Commissie Digitale Zaken

Kapteynstraat 1, SBIC - Building
suite 220 / 2201 BB Noordwijk

info@cyberveilignederland.nl
www.cyberveilignederland.nl

KvK 71802525

Noordwijk, 3 februari 2025
Ref.: PA902-250203

Betreft: Input rondetafelgesprek over *Digitale soevereiniteit bij de Rijksoverheid*

Geacht lid van de commissie Digitale Zaken,

Onze maatschappij is in een hoog tempo afhankelijk geworden van digitale netwerken. Ook de Rijksoverheid is hierin mee ontwikkeld. Recente IT-storingen (bijvoorbeeld de foutieve Crowdstrike-update en de problemen met NAFIN) benadrukken hoe afhankelijk onze samenleving is geworden van digitale netwerken, maar ook van een digitale overheid.

U heeft aan Cyberveilig Nederland (CVNL) gevraagd welke risico's volgen uit de afhankelijkheid van de Rijksoverheid ten aanzien van andere mogendheden en actoren, oftewel de digitale soevereiniteit van de Rijksoverheid. Vragen die u hierbij heeft zijn:

- Welke cyberveiligheidsrisico's kleven er aan strategische afhankelijkheden?
- Welke afhankelijkheden ziet u momenteel als grootste kwetsbaarheid in de digitale infrastructuur van Nederland?
- Is de Nederlandse ICT-sector nu in staat om cyberveilige infrastructuur en applicaties te leveren?
- Draagt het zwaar(der) meewegen van autonomie in de risicobeoordeling bij aanbestedingen van het Rijk bij aan de digitale weerbaarheid van Nederland?

In deze position paper beschrijven we hoe we vanuit CVNL naar deze uitdagingen kijken en suggereren we enkele oplossingsrichtingen. We beschrijven daarbij niet alleen de uitdagingen voor de Rijksoverheid, maar breder ten aanzien van de Nederlandse maatschappij.

Digitale soevereiniteit: wat is haalbaar?
Onze afhankelijkheid van digitale computernetwerken met technologie van buiten Europa wordt steeds groter. Veel IT-oplossingen worden ingekocht bij leveranciers uit bijvoorbeeld China en de Verenigde Staten. Tegelijkertijd is er een geopolitiek landschap ontstaan waarin het vertrouwen in de landen waar we deze oplossingen inkopen is afgenomen. Bevriende naties van vandaag kunnen morgen risico's vormen voor onze nationale veiligheid.

Het Draghi-rapport van september 2024[1] bevestigt dat we als Europa in de afgelopen jaren steeds verder afhankelijk zijn geworden van leveranciers buiten Europa. Of het nou gaat om maakindustrie, IT industrie of defensieindustrie: we zijn onvoldoende in staat geweest om goede competitieve tegenhangers tegenover Chinese en Amerikaanse bedrijven te zetten. En hoewel twee hoogleraren economie in het FD nog pleitten voor het terughalen van toeleverancierssketens[2], zien wij het als onhaalbaar om in Europa een volledig concurrerende IT industrie op te bouwen. Dat is veel te duur en tijdrovend.

In plaats van het streven naar een eigen industrie die gericht is op het produceren van Europese IT-systemen, moeten Nederland en Europa zich naar onze mening richten op het vergroten van controle over bepaalde aspecten van ons IT-landschap. Dit sluit aan bij de definitie van digitale soevereiniteit die TNO geeft in haar rapport over dit onderwerp uit 2024[3]:

> *Digitale soevereiniteit betekent dat men de digitale capaciteiten en mogelijkheden heeft om digitale goederen, diensten en infrastructuren te produceren, te leveren en te gebruiken en dat men de controle hierover heeft om de soevereiniteit te beschermen.*

Soms wordt voor digitale souvereiniteit een bredere definitie gehanteerd waarbij het uitgangspunt is dat onafhankelijkheid wordt bereikt op economisch vlak, op technologisch vlak én op gebied van het gebruik, verwerking en opslag van data. Aanvullend dat er normatieve controle moet plaatsvinden op basis van eigen wet- en regelgeving. CVNL gaat in dit paper uit van de smallere TNO-definitie omdat zij dit ziet als realistisch perspectief en al zeer complex om te realiseren.

