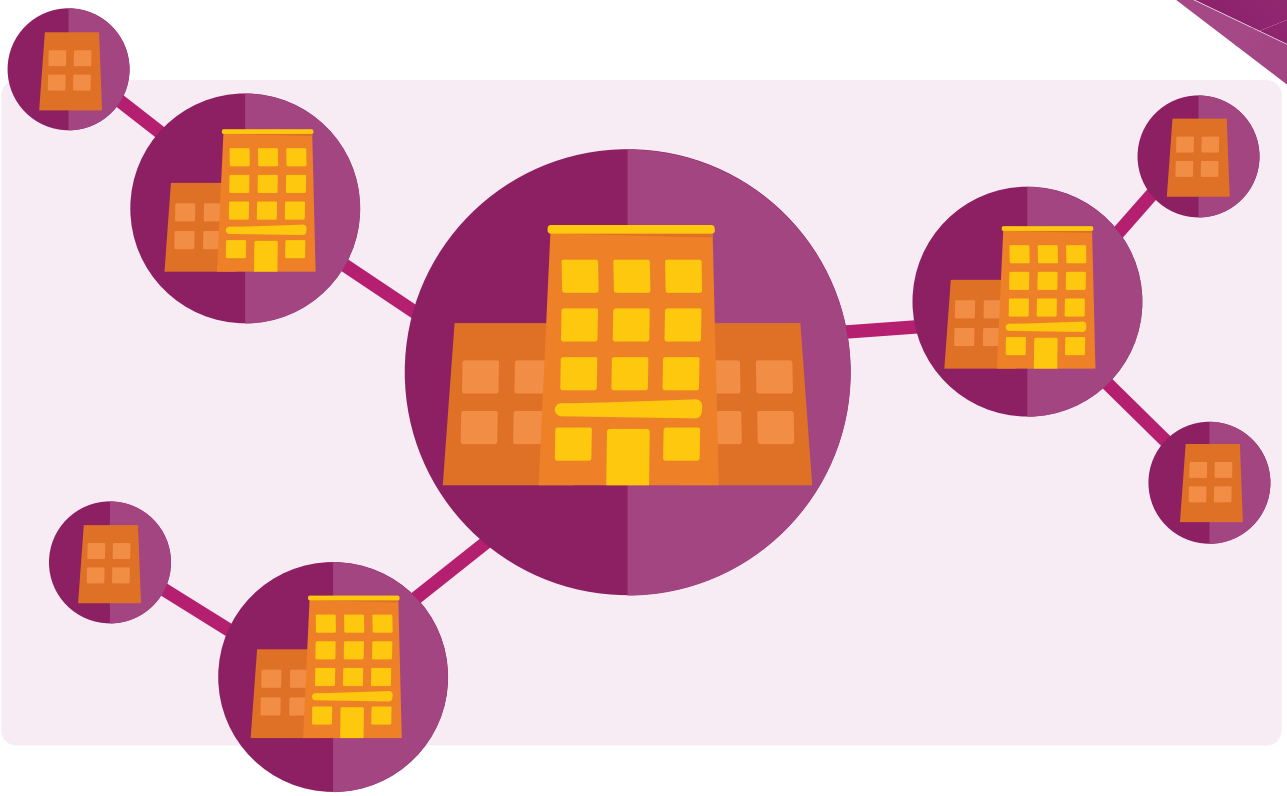
In reactie op de discussie over digitale soevereiniteit en autonomie, en de toenemende zorgen bij Europese organisaties, hebben de grote internationale cloudleveranciers veelal een “soevereine” variant van hun clouddienstverlening ontwikkeld. Deze oplossingen zijn gericht op het adresseren van zorgen rondom vertrouwelijkheid, integriteit en beschikbaarheid, en combineren juridische, organisatorische en technische maatregelen.

De soevereine alternatieven van deze cloudleveranciers vergroten in de praktijk de controle en transparantie, maar nemen de onderliggende afhankelijkheid niet volledig weg. Zo kan het opzetten van een EU-entiteit en het inzetten van EU-medewerkers juridische drempels verhogen voor toegang tot data, maar biedt dit geen garantie tegen invloed via de buitenlandse moedermaatschappij. Ook op technisch vlak worden aanvullende maatregelen getroffen. Mechanismen zoals end-to-end encryptie en trusted computing kunnen de vertrouwelijkheid en integriteit van de data versterken. Tegelijkertijd verdienen deze oplossingen nuance. Bij end-to-end encryptie met klant-gecontroleerde sleutels blijft de leverancier verantwoordelijk voor de softwarelaag waarin versleuteling en ontsleuteling plaatsvinden. In situaties waarin diezelfde leverancier onderdeel is van het dreigingsmodel, kan dit de effectiviteit van deze maatregel beperken. End-to-end encryptie blijft daarmee waardevol, maar vooral in scenario’s waarin de infrastructuur niet wordt vertrouwd en de applicatielaag wel, bijvoorbeeld wanneer data wordt opgeslagen in de cloud, maar wordt verwerkt via eigen software. Daarnaast zijn de grote internationale cloudleveranciers maar tot zekere hoogte transparant over hoe zij omgaan met toegangsvorderingen van buitenlandse autoriteiten. Hierdoor blijft onzekerheid bestaan over de vraag in hoeverre getroffen maatregelen dergelijke verzoeken daadwerkelijk kunnen beperken of voorkomen.

