

Amerikaanse sancties tonen IT-afhankelijkheid

Soevereiniteit is geen ideologie, het is beveiligingsbeleid

Een buitenlandse overheid hoeft geen server te hacken om de IT in een organisatie plat te leggen. Een sanctiebesluit kan genoeg zijn. Het Internationaal Strafhof ontdekte dat hun cruciale dienstverlening afhankelijk is van buitenlandse leveranciers. Digitale soevereiniteit is daarmee geen ideologie, maar een concreet informatiebeveiligingsrisico.

KARIM KHAN, HOOFDAANKLAGER VAN HET INTERNATIONAAL STRAFHOF IN DEN HAAG, VERLOOR ZIJN Microsoft-werkplek. De Verenigde Staten eisten dat, nadat het Hof arrestatiebevelen had uitgevaardigd tegen Israëliische leiders. Amerikaanse tech-bedrijven moeten die sancties wettelijk uitvoeren, dus ging de deur dicht. Een buitenlandse overheid legde een internationale rechtbank digitaal plat zonder één computer aan te raken.

Het Hof begon een migratie naar openDesk, het Europese opensource-alternatief. Precies wat je zou hopen. Toen werd het erger.

De sanctie als aanvalsvector

Eind augustus 2026 zetten de VS een ideële Italiaanse internetprovider Autistici/Inventati op de terrorismelijst, omdat die onwelgevallige blogs host. De Italiaanse bank blokkeerde per direct alle rekeningen, uit angst zelf te worden afgesloten van het door de VS gedomineerde betaalsysteem en van creditcard-netwerken. Dat signaal is aangekomen. Procolix, de Nederlandse dienstverle-

ner van het Strafhof, heeft het Hof laten weten de dienstverlening te moeten staken. Niet omdat Procolix het Strafhof niet steunt, maar een kleine speler overleeft geen Amerikaanse boycot op bankrekening, PayPal-transacties of domeinregistraties. Dat betekent faillissement.

De Europese Unie heeft op papier wapens. Het Anti-Coercion Instrument en de Blocking Statute verbieden Europese bedrijven om aan Amerikaanse sancties te voldoen en maken tegenmaatregelen mogelijk. Alleen: een mkb-hoster kan weinig met bescherming achteraf, wanneer je morgen vermorzeld wordt. Soevereiniteit is een illusie, zolang buitenlandse mogelijkheden onze leveranciers via het betalingsverkeer chanteren.

Deze geopolitiek knelt, want economische macht inzetten om een ander tot ander gedrag te dwingen is klassiek machtspolitiek handwerk. Geopolitiek klinkt als: een systeem boven onze hoofden, zonder dader, waar vooral de parlement en Brussel over gaan. Zo wordt buitenlands beleid van één land



Beeld: Shutterstock

aan ons verkocht als een natuurverschijnsel. Maar het is beleid, het heeft een afzender en het is op ons gericht. En het komt uit bij iets veel banalers, en daarmee veel dwingenders: een handtekening onder een contract.

Verzwakte encryptie

Informatiebeveiliging draait om beschikbaarheid, integriteit en vertrouwelijkheid. Die drie doelen staan in het beleid, in het Information Security Management System (ISMS), in het jaarplan. Kijk nu nog eens naar de casus van het Strafhof. Beschikbaarheid: een dienst valt weg op last van een vreemde mogelijkheid. Geen contractbreuk, geen storing, gewoon een beleidsbeslissing. Oekraïne maakte hetzelfde mee toen de toegang tot satellietbeelden van Maxar Technologies werd afgeknepen. Op het

slagveld was dat dodelijk. Vertrouwelijkheid: de CLOUD Act verplicht Amerikaanse bedrijven klantdata te overhandigen, ongeacht waar die staan opgeslagen. FISA Section 702 en Executive Order 12333 gaan verder, en China heeft een vergelijkbaar instrumentarium. Wie data toevertrouwt aan een aanbieder met juridische banden buiten Europa, accepteert dat meerdere rechtsstelsels tegelijk aanspraak maken op dezelfde gegevens.