[1] https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en
[2] https://fd.nl/politiek/1542754/het-oude-model-van-open-grenzen-werkt-niet-meer-als-de-wereld-voor-iets-anders-kiest
[3] https://publications.tno.nl/publication/34642268/o5remY/TNO-2024-R10300.pdf

Mogelijke oplossingen voor het vergroten van digitale soevereiniteit
Voor wat betreft het vergroten van controle over delen van het IT-landschap (binnen de Rijksoverheid, maar ook daarbuiten) zien we als CVNL vanuit cybersecurityperspectief een aantal mogelijke oplossingen die we graag onder uw aandacht willen brengen:

1. Risicospreiding door een aangepaste inkoopstrategie
2. Fallback oplossingen bij uitval
3. Betere bescherming van gevoelige data
4. Inzet van Europese en Nederlandse regulering
5. Fysieke bescherming van de Nederlandse digitale infrastructuur
6. Versterken van human capital

1. Risicospreiding door een aangepaste inkoopstrategie
Bij het inrichten van een IT-landschap hebben organisaties veel mogelijkheden als het gaat om de keuze voor toeleveranciers. Vanuit het perspectief van beheersbaarheid, gemak en kosten kan de keuze vallen op een beperkte set van toeleveranciers voor onderdelen in het IT-landschap zoals hardware, netwerkcomponenten en software.

Belangrijk bij inkoop van IT-oplossingen is echter dat ook het perspectief van digitale soevereiniteit wordt meegewogen. Risico's op dit gebied kunnen ontstaan door bijvoorbeeld veel oplossingen in te kopen bij dezelfde leverancier, maar ook door de oplossingen in te kopen bij meerdere leveranciers uit hetzelfde land. In plaats daarvan zouden inkoopstrategieën gericht moeten zijn op spreiding, zowel geografisch als voor de keuze van verschillende toeleveranciers. Hierbij dient ook kritisch gekeken te worden naar de zogenaamde Software/Hardware Bill of Materials (SBOM/HBOM), aangezien een leverancier bijvoorbeeld ook (delen van) hard- en software uit onvriendelijke landen zou kunnen gebruiken. Geografische spreiding en verschillende leveranciers alleen is daarom niet voldoende. Het opvragen van een SBOM/HBOM helpt bij het identificeren van mogelijke risico's. Op deze manier inkopen maakt een organisatie minder kwetsbaar als geopolitieke spanningen ervoor zorgen dat je moet of wilt veranderen van (toe)leverancier. Een bijkomend voordeel is dat het vendor lock-in voorkomt.

Idealiter zou je over bepaalde sectoren heen deze vorm van spreiding willen toepassen om te voorkomen dat bijvoorbeeld alle overheidsinstanties, banken, universiteiten of energiebedrijven afhankelijk zijn van dezelfde toeleveranciers of landen. Dit is echter complex om te bewerkstelligen, zo laat het recente rapport van de Algemene Rekenkamer over het cloudgebruik van de Nederlandse overheid ook zien[4].

[4] https://www.rekenkamer.nl/publicaties/rapporten/2025/01/15/het-rijk-in-de-cloud

Zo'n slimme inkoopstrategie is haalbaar voor met name vitale[5] organisaties en de Rijksoverheid. Voor kleinere (MKB-)organisaties is deze strategie veel moeilijker te realiseren. Deze organisaties willen vaak off-the-shelf oplossingen en beschikken zelf meestal over minder specialistische kennis om hierin weloverwogen keuzes te maken. Wellicht ontstaan er in de toekomst nieuwe leveranciers die deze inkoopstrategie als dienst kunnen leveren en als het ware off-the-shelf een goede leveranciersmix kunnen samenstellen en aan kleine bedrijven kunnen aanbieden. Wel is het concurrentievermogen van dit soort inkoopleveranciers een punt van zorg omdat dit soort diensten kostbaar kunnen zijn. Wellicht zal de overheid de ontwikkeling van dit soort spelers in de markt actief moeten bevorderen en financieel ondersteunen.

2. Fallback oplossingen bij uitval

Veel primaire processen van organisaties zijn tegenwoordig afhankelijk van genetwerkte IT-systemen die verbonden zijn met het Internet. Hierdoor zijn organisaties vaak kwetsbaar als onderdelen uit zo'n systeem uitvallen. Als deze onderdelen het primaire proces raken kan de continuiteit van een organisatie in het geding zijn.

Een relatief nieuw principe bij het ontwerp van IT-systemen is dat van *graceful degradation*. Dit principe houdt in dat als er een probleem optreedt in een IT-systeem, andere delen dan wel blijven functioneren. Weliswaar is dat een verslechtering van het oorspronkelijke systeem, maar er is dan nog geen volledige uitval. Voorbeelden hiervan zijn dat verbindingen doorgaan met een lagere snelheid, dat computersystemen zelfstandig blijven functioneren als er geen internetverbinding is, maar ook fysieke fallback-oplossingen zoals het beschikbaar hebben van actuele telefoonlijsten op papier als computersystemen zijn uitgevallen. Het uitgangspunt is het bouwen van een keten waarbij het wegvallen van een oplossing van een bepaalde leverancier uit de keten beperkte invloed heeft op het functioneren van de keten als totaal.