Gezamenlijk laten deze ontwikkelingen zien dat cloudleveranciers digitale soevereiniteit steeds beter ondersteunen, maar dat geen van de geboden oplossingen volledige autonomie realiseert.

Het Europese Cloud Sovereignty Framework (SEAL) kan helpen om deze ontwikkelingen beter te duiden. Het Framework biedt een praktisch beoordelingskader met zogenoemde Sovereignty Effective Assurance Levels (SEAL), dat organisaties helpt om te beoordelen in hoeverre zij controle hebben over hun data, toegang, beveiliging en afhankelijkheden. De niveaus lopen van SEAL-0 (geen specifieke soevereiniteitsmaatregelen) tot SEAL-4 (volledige digitale soevereiniteit onder uitsluitend Europees recht). De niveaus zijn gebaseerd op verschillende aspecten van soevereiniteit, zoals juridische onafhankelijkheid, technologische controle en afhankelijkheden in de leveringsketen. Hierdoor kunnen organisaties de mate van digitale soevereiniteit beter beoordelen en vergelijken. In de praktijk ziet deze indeling er als volgt uit:

SEAL NIVEAU	OMSCHRIJVING
SEAL-0	Geen soevereiniteitsmaatregelen; volledige afhankelijkheid van externe partijen
SEAL-1	Formele juridische afspraken, maar beperkte technische controle
SEAL-2	Data blijft binnen EU-grenzen; basiswaarborgen voor toegang en beheer
SEAL-3	Digitale weerbaarheid onder EU-controle; operationele onafhankelijkheid van niet-EU-partijen
SEAL-4	Volledige soevereiniteit; alle componenten vallen uitsluitend onder EU-jurisdictie en -beheer



Hoewel het Cloud Sovereignty Framework vooral relevant is voor cloudleveranciers die soevereiniteitswaarborgen willen beoordelen, kan het ook relevant zijn voor andere organisaties in de keten. Wanneer cloudplatforms worden gebruikt bij dienstverlening aan (semi-) overheden, kunnen leveranciers en partners aantonen dat zij voldoen aan relevante soevereiniteitseisen. Dit gebeurt vaak via contracten, aanbestedingen en audits. Het SEAL-framework biedt daarmee een manier om digitale soevereiniteit te beoordelen en bespreekbaar te maken, ook buiten de directe context van aanbestedingen.

Voor de meeste organisaties is SEAL-4 echter geen realistisch of noodzakelijk doel. De kracht van de SEAL-niveaus ligt vooral in de mogelijkheid om per dienst, datadomein of use case een bewuste afweging te maken en een passend niveau te bepalen op basis van risico's en afhankelijkheden. Het framework kan organisaties helpen om gericht verbetermaatregelen te nemen, zonder dat volledige digitale soevereiniteit het uitgangspunt hoeft te zijn. De praktische toepassing is nog beperkt doordat cloudleveranciers niet altijd voldoende inzicht geven in hun aanpak. Hierdoor is vaak onduidelijk hoe de grote cloudleveranciers zich verhouden tot de verschillende SEAL-niveaus en welke verplichtingen zij daarbij willen aangaan. Daardoor is het voor organisaties lastig om vast te stellen of aan een bepaald SEAL-niveau wordt voldaan en dit ook aantoonbaar te maken. Dat betekent niet dat cloudleveranciers geen stappen zetten richting hogere SEAL-niveaus, maar wel dat deze stappen momenteel moeilijk te vergelijken en te verifiëren zijn.

Voor cybersecurity- en IT-dienstverleners betekent dit dat zij in de praktijk sterk afhankelijk blijven van de implementatiekeuzes van cloudleveranciers. Hoewel het framework helpt bij het structureren van eisen en verwachtingen, blijft de daadwerkelijke borging van digitale soevereiniteit afhankelijk van aanvullende technische, organisatorische en contractuele maatregelen. Digitale autonomie wordt daarmee uiteindelijk niet bepaald door de keuze voor een specifieke cloudvariant, maar door de mate waarin organisaties zelf regie houden over toegang tot data, sleutels, architectuur en continuïteit.

Kortom, de huidige oplossingen van cloudleveranciers bieden waardevolle bouwstenen, maar geen volledige oplossing. Digitale autonomie bestaat pas als organisaties deze mogelijkheden combineren met eigen technische, organisatorische en contractuele maatregelen. In het volgende hoofdstuk vertalen we dit naar concrete handelingsperspectieven.

Digitale autonomie in de praktijk: van debat naar controle

Dit is geen bedreiging — het is een kans

De voorgaande hoofdstukken hebben de dreiging in kaart gebracht: de geopolitieke kwetsbaarheid van onze digitale afhankelijkheden, de juridische complexiteit van grensoverschrijdende dataverwerking en de concrete scenario's waarin die afhankelijkheden zich kunnen vertalen naar operationele en strategische schade. De vraag die resteert is niet óf organisaties actie moeten ondernemen, maar hoe zij dat het meest effectief doen.

Het antwoord ligt dichter bij huis dan de politieke discussie soms doet vermoeden. Want wie de dreigingen van digitale soevereiniteit zorgvuldig analyseert, herkent daarin een vraagstuk dat securityprofessionals al jaren adresseren: hoe bescherm je gevoelige data tegen ongeautoriseerde toegang, en hoe zorg je ervoor dat kritieke bedrijfsprocessen blijven functioneren wanneer een leverancier of omgeving wegvalt? De geopolitieke context voegt een nieuwe dimensie toe aan dit vraagstuk, maar verandert de aard ervan niet fundamenteel.