Integriteit: het Huawei-debat in de 5G-netwerken gaat over de vraag of u zelfstandig kunt vaststellen dat uw systemen uitsluitend doen wat ze horen te doen. Die vraag is terecht. Ruim honderd landen vertrouwden decennialang hun diplomatieke en militaire communicatie toe aan de encryptieapparatuur van het Zwitserse Crypto AG. Dat bedrijf

bleek eigendom van de CIA en de Duitse inlichtingendienst, die de versleuteling doelbewust hadden verzwakt om mee te kunnen lezen. Bij de lekken Shadow Brokers en Vault 7 kwamen de digitale wapens van NSA en CIA op straat te liggen. Die draaien op softwarefouten die de Amerikaanse overheid bewust niet liet repareren, omdat ze er zelf mee wilde spioneren. Maar criminelen vonden diezelfde fouten en dat had schade. De integriteit van systemen was jarenlang in het geheim aangetast, zonder dat één beheerder dat kon zien.

Soevereiniteit is dus geen nieuw paradigma naast informatieveiligheid, maar de toetssteen van wat we al twintig jaar beweren te doen. Geen mening, maar een beheersmaatregel waar bestuurders onder NIS2 op afrekenbaar

Wie nooit gunt, maakt het probleem niet kleiner

zijn. Een afhankelijkheid die een derde land als drukmiddel kan gebruiken, is een risico.

Wij liggen in scheiding

Historicus Rob de Wijk vatte het onbarmhartig samen: Amerika heeft de scheiding met Europa aangevraagd, en wij willen het nog niet echt geloven. De meesten van ons willen die scheiding ook helemaal niet. Decennia aan gedeelde belangen, waarden en infrastructuur laat je niet graag los. Dus blijven we hopen dat het meevalt, dat de volgende regering het terugdraait, dat onze leverancier zich wel zal verzetten.

Maar de andere partij heeft de papieren ingediend. In sanctielijsten, op de veiligheidsconferentie in München, in de Cyber Security Strategie van maart 2026, die aankondigt de verspreiding van buitenlandse AI-platforms te zullen dwarsbomen. Wie na zo'n boodschap blijft fixeren op de ex-partner, doet niet aan relatiebeheer, maar aan stalking. Dat is een beroerde basis voor een continuïteitsplan.

Zaken doen is zaken gunnen

Ook de Amerikaanse dominantie in digitale infrastructuur is geen natuurverschijnsel, en geen bewijs van superieure ondernemerschap. Het Amerikaanse

ministerie van Defensie was decennialang de grootste technologie-inkoper ter wereld. ARPA, later DARPA, stelde functionele eisen, financierde onderzoek en liet de uitwerking aan de markt: een veeleisende eerste afnemer die innovatie mogelijk maakte zonder alles zelf te bouwen. Internet, GPS en micro-elektronica begonnen als defensieproject.

Cruciaal daarbij is dat die orders werden gegund voordat het resultaat perfect was. Bedrijven kregen ruimte om zich te ontwikkelen. Vergelijk dat met onze praktijk. Elke Europese aanbieder die zich meldt, krijgt te horen dat het alternatief nog niet volwassen genoeg is, nog niet alle functies heeft, nog niet de schaal kan leveren. Waarna we tekenen bij de partij die dankzij dertig jaar Amerikaans inkoopbeleid wel zover is. Wie nooit gunt, maakt het probleem niet kleiner.

De cijfers bewijzen dit. Van de ruim €61 miljard Europese cloudmarkt gaat 80% tot 85% naar bedrijven onder Amerikaans recht. Tussen 2017 en 2022 groeide de omzet van Europese aanbieders met 167%, terwijl hun marktaandeel daalde van 27% naar 13%. Ze renden hard en raakten toch achterop. Zaken doen is zaken gunnen. Enig ongemak dan is geen liefdadigheid, maar industriepolitiek. Dat is ons decennialang voorgedaan.

