In deze rubriek geven enkele IB-redacteuren in een kort stukje hun reactie op recente nieuwsitems over informatiebeveiliging. Dit zijn persoonlijke reacties van de auteurs en deze geven niet noodzakelijkerwijs het officiële standpunt weer van hun werkgever of van PvIB. Vragen en/of opmerkingen kun je sturen naar ibmagazine@pvib.nl.

De hoogste tijd voor een Ministerie van Digitale Zaken

Op het moment dat de kopij van iB-Magazine nummer 1 wordt ingeleverd is het (nog/alweer) verkiezingstijd. Het nieuws wordt gedomineerd door de campagne, de peilingen en de verhalen in de media over achtergronden en deskundigheden van de politici die door hun partij op de lijst zijn geplaatst. Welke kennis van zaken ten aanzien van cyber brengen deze toekomstige volksvertegenwoordigers in voor de komende regeerperiode?

Er is veel digitaal talent uit de Kamer vertrokken en het is nog even afwachten wie de opvolgers zijn. Volt heeft een heel leger ICT-deskundigen op de lijst staan, maar de instroom zal wel beperkt blijven. De vraag is of dat genoeg is. Levert dat beetje deskundigheid dat uiteindelijk in de Kamer actief wordt voldoende input om de uitdagingen die met name uit het digitale domein op ons afkomen aan te kunnen? Moeten we het niet rigoureus anders aanpakken? Het is de hoogste tijd voor een Ministerie van Digitale Zaken!

Leo van Koppen – Sturing nodig

Ik mag hopen dat – op het moment dat je dit leest – er volop ge(in)formeerd wordt. Aan de informateur zou ik graag de volgende boodschap willen meegeven: maak nu ook eindelijk eens een Ministerie van Digitale Zaken mogelijk! De hele samenleving en economie is inmiddels digitaal geworden, zwaar afhankelijk van al die digitale technologieën die over ons worden uitgestort. Met de uitbreiding van AI in het digitale domein, de komst van meer Europese wetgeving voor het digitale domein en de problemen die we dagelijks ondervinden op het vlak van digitale criminaliteit en warfare, neemt de urgentie toe. Het lijkt me in het kader van een 'nieuwe bestuurscultuur' de hoogste tijd om sturing en een passende invulling te geven aan (veilige) digitalisering dat gestalte krijgt via een apart ministerie met een grote reikwijdte.

In het digitale domein is zoveel te doen en met mijn geringe deskundigheid en met het oog op de lezersdoelgroep beperk ik me nu even tot het takenpakket cyber van zo'n MvDZ. Er ligt al een goede


Fook Hwa Tan


Leo van Koppen

cybersecuritystrategie op de plank met een perspectief tot 2028. Dat past dus precies in de beoogde zittingsperiode van vier jaar. Als je dat document (1) erbij pakt dan zie je dat het gaat om vier pijlers:

I. Digitale weerbaarheid van de overheid, bedrijven en maatschappelijke organisaties;
II. Veilige en innovatieve digitale producten en diensten;
III. Tegengaan van digitale dreigingen van staten en criminelen;
IV. Cybersecurity-arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers.

Graag zou ik er dan direct ook aan willen toevoegen: de leefbaarheid in de digitale samenleving of wellicht nog beter te framen als digitale bestaanszekerheid, maar door anderen soms ook wel aangeduid als privacy.

Ik maak de scope van mijn betoog nog weer wat kleiner omdat mijn kennis van zaken zich met name beperkt tot pijler IV. Bij de doelstellingen en de bijbehorende acties van pijler IV staan al enorme uitdagingen geformuleerd zoals (1) het bewustzijn van cyberrisico's bij burgers vergroten. Wat ik wekelijks als vrijwilliger in de bibliotheek (op zo'n digitaal informatiepunt) meemaak is dat het niet gaat om bewustzijn, maar dat enorme gebrek aan digitale kennis en vaardigheden leidt tot angst en grote onkunde. Daar is dus nog een hele lange weg te gaan.