Wat wel verandert, is de prioriteit die bestuurders hieraan toekennen. De discussie over digitale soevereiniteit bereikt de bestuurskamer vaker dan traditionele technische of cybersecurityargumenten, omdat het soevereiniteitsvraagstuk direct raakt aan strategische belangen en bedrijfscontinuïteit. Hiermee ontstaat een unieke situatie: de strategische agenda van bestuurders en de operationele agenda van security professionals wijzen nu in dezelfde richting. De strategische meerwaarde voor security investeringen wordt aanzienlijk sterker wanneer diezelfde investeringen tegelijkertijd de digitale soevereiniteit en autonomie van de organisatie versterken. Sterker nog: maatregelen die organisaties weerbaar maken tegen geopolitieke risico's, wapenen hen tegelijkertijd tegen cyberdreigingen.

Voor security professionals en Nederlandse security leveranciers is dit dan ook geen moment voor afwachten, maar voor een duidelijke positionering. Dit hoofdstuk biedt daarvoor het praktische handvat: hoe vertaal je de soevereiniteitsdiscussie naar concrete maatregelen, passend bij het risicoprofiel van jouw organisatie, en uitvoerbaar met bestaande security expertise ondersteund door soevereine Nederlandse en Europese oplossingen.

Risico als kompas

De neiging om digitale soevereiniteit als een alomvattend organisatievraagstuk te benaderen is begrijpelijk, maar leidt in de praktijk tot moeilijkheden. Niet elke applicatie, elk systeem of elke dataset vraagt om dezelfde mate van bescherming. De eerste en meest fundamentele stap is daarom niet het bepalen van een soevereiniteitsstrategie, maar het identificeren van wat er werkelijk op het spel staat.

Twee vragen staan daarbij centraal:

1. Welke data is zo gevoelig dat toegang door buitenlandse autoriteiten — al dan niet via juridische mechanismen zoals de CLOUD Act — onaanvaardbare risico's met zich meebrengt?

2. Welke bedrijfsprocessen zijn zo kritiek dat (gedeeltelijke) uitval of beperking van dienstverlening, bijvoorbeeld door sancties, exportbeperkingen of geopolitieke druk, de continuïteit van de organisatie direct in gevaar brengt?

De vraag hoe groot de kans is dat een buitenlandse overheid daadwerkelijk toegang vordert, of dat een leverancier onder politieke druk zijn dienstverlening staakt, is in de huidige geopolitieke context nauwelijks te beantwoorden.

Organisaties kunnen niet altijd bepalen óf een dreiging zich voordoet, maar wel hoe kwetsbaar zij ervoor zijn, hoe snel een dreiging gevolgen kan hebben en wat de impact daarvan zou zijn. Deze factoren helpen bij het bepalen welke maatregelen prioriteit hebben.

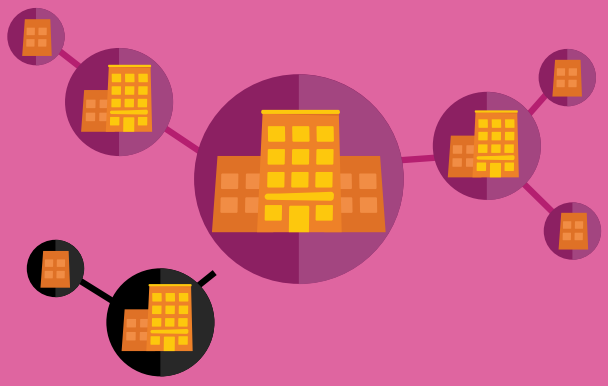
Het SEAL-framework kan hierbij als referentie dienen. Een hogere SEAL-classificatie geeft aan hoe de infrastructuur juridisch en organisatorisch is ingericht, maar zegt niets over hoe deze in de praktijk wordt gebruikt. Organisaties blijven daarom zelf verantwoordelijk voor aanvullende maatregelen. Ook de 'soevereine' cloudoplossingen van grote cloudleveranciers nemen die verantwoordelijkheid niet weg. Wie digitale soevereiniteit en autonomie wil versterken, moet maatregelen treffen die niet afhankelijk zijn van één specifieke leverancier. Uiteindelijk draait het niet om een volledig soevereine oplossing, maar om aantoonbare beheersing van risico's: maatregelen die risico's verlagen en waarvan de werking kan worden gecontroleerd, ongeacht de gekozen leverancier.

Twee dreigingen, één vakgebied

De dreigingen die in de voorgaande hoofdstukken zijn beschreven laten zich, ondanks hun geopolitieke context, terugbrengen tot twee fundamentele vraagstukken die iedere security professional herkent.

1. DATA SOEVEREINITEIT

De dreiging dat gevoelige data toegankelijk wordt voor buitenlandse overheden op grond van juridische verzoeken (bijvoorbeeld onder de CLOUD Act) is in essentie een vertrouwelijkheidsvraagstuk. Een belangrijke maatregel is: gegevens versleutelen en de encryptiesleutels zelf beheren, bijvoorbeeld met een Nederlandse of Europese sleutelbeheeroplossing. Hierdoor wordt het voor buitenlandse partijen veel moeilijker om toegang te krijgen tot de inhoud van de data. De infrastructuur waarop data wordt opgeslagen kan buitenlands zijn — wat telt is dat het sleutelbeheer niet bij de leverancier ligt. Wie de sleutel beheert, bepaalt in belangrijke mate wie bij de data kan.