Aan of uit

Tegelijk moeten we af van het idee dat soevereiniteit een schakelaar is die aan of uit staat. Volledige onafhankelijkheid is voor vrijwel niemand realistisch, dus dat frame maakt het gesprek onmogelijk. Het European Cloud Sovereignty Framework biedt een bruikbaar model. Het ontleedt soevereiniteit in acht doelen, van strategische verankering en rechtsmacht tot data, keten, techniek en duurzaamheid, met per doel vijf niveaus: de SEAL-niveaus, van geen inzicht tot volledige controle. Zo stelt u vast waar u nu staat, op basis van aantoonbare kenmerken in plaats van



intenties: onder welke jurisdictie valt de leverancier, wie beheert de sleutels, wie heeft operationele toegang. En u bepaalt per proces waar u naartoe wilt. Een gemeente mag prima zeggen dat zij voor interne werkprocessen meer afhankelijkheid accepteert dan voor burgergegevens. Dat is een verdedigbare positie.

Het raamwerk sluit geen landen uit, maar verschuift het gesprek van herkomst naar eigenschappen: niet: 'Waar komt deze leverancier vandaan', maar: 'Kan deze dienst aantoonbaar voldoen aan de vereiste controle en afdwingbaarheid'. Daarmee is het bruikbaar als eis in een aanbesteding, zonder juridisch glad ijs. Een Europees bedrijf met zwakke waarborgen levert minder soevereiniteit dan een Amerikaans bedrijf met harde technische isolatie en afdwingbare Europese jurisdictie.

Soevereiniteit zit dan ook niet alleen in een datacentrum of een juridisch construct, maar evengoed in eigen technologie, eigen kennis en het vermogen zelf door te ontwikkelen. Soevereiniteit zit dan ook niet alleen in een datacentrum of een juridisch construct, maar evengoed in eigen technologie, eigen kennis en het vermogen zelf door te ontwikkelen.

Proef op de som

Ik nam de proef op de som bij een voor mij cruciaal proces: maken en geven van presentaties. Vanuit Stichting LibreKAT bouwden we OciDeck. Het gangbare verhaal luidt dat een alternatief ongeveer 80% van de functionaliteit haalt. Voor OciDeck klopt dat niet, en niet in de richting die u verwacht. Het doet meer dan Keynote of PowerPoint. Presentaties worden opgeslagen als standaard Markdown. Er zijn gespecialiseerde editors per slidetype, grafieken uit CSV-data, een presenterweergave met dual-screen en aantekeningen, en classificatie voor gerubriceerde inhoud. Een ingebouwde privacyscan detecteert en verwijdert persoonsgegevens. Geen backend voor het bewerken, geen

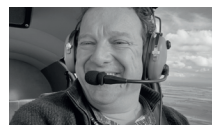
telemetrie, en het draait op macOS, Windows, Linux en in de browser.

De gevolgen merk ik dagelijks. Ik maak presentaties sneller, doorzoek al mijn slides van jaren terug in een oogwenk en importeer wat ik nodig heb, tegen een fractie van de schijfruimte. Het belangrijkste: ik ben in control. Als mijn eigen software morgen ophoudt te bestaan, draaien die bestanden door met minder fraaie alternatieven, en blijven ze over dertig jaar leesbaar. Dat is het punt dat Martijn Aslander maakt met zijn Pilot Informatie Autonomie: de soevereiniteit zit niet in de tool, maar in het formaat. Eén persoon, één proces, één jaar. Als dat kan, is 'het kan niet' geen argument meer. Het is een keuze.

Drie processen

Begin klein en bestuurlijk. Kies drie processen die uw organisatie werkelijk niet kan missen en breng daarvoor de feitelijke situatie in kaart: jurisdictie, sleutelbeheer, operationele toegang, de keten onder uw leverancier. Leg vast welk niveau u passend vindt en waar het verschil zit. Neem in uw volgende inkoop of aanbesteding het gewenste SEAL-niveau op als toetscriterium. En gun daarna iets aan een partij die er nog niet helemaal is. Accepteer dat ongemak, want het is de enige manier waarop hier ooit iets ontstaat om naartoe te migreren.

De gevaarlijkste positie is de positie die nooit is ingenomen. ProcoliX maakte afgelopen maand de keuze die de omstandigheden afdwongen. Maak die van u liever zelf, op een moment dat u er nog een hebt. 



Brenno de Winter
is expert informatie-beveiliging.