Een ander actiepunt van pijler IV is (2) het aanbrengen van cybervaardigheden in het basis- en voortgezet onderwijs. Dat dient opgenomen te worden in alle curricula! Ja, papier is geduldig, maar hoe zorg je ervoor dat die overbelaste docenten, die toch al steeds nieuwe apen op hun schouders geplaatst zien, deze vaardigheden kunnen aanleren als ze deze zelf onvoldoende beheersen? Daar moet de nodige ondersteuning voor worden ingericht wil dat op korte termijn succesvol kunnen zijn.

En last but not least (3) aandacht voor cybersecurity op de arbeidsmarkt. Cyberspecialisten opleiden is al tijden een enorme uitdaging, via initieel onderwijs, via omscholing en via bij- en nascholing etc. Bijzondere opleidingstrajecten zoals ITvitae of als DIVD-Academy die aansluiten op speciale doelgroepen, zijn prachtig. De vraag die ik al jaren stel is: waar halen we al die deskundigen en de deskundigheid vandaan om de opleiders te ondersteunen in hun taak om al de cyberkennis tussen de oren van de verschillende doelgroepen te krijgen? Formateur en ook PvIB-leden, er wacht u een schone taak!

Fook Hwa Tan – Kritische kijk op de noodzaak van een Ministerie van Digitale Zaken

In een tijd waarin verkiezingskoorts hoogtij viert, blijkt de schaarste aan digitale deskundigheid in de Tweede Kamer een zorgwekkend hiaat. Terwijl de verkiezingscampagnes, peilingen en mediaverhalen over politici de headlines domineren, blijft de cruciale vraag hangen: welke expertise brengen onze toekomstige volksvertegenwoordigers met zich mee op het gebied van cybersecurity? Terwijl de roep om een Ministerie van Digitale Zaken steeds luider klinkt, is het belangrijk om een kritische blik te werpen op de vraag of dit werkelijk de oplossing is voor de digitale uitdagingen waar Nederland voor staat. Hier zijn enkele redenen waarom een dergelijk ministerie mogelijk niet de panacee is die sommigen verwachten.

- Nederland beschikt al over bestaande organen, zoals het Nationaal Cyber Security Centrum (NCSC) en het ministerie van Justitie en Veiligheid, die digitale veiligheid behandelen. Het oprichten van een nieuw ministerie zou kunnen leiden tot overlapping van verantwoordelijkheden en bureaucratie, eerder dan tot een efficiënte aanpak.
- Het digitale landschap evolueert voortdurend, en een statisch ministerie zou moeite kunnen hebben om gelijke tred te houden. Flexibele en snelle reacties zijn cruciaal bij cyberdreigingen, en een nieuw ministerie kan leiden tot trage besluitvorming en implementatie.
- Het pleidooi voor een specifiek ministerie suggereert mogelijk een gebrek aan samenwerking tussen bestaande instanties. In plaats van een nieuw ministerie op te richten, zou de focus moeten liggen op het versterken van samenwerking en coördinatie tussen de reeds bestaande organen.
- Het oprichten van een nieuw ministerie vergt aanzienlijke financiële middelen. In een tijd waarin overheidsbudgetten onder druk staan, moet de vraag worden gesteld of deze middelen niet effectiever elders kunnen worden ingezet, bijvoorbeeld in het versterken van bestaande digitale veiligheidsstructuren.
- In plaats van een algemeen ministerie zou een sectorgerichte aanpak wellicht effectiever zijn. Door samen te werken met experts uit de industrie en het bedrijfsleven kan de overheid gerichte oplossingen ontwikkelen die beter aansluiten bij specifieke behoeften en uitdagingen.

Hoewel de roep om meer aandacht voor digitale veiligheid begrijpelijk is, moeten we voorzichtig zijn met het omarmen van een nieuwe laag van bureaucratie zonder de mogelijke nadelen zorgvuldig te overwegen. Wellicht is het versterken van bestaande structuren en het bevorderen van samenwerking een pragmatischer alternatief.

Referentie

(1) Nederlandse Cybersecuritystrategie 2022-2028 Ambities en acties voor een digitaal veilige samenleving