2. OPERATIONELE AUTONOMIE

De kans dat belangrijke bedrijfsprocessen uitvallen doordat een leverancier onder geopolitieke druk of door sancties zijn dienstverlening stopt, is vooral een risico voor de beschikbaarheid van diensten. Het gaat daarbij om de vraag hoe goed een organisatie kan blijven functioneren als een leverancier, systeem of omgeving wegvalt. De maatregelen die organisaties nemen tegen ransomware, datalekken of uitval van een datacenter helpen vaak ook tegen dit soort geopolitieke verstoringen.

Dat is de kern van dit whitepaper. Digitale soevereiniteit en autonomie zijn geen volledig nieuwe onderwerpen die om nieuwe oplossingen vragen. Het zijn bekende beveiligings- en weerbaarheidsvraagstukken die meer aandacht hebben gekregen. Internationale infrastructuur kan prima worden gebruikt, zolang de organisatie zelf aantoonbaar de regie houdt over de beveiliging en continuïteit van haar systemen en diensten.

Van weerbaar naar adaptief

Weerbaarheid is voor de meeste organisaties inmiddels een vertrouwd begrip. De capaciteit om na een incident te herstellen — of het nu gaat om een ransomware-aanval, een storing in een datacenter of het wegvallen van een leverancier — is essentieel in iedere volwassen securitystrategie. In de context van digitale autonomie krijgt weerbaarheid echter een extra dimensie.

De geopolitieke dreigingen die in dit paper zijn beschreven lijken in hun gevolgen vaak op de “traditionele cyberdreigingen”: zij kunnen zich geleidelijk aankondigen maar ook plotseling en definitief. Een leverancier die onder sancties valt, stopt niet tijdelijk maar mogelijk permanent. Als gegevens eenmaal zijn verstrekt, is dat in de praktijk vaak niet terug te draaien. Daarom is het belangrijk om toegang technisch te beperken. Wie uitsluitend is voorbereid op herstel, mist daarmee een cruciale stap in de voorbereiding.

Een volwassen benadering van weerbaarheid begint dan ook bij *graceful degradation*: het principe waarbij systemen zo zijn ingericht dat bij uitval van een onderdeel de overige functies blijven werken. Volledige operationele stilstand wordt daarmee voorkomen. Kritieke processen kunnen doordraaien terwijl minder essentiële functies tijdelijk wegvallen. Dit vraagt om bewuste architectuurkeuzes bij het ontwerp van systemen en processen of om een herevaluatie van eerder gemaakte architectuurkeuzes. Het toepassen van *graceful degradation* verlaagt het risico op totale uitval aanzienlijk.

De volgende stap voorbij weerbaarheid is een adaptieve architectuur. Waar weerbaarheid gericht is op terugkeren naar de oorspronkelijke situatie, is een adaptieve architectuur ingericht op continuïteit onder wisselende omstandigheden. Concreet betekent dit dat kritieke bedrijfsprocessen kunnen blijven draaien wanneer een primaire leverancier wegvalt. Dit doe je door vooraf een alternatieve omgeving gereed te hebben — bijvoorbeeld een private cloud of een omgeving bij een Europese leverancier — die op het juiste moment kan worden geactiveerd.

De ultimate recovery site, een concept dat in traditionele business continuity planning al langer bestaat, krijgt in dit licht een nieuwe strategische betekenis. Het gaat niet langer alleen om het bewaren van een kopie van data op een onafhankelijke locatie, maar om het bouwen van een omgeving die operationeel inzetbaar is wanneer de primaire omgeving niet langer beschikbaar of betrouwbaar is.

Wat dit betekent in de praktijk

Dit hoofdstuk laat zien welke concrete maatregelen organisaties kunnen nemen voor datasoevereiniteit en operationele autonomie. Het succes van deze maatregelen hangt af van goede sturing binnen de organisatie en duidelijke afspraken met leveranciers.

WEET WAT JE TE VERLIEZEN HEBT

De basis van alles is inzicht. Welke bedrijfsprocessen zijn essentieel binnen de organisatie? Welke data is zo gevoelig dat toegang door derden onaanvaardbaar is? Van welke andere partijen ben je afhankelijk, en wat gebeurt er als een van die partijen wegvalt? Hoe kwetsbaar ben je, hoe snel zou je dit merken en wat is de impact op de organisatie?

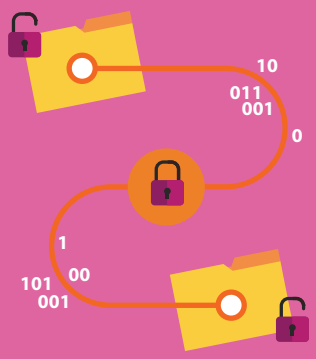
Dit vormt de kern van de organisatie en is het uitgangspunt voor alle verdere maatregelen in de bescherming van systemen en processen. Niet elk systeem of proces vraagt om dezelfde bescherming. Een CRM-systeem met marketinggegevens brengt andere risico’s met zich mee dan software die essentieel is voor de dagelijkse bedrijfsvoering. Daarom is het belangrijk om bewust te bepalen welke systemen en processen het meest kritisch zijn. Dat is geen beperking, maar juist een voorwaarde voor effectieve bescherming.

Vraag voor de bestuurder: als onze drie belangrijkste diensten morgen wegvallen of worden geblokkeerd, welke zijn dat, hoe lang kunnen we dan nog functioneren en wie belt ons als eerste?

ENCRYPTIE EN SLEUTELBEHEER

Voor data die absoluut niet toegankelijk mag zijn voor buitenlandse autoriteiten is encryptie met onafhankelijk sleutelbeheer een van de belangrijkste maatregelen. Goed sleutelbeheer betekent dat de organisatie — of een door haar aangestelde Europese partij — de regie voert over de sleutels. Wanneer de encryptiesleutels bij dezelfde partij liggen als de data zelf, biedt encryptie in dat scenario slechts beperkte aanvullende bescherming. Bring Your Own Key of Hold Your Own Key constructies, ondersteund door Nederlandse of Europese encryptie managementoplossingen, maken de beveiligingslaag onafhankelijk van de infrastructuurleverancier.

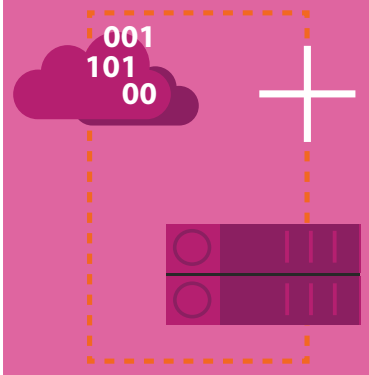
Vraag voor de CISO: wie kan bij onze kritische data zonder onze toestemming, technisch, juridisch of contractueel?



PORTABILITEIT EN EXIT

Vendor lock-in zit zelden alleen in contracten — het zit vooral in de technische verwevenheid van een leverancier in de digitale architectuur. Een modulaire en waar mogelijk op open standaarden gebaseerde architectuur vergroot de technische bewegingsvrijheid om te migreren wanneer dat nodig is. Een exit-strategie is pas een echte exit-strategie als zij praktisch uitvoerbaar is: is de data daadwerkelijk exporteerbaar, is een migratie ooit getest, en is er een alternatieve omgeving uitgewerkt en (periodiek) getest?

Vraag voor de CIO: wanneer hebben we voor het laatst onze eigen data succesvol geëxporteerd of een migratie getest?



WEERBAARHEID EN HERSTEL

Back-ups die op dezelfde omgeving staan als de productieomgeving, bij dezelfde aanbieder of bereikbaar via hetzelfde account, bieden onvoldoende bescherming op het moment dat die omgeving wegvalt of wordt geblokkeerd. Een onafhankelijke herstelomgeving — bij een aparte leverancier of op een gescheiden account — is de minimale voorwaarde voor echte continuïteit. Gecombineerd met graceful degradation en een adaptieve architectuur zoals beschreven in de vorige sectie, ontstaat een weerbaarheid die verder gaat dan herstel alleen.

Vraag voor de CIO: als onze primaire cloudleverancier morgen onbereikbaar is, wie pakt dan intern de regie en beschikken we over voldoende eigen kennis om die situatie het hoofd te bieden?

ECOSYSTEEM EN SAMENWERKING

Digitale autonomie is geen soloproject. De uitdagingen rondom afhankelijkheid, jurisdictie en weerbaarheid zijn breed genoeg om een gezamenlijke aanpak te rechtvaardigen. Organisaties die actief deelnemen aan sectorale netwerken en publiek-private samenwerkingsverbanden vergroten niet alleen hun eigen risicobewustzijn, maar oefenen gezamenlijk invloed uit op marktstandaarden, aanbestedingseisen en wet- en regelgeving.

Vraag voor de bestuurder: zijn wij aangesloten bij relevante sectorale netwerken rondom digitale weerbaarheid en dragen wij actief bij aan kennisdeling die ook onze eigen positie versterkt?
Let wel, genoemde maatregelen werken het best in combinatie: techniek, organisatie/governance, mens, en contract versterken elkaar.

Conclusie

De discussie over digitale soevereiniteit is de afgelopen jaren verschoven van academisch debat naar bestuurlijke urgentie. Dat is winst, maar de vertaalslag van politieke urgentie naar operationele actie blijft voor veel organisaties een uitdaging. Dit paper heeft geprobeerd die vertaalslag te maken.

De centrale conclusie is even eenvoudig als verstrekkend. De dreigingen die voortkomen uit onze digitale afhankelijkheden — ongewenste toegang tot gevoelige data, uitval van kritieke processen door geopolitieke druk — zijn geen nieuwe categorie risico. Zij zijn een nieuwe manifestatie van vraagstukken die het security vakgebied al decennia kent. Vertrouwelijkheid, beschikbaarheid, integriteit, weerbaarheid: de begrippen zijn bekend, de oplossingen zijn voorhanden en de expertise is aanwezig. Wat onderscheidt is de politieke en bestuurlijke context die de prioriteit van deze maatregelen op dit moment versterkt. De strategische onderbouwing voor encryptie met onafhankelijk sleutelbeheer, voor een adaptieve architectuur en voor een onafhankelijke herstelomgeving (bij voorkeur onder een juridisch en operationeel kader dat de organisatie controleerbaar acht) is toegenomen. Niet omdat de technologie is veranderd, maar de wereld eromheen.

Dit pleit niet tegen internationale leveranciers op zichzelf: internationale technologie kan uitstekend passen binnen deze benadering, zolang de technische en organisatorische beheersmaatregelen aantoonbaar op orde zijn en afhankelijkheden bestuurbaar blijven.

Voor security professionals is dit het moment om die versterkte business case te benutten. Voor bestuurders is dit het moment om de soevereiniteitsdiscussie te vertalen naar concrete investeringsbeslissingen. En voor Nederlandse en Europese security leveranciers is dit het moment om te laten zien wat soevereine beveiliging in de praktijk betekent: geen alternatieve infrastructuur, maar een onafhankelijke beveiligingslaag die de infrastructuurkeuze van de organisatie completeert en versterkt.

Dit is in de kern geen politieke discussie. Dit is bedrijfscontinuïteit.

Bijlage:
Van risicoanalyse naar actie

De maatregelen die digitale soevereiniteit en autonomie in de praktijk noodzakelijk maken zijn niet voor iedere organisatie gelijk. Welke maatregelen prioriteit verdienen hangt af van het risicoprofiel van de organisatie. De onderstaande beslisboom helpt om op basis van twee centrale vragen te bepalen waar de focus moet liggen.

Stap 1: Bepaal je uitgangspositie

Beantwoord de volgende twee vragen:

VRAAG A: Beschikt de organisatie over data die in géén geval toegankelijk mag zijn voor buitenlandse autoriteiten?

VRAAG B: Beschikt de organisatie over kritieke bedrijfsprocessen die niet mogen wegvallen als een leverancier uitvalt, zijn dienstverlening staakt of onder sancties valt?

Beide vragen kunnen gelijktijdig van toepassing zijn. Voor elke vraag die met ja wordt beantwoord, doorloop je het bijbehorende spoor.

Stap 2: Bepaal de urgentie per spoor

Voor elk spoor dat van toepassing is, beantwoord je drie vervolgvragen die de prioriteit van maatregelen bepalen:

VRAAG	LAAG	MIDDEN	HOOG
Hoe kwetsbaar ben je?	De organisatie verwerkt weinig gevoelige data en is beperkt afhankelijk van niet-soevereine IT	De organisatie verwerkt gevoelige data en is deels afhankelijk van niet-soevereine IT voor beheer of opslag daarvan	De organisatie verwerkt zeer gevoelige data en is sterk afhankelijk van niet-soevereine IT- infrastructuur of diensten
Hoe snel kan de dreiging zich manifesteren?	Dreiging kondigt zich ruim van tevoren aan, er is tijd om te reageren	Dreiging is deels voorzienbaar maar tijdsdruk is reëel	Dreiging kan zich plotseling en structureel manifesteren zonder waarschuwing
Wat is de impact als het scenario zich voordoet?	Beperkte operationele of reputatieschade	Significante schade maar herstel is mogelijk	Existentiële schade voor de organisatie of haar klanten (bijv. langdurige uitval vitale dienstverlening, wettelijke taken in gevaar, grote maatschappelijke impact).

[·] met “niet-soevereine IT” wordt hier bedoeld: IT-diensten of –componenten waarbij de organisatie onvoldoende aantoonbare regie heeft over de regels rond toegang, sleutelbeheer, auditability/transparantie en exit/continuïteit, waardoor afhankelijkheden niet bestuurbaar zijn (ongeacht de herkomst van leverancier). Ofwel, “buiten eigen regie/controle”.

Stap 3: Prioriteer maatregelen per spoor

SPOOR A — DATA SOEVEREINITEIT

Prioriteit	Maatregel
Direct	Inventariseer welke gevoelige data op buitenlandse infrastructuur staat en onder wiens sleutelbeheer
Korte termijn	Implementeer onafhankelijk sleutelbeheer onder Europese regie (bijv. BYOK of HYOK of external key management)
Middellange termijn	Toets contractueel wie technisch en juridisch toegang kan hebben tot kritieke data en pas aan waar nodig
Structureel	Bouw encryptie en sleutelbeheer in als ontwerpprincipe bij nieuwe systemen en applicaties

SPOOR B — OPERATIONELE AUTONOMIE

Prioriteit	Maatregel
Direct	Inventariseer welke kritieke processen afhankelijk zijn van één leverancier en wat de impact is bij uitval
Korte termijn	Richt een onafhankelijke herstelomgeving in bij een onafhankelijke leverancier of in een gescheiden omgeving (bij voorkeur onder een kader dat de organisatie controleerbaar acht) en test deze periodiek (bijv. halfjaarlijks)
Middellange termijn	Pas architectuurkeuzes aan op het principe van graceful degradation zodat deelfuncties blijven werken bij uitval
Structureel	ouw een adaptieve architectuur die omschakeling naar een alternatieve omgeving operationeel mogelijk maakt

BEIDE SPOREN

Prioriteit	Maatregel
Direct	Sluit aan bij sectorale netwerken en publiek-private samenwerkingsverbanden rondom digitale weerbaarheid.
Structureel	Draag actief bij aan kennisdeling en beïnvloeding van marktstandaarden en aanbestedingseisen

Afkortingen en verklarende woordenlijst (op alfabetische volgorde)

A

ADAPTIEVE ARCHITECTUUR
Een IT-architectuur die niet alleen gericht is op herstel na verstoring, maar op het operationeel kunnen blijven functioneren onder veranderende omstandigheden.

ADEQUAATHEIDSBESLUIT
Besluit van de Europese Commissie waarin wordt vastgesteld dat een land buiten de EU een passend beschermingsniveau biedt voor persoonsgegevens. Hierdoor mogen persoonsgegevens onder voorwaarden naar dat land worden doorgegeven.

AUDITABILITY / AUDITBAARHEID
De mate waarin toegang, wijzigingen en handelingen binnen systemen controleerbaar en verifieerbaar zijn. Een audit is een onderzoek waarmee men beoordeelt hoe de werkelijkheid binnen een afgekaderd gebied zich verhoudt tot een bepaalde (vastgestelde) norm.

AVG (ALGEMENE VERORDENING GEGEVENSBESCHERMING)
AVG is de Nederlandse benaming voor de General Data Protection Regulation (GDPR), de rechtstreeks toepasselijke Europese verordening voor de bescherming van persoonsgegevens. In Nederland wordt de AVG aangevuld door de Uitvoeringswet Algemene verordening gegevensbescherming. De AVG is in Nederland de opvolger van de Wet bescherming persoonsgegevens.

AZURE
Het cloudplatform van Microsoft waarop organisaties infrastructuur, opslag, applicaties en digitale diensten kunnen draaien.

B

BACK-UP
Een reservekopie van gegevens of digitale systemen. Hiermee kan men gegevens of systemen herstellen als het origineel beschadigd of weg is.

BEST PRACTICES
Bewezen effectieve werkwijzen en beveiligingsmaatregelen die binnen een sector of vakgebied algemeen worden toegepast.

BRING YOUR OWN KEY (BYOK)
Een vorm van sleutelbeheer waarbij een organisatie zelf encryptiesleutels aanlevert voor data in een cloudomgeving. Hiermee blijft de organisatie meer regie houden over toegang tot data.

BUSINESS CONTINUITY PLANNING
Het voorbereiden van processen, systemen en organisatiestructuren zodat kritieke dienstverlening kan blijven functioneren tijdens verstoringen of crises.

C

CISO (CHIEF INFORMATION SECURITY OFFICER)
De medewerker die verantwoordelijk is voor cybersecurity binnen een organisatie. Rol op strategisch niveau

CLOUD
Het toegankelijk maken van IT-diensten, zoals bijvoorbeeld hardware en software via een netwerk, meestal het Internet. Voorbeelden van Clouddiensten zijn Software-as-a-Service (SAAS), Platform-as-a-Service (PAAS) en Infrastructure-as-a-Service (IAAS).

CLOUD ACT
Amerikaanse wetgeving die bepaalde dienstverleners onder Amerikaanse jurisdictie onder voorwaarden kan verplichten om data beschikbaar te stellen aan Amerikaanse autoriteiten, ook wanneer die data buiten de Verenigde Staten staat opgeslagen.

CLOUD SOVEREIGNTY FRAMEWORK
Europees referentiekader waarmee organisaties de mate van digitale soevereiniteit van cloudomgevingen kunnen beoordelen.

COMPLIANCE
De activiteiten die men uitvoert om als persoon of organisatie te voldoen aan bepaalde eisen. Dat kan een wet zijn, maar ook eisen uit de branche of regels van de eigen organisatie.

D

DATA ACT / DATAVERORDENING
Europese verordening die onder andere gericht is op betere dataportabiliteit, interoperabiliteit en het verminderen van vendor lock-in bij cloud- en datadiensten.

DATA-RESIDENTIE
De fysieke locatie waar data wordt opgeslagen.

DATALEK
Een gangbare term voor een inbreuk in relatie tot persoonsgegevens. In de context van de Algemene Verordening Gegevensbescherming is een datalek een leken-term voor ‘inbreuk in verband met persoonsgegevens’, inhoudende een incident waardoor de integriteit, beschikbaarheid en/of vertrouwelijkheid van persoonsgegevens worden aangetast. Voorbeelden zijn ransomware aanvallen, of een e-mail met alle geadresseerden in het “To” – veld.

DATACENTER
Fysieke locatie waarin servers, opslag en netwerkapparatuur worden beheerd.

DIGITALE AUTONOMIE
Het vermogen van een organisatie om zelfstandig keuzes te maken in het digitale domein, zonder onwenselijke afhankelijkheden die die handelingsvrijheid beperken.

DIGITALE SOEVEREINITEIT
De mate waarin een organisatie of overheid zeggenschap houdt over data, infrastructuur, systemen en digitale afhankelijkheden, inclusief de juridische en bestuurlijke controle daarop.

DIGITALE WEERBAARHEID
Het vermogen om inbreuken op de vertrouwelijkheid en integriteit van informatie, en de continuïteit van bedrijfsprocessen te voorkomen, herkennen, op te vangen en te herstellen en daarbij zo goed mogelijk te blijven functioneren.

E

ENCRYPTIE
Informatie omzetten in een code zodat een ander het niet kan lezen. Dit doet men als men gevoelige informatie veilig wil bewaren of versturen.

END-TO-END ENCRYPTIE
Een vorm van encryptie waarbij gegevens alleen leesbaar zijn voor de verzender en ontvanger, en niet voor de infrastructuurleverancier of tussenliggende partijen.

EXIT-STRATEGIE
Een praktisch uitvoerbaar plan om data, systemen en processen gecontroleerd te migreren naar een andere leverancier of omgeving.

G

GDPR (GENERAL DATA PROTECTION REGULATION)
De Engelstalige benaming voor de AVG.

GEOPOLITIEK
Internationale politieke en economische machtsverhoudingen die invloed hebben op technologie, handel, wetgeving en digitale afhankelijkheden.

GOVERNANCE
De inrichting van verantwoordelijkheden, besluitvorming, toezicht en controle binnen een organisatie.

GRACEFUL DEGRADATION
Architectuurprincipe waarbij systemen bij verstoringen gedeeltelijk blijven functioneren in plaats van volledig uitvallen.

H

HOLD YOUR OWN KEY (HYOK)
Een vorm van sleutelbeheer waarbij een organisatie volledige controle houdt over encryptiesleutels buiten de cloudleverancier om.

I

IEC62443
Internationale norm voor cybersecurity binnen industriële automatisering en operationele technologie.

INCIDENTRESPONS
Het reageren op een cyberincident. Het is een (gestructureerde) aanpak op alle niveaus: operationeel, tactisch en strategisch. Incident response kan gezien worden als een soort brandweer bij een cyberincident.

INTEGRITEIT (INFORMATIEBEVEILIGING)
1. Bij data: juiste en volledige informatie, en verwerking van informatie. 2. Bij personen: de betrouwbaarheid van iemand. 3. Bij digitale diensten, processen of systemen: hun correcte werking.

INTEROPERABILITEIT
Het vermogen van systemen, applicaties en diensten om gegevens uit te wisselen en samen te werken.

ISO27001
Internationale norm voor het inrichten en beheersen van informatiebeveiliging.

J

JURISDICTIE
Het rechtsgebied en de wetgeving waaronder een organisatie, leverancier of infrastructuur valt.

K

KEY MANAGEMENT / SLEUTELBEHEER
Het beheren van encryptiesleutels die bepalen wie toegang heeft tot versleutelde data.

L

LEVERANCIERSKETEN
Het geheel van leveranciers, dienstverleners en technologiepartners waarvan een organisatie afhankelijk is.

LOGGING
Het registreren van gebeurtenissen, toegang en systeemactiviteiten om controle, monitoring en onderzoek mogelijk te maken.

N

NEN7510
Nederlandse norm voor informatiebeveiliging in de zorgsector.

NIS2-RICHTLIJN
Europese richtlijn die bepaalde essentiële en belangrijke entiteiten verplicht om cyberrisico's en ketenafhankelijkheden aantoonbaar te beheersen.

O

ON-PREMISE IT
IT-systemen die draaien op infrastructuur in eigen beheer, bijvoorbeeld in een eigen datacenter.

P

PORTABILITEIT/ PORTABILITY
De mogelijkheid om data, applicaties of systemen eenvoudig te verplaatsen naar een andere omgeving of leverancier.

PRIVATE CLOUD
Cloudomgeving die exclusief wordt gebruikt door één organisatie.

R

RANSOMWARE
Kwaadaardige software waarbij een slachtoffer afgeperst wordt, nadat zijn digitale systeem of de bestanden erop met een code op slot zijn gezet. De aanvaller biedt de code tegen betaling aan, zodat hij er weer bij kan. Maar zelfs dat is niet zeker. Ransomware is een samenvoeging van de woorden ransom (losgeld) en software. Tegenwoordig is de daadwerkelijke software maar een kleine stap in de totale aanval die plaatsvindt. Alle stappen samen vormen de Ransomware Killchain.

RECOVERY SITE / ULTIMATE RECOVERY SITE
Een onafhankelijke omgeving die operationeel ingezet kan worden wanneer de primaire IT-omgeving uitvalt of niet langer beschikbaar is.

RISICOGEBASEERDE AANPAK
Benadering waarbij beveiligingsmaatregelen worden afgestemd op de gevoeligheid van data, kritieke processen en afhankelijkheden.

S

SCA (STORED COMMUNICATIONS ACT)
Amerikaanse wetgeving die onderdeel vormt van het juridische kader waarbinnen toegang tot opgeslagen digitale communicatie kan worden gevorderd.

SEAL (SOVEREIGNTY EFFECTIVE ASSURANCE LEVELS)
Classificatiemodel binnen het Europese Cloud Sovereignty Framework waarmee de mate van digitale soevereiniteit kan worden beoordeeld. De niveaus variëren van volledige afhankelijkheid van externe partijen (SEAL-0) tot volledige digitale soevereiniteit onder uitsluitend EU-jurisdictie (SEAL-4).

SLEUTELBEHEER
Zie: key management.

T

THREAT INTELLIGENCE CENTER
Organisatieonderdeel dat dreigingsinformatie verzamelt, analyseert en gebruikt om cyberdreigingen vroegtijdig te detecteren.

TRUSTED COMPUTING
Technologie die moet waarborgen dat systemen

V

VENDOR LOCK-IN
Situatie waarin overstappen naar een andere leverancier technisch, organisatorisch of contractueel moeilijk of kostbaar wordt.

VERTROUWELIJKHEID
De zekerheid dat informatie en/of digitale diensten, processen of systemen alleen toegankelijk zijn voor personen of software die hiertoe zijn geautoriseerd.

W

WEERBAARHEID
Het vermogen van een organisatie om verstoringen op te vangen en operationeel te blijven functioneren.

Z

ZERO-ACCESS ARCHITECTUUR
Architectuur waarbij een leverancier technisch geen toegang heeft tot klantdata, ook niet wanneer de infrastructuur door die leverancier wordt beheerd.