INFORMATIEBEVEILIGING MAGAZINE

DOSSIERS

- Soevereiniteit
- Competentie
- Quantum perikelen

JAARGANG 26 - 2026 - EDITIE 3

PvIB Platform voor InformatieBeveiliging

COLOFON

IB Magazine is het huisorgaan van het Platform voor InformatieBeveiliging (PvIB) en bevat ontwikkelingen en achtergronden over onderwerpen op het gebied van informatiebeveiliging.

HOOFDREDACTEUR
Chris de Vries

REDACTIE
Tim Deahl
Alex Dingemanse
Maarten Hartsuijker
Lilian Knippenberg
Leo van Koppen
Rachel Marbus
Fook Hwa Tan
Chris de Vries
Zoëlle Yusufi

BLADMANAGEMENT
Congres- en Organisatiebureau Interactie BV
Zeynep Turkan
ibmagazine@pvib.nl

VORMGEVING
Neverseen Art & Design
Dimitri van den Berg

DRUK
Veldhuis Media, Meppel

UITGEVER
Platform voor InformatieBeveiliging (PvIB)
Horapark 9
6717LZ Ede
+31 85 799 0233
secretariaat@pvib.nl
www.pvib.nl

Heb je vragen, opmerkingen of suggesties, mail dan naar ibmagazine@pvib.nl

ABONNEMENTEN
De abonnementsprijs in 2026 bedraagt € 123,- (exclusief btw), prijswijzigingen voorbehouden.

ABONNEMENTENADMINISTRATIE
Platform voor InformatieBeveiliging (PvIB)
Postbus 1058
3860 BB NIJKERK
secretariaat@pvib.nl

ISSN 1569-1063

Soevereiniteit en competentie

Chris de Vries

Twee betekenisvolle woorden, die ons alles zeggen en centraal staan in het informatiebeveiligingsdenken. Of niet soms? "Nee" dus; want achter dergelijke begrippen schuilen de woorden: "onafhankelijkheid en vaardigheid". Dat kan je weer vertalen naar niet "slaaf zijn" en "praktische ervaring door korte of langere tijd regelmatig te oefenen"!

Als wij dat meenemen in ons vak, dan zien wij de reactie op cybersecurityrisico's als meer dan een technisch spel van aanval en verdediging. Meer dan een training op willekeurig welk speelveld dan ook, meer dan persoonlijke slimheid om flexibel, snel en effectief te reageren op veranderingen.

Soevereiniteit en competentie, als modewoorden en voortkomende uit angst, zijn zonder betekenis, zijn loos (niet echt). Om de Duitse jurist & schrijver, Hans Krailsheimer (29.01.1888 – 12.01.1958) aan te halen: "Men moet er zich voor hoeden, slaaf te worden van zijn onafhankelijkheid".

Neem dat als uitgangspunt bij het lezen van het artikel van Ron Kolkman (RWS), die de vraag stelt: "Wat werken blijft, als het mis gaat!?" of Etienne Lemmens artikel over "Wat 25 gemeentelijke rekenkamerrapporten onthullen