Redundantie, het dubbel uitvoeren van oplossingen, biedt hiervoor ook een oplossing. Verstandig is om niet alleen oplossingen te dupliceren, maar als vervangende systemen te kiezen voor oplossingen die niet of minder gevoelig zijn voor dezelfde kwetsbaarheid of aanval. Deze aanpak is ook relevant in het kader van digitale autonomie, omdat bij het snel afscheid moeten nemen van een leverancier een redundant systeem van een andere leverancier al in gebruik kan zijn.

[5] We hanteren nu nog de term ' vitale organisaties'. Met de implementatie van de Cyberbeveiligingswet (Cbw)bedoelen we hier de essentiële en belangrijke eniteiten onder de Cbw mee.

Wel moet worden opgemerkt dat dit soort oplossingen kostbaar kunnen zijn in termen van aankoop en beheersbaarheid. Beheerders hebben kennis nodig van een grotere diversiteit aan oplossingen. Ook zorgt een grote keten van verschillende oplossingen voor een groter aanvalsoppervlak. Immers kunnen in alle gebruikte hard- en software kwetsbaarheden zitten die door kwaadwillenden kunnen worden misbruikt.

3. Beter beschermen van gevoelige data

Naast zorgen over het blijven functioneren van IT-infrastructuur en mogelijke uitval is een ander aandachtspunt het beschermen van gevoelige data die in deze infrastructuur wordt opgeslagen en verplaatst. Juist als er IT-systemen worden ingezet waarbij er zorgen bestaan dat een buitenlandse mogendheid toegang tot de data in die systemen kan verkrijgen, is het van belang gevoelige data extra te beschermen.

Voor het beschermen van data wordt veel gebruik gemaakt van encryptiestandaarden. Als data versleuteld wordt opgeslagen, is het lastiger (zo niet onmogelijk) voor derden om zonder een geldige sleutel daar toegang toe te krijgen.

In het kader van digitale soevereiniteit is het daarom van belang om zoveel mogelijk van dit proces onder controle te houden. Denk dan bijvoorbeeld aan het in Nederland (of Europa) produceren van encryptiesleutels, maar ook aan het verder stimuleren van een Nederlandse (en Europese) crypto-industrie en het toepassen van concepten zoals *bring-your-own-key* waardoor je altijd zelf de controle behoudt over encryptiesleutels omdat leveranciers er niet bij kunnen.

Hierop voortbordurend kunnen we vaststellen dat de cybersecurity-industrie nog volop in beweging is en, in tegenstelling tot de IT-industrie, nog wél kansen liggen voor ontwikkeling en innovatie van cybersecurity-oplossingen in Nederland en Europa. Hierin zou dan wel fors moeten worden geïnvesteerd. Ook zou de overheid vaker als launching customer moeten willen optreden van in Nederland en Europa ontwikkelde cybersecuritytechnologie om daarmee de Nederlandse en Europese cybersecuritymarkt te versterken.

4. Inzet van Europese en Nederlandse regulering

Een andere methodiek die kan worden ingezet voor het verkrijgen van meer controle in het kader van digitale soevereiniteit is het *'Brussels Effect'*: het in Europa opstellen van regels voor gebruik van IT-systemen die ervoor zorgen dat leveranciers van buiten Europa aan bepaalde regels moeten voldoen die de digitale soevereiniteit beter waarborgen. CVNL verwacht dat de Network and Information Systems Directive (NIS2, in Nederland geïmplementeerd in de Cyberbeveiligingswet) en de Cyber Resilience Act (CRA, in Nederland de Verordening Cyberweerbaarheid genoemd) hieraan een positieve bijdrage zullen leveren, maar ook de Algemene Beveiligingseisen voor Rijksoverheid Opdrachten (ABRO) die beveiligingseisen stelt aan leveranciers die meewerken aan projecten op gebied van nationale veiligheid. Het effect van deze regulering zal in de komende jaren duidelijker worden.

Nederland zou ten opzichte van deze ontwikkelingen nog verder kunnen gaan door in sommige gevallen Nederlandse bedrijven voorrang te geven bij aanbestedingen voor de Rijksoverheid als het gaat om projecten die een directe relatie hebben met het beschermen van de nationale veiligheid.

5. Fysieke bescherming van de Nederlandse digitale infrastructuur

Tot slot wil CVNL uw aandacht richten op de fysieke beveiliging van digitale infrastructuur. We hebben in het afgelopen jaar gezien dat er kwetsbare plekken zitten in de internationale genetwerkte infrastructuur toen er problemen ontstonden met zeekabels. Aanvallen (of ongelukken?) ontstonden door met een anker over de zeebodem te slepen en zo belangrijke knooppunten in het netwerk te saboteren. Het betreft hier een heel andere aanvalsmethodiek dan het hebben van hoogwaardige IT-kennis om een netwerk digitaal plat te leggen. CVNL adviseert in dit kader om het gehele nationale IT-landschap (van de Rijksoverheid, maar ook van essentiële en belangrijke organisaties (onder de Cyberbeveiligingswet) door deze bril te bekijken en na te gaan of we in de steeds veranderende geopolitieke situatie voldoende weerbaar zijn tegen aanvallen, maar ook uitval als gevolg van fysieke incidenten met onze essentiële digitale infrastructuur.

6. *Versterken van human capital*

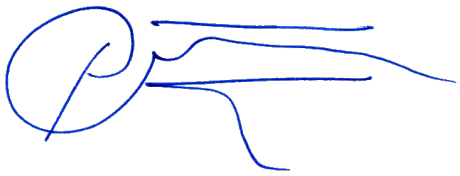
Voorgaande oplossingen zijn niet uitvoerbaar zonder te werken aan het kwalitatieve en kwantitatieve tekort aan cybersecurityprofessionals. Hierover zijn al verschillende rapporten[6] verschenen en vinden al diverse activiteiten op plaats vanuit het ministerie van Economische Zaken die dit vanuit een multi-stakeholder principe heeft opgepakt. Echter het welslagen hiervan vraagt ook politiek commitment én ook om voldoende investeringsbereidheid.

Tot slot

De geopolitieke situatie maakt dat we op een andere manier moeten gaan kijken naar digitale soevereiniteit. We moeten meer controle krijgen over de toeleverancierskeketen in al haar aspecten, waaronder inkoop, uitval, beveiliging van data, regulering, fysieke bescherming en human capital. Om dit te bewerkstelligen zijn er mogelijke oplossingen voorhanden, zoals hierboven geschetst. Om die haalbaar te maken zijn flinke investeringen nodig, ook in menselijk kapitaal (onderzoek en onderwijs) en de wens tot digitale soevereiniteit staat of valt daarom met de bereidheid deze investeringen ook daadwerkelijk te gaan doen.

Graag licht ik bovenstaande tijdens het Rondetafelgesprek op donderdag 13 februari nader aan u toe.

Met vriendelijke groet,
namens Cyberveilig Nederland,



Petra Oldengarm
Directeur

[6] https://intgovforum.org/en/filedepot_download/56/28580
https://www.rijksoverheid.nl/documenten/rapporten/2024/05/15/bijlage-onderzoeksrapport-adviesrapport-onderwijs-en-arbeidsmarkt-cybersecurity-ptvt

Over Cyberveilig Nederland

Cyberveilig Nederland (CVNL) is de belangenvereniging van de cybersecuritysector. In die hoedanigheid maken we ons sterk voor het creëren van meer transparantie en kwaliteit in de markt. Ook behartigen we de belangen van de cybersecuritysector richting stakeholders zoals de overheid, wetenschap en politiek. Onze missie is de digitale weerbaarheid van Nederland te vergroten. Eén van de manieren om dit te bereiken is het delen van dreigingsinformatie. Vanuit CVNL stimuleren we dit actief door samen te werken met relevante overheidspartijen en andere belanghebbenden. In die hoedanigheid zijn we door het ministerie van Justitie en Veiligheid in 2020 aangewezen als schakelorganisatie onder de Wet beveiliging netwerk informatiesystemen (Wbni).[7] Daarnaast spelen we een actieve rol in het tot stand komen van het Cyberweerbaarheidsnetwerk[8], zijn we vanaf de start betrokken bij het Anti Abuse Netwerk (AAN)[9], zijn we deelnemer in het Programma Cyclotron en zijn we mede-initiatiefnemer van Project Melissa waarin we (de gevolgen van) ransomware bestrijden.[10]

[7] https://www.ncsc.nl/actueel/nieuws/2020/december/9/intensievere-informatie-uitwisseling-ncsc-en-nederlandse-cybersecuritybedrijven

[8] https://www.nctv.nl/documenten/publicaties/2024/05/23/toekomstvisie-cyberweerbaarheidsnetwerk

[9] https://www.abuse.nl/

[10] Project Melissa is een samenwerkingsverband tussen publieke en private partijen om ransomware aanvallen te bestrijden. Vanuit de overheid zijn het NCSC, OM en politie betrokken. Het gezamenlijke doel is om Nederland een onaantrekkelijk doelwit te maken voor ransomware criminelen. Zie: https://zoek.officielebekendmakingen.nl/stcrt-2023-29185.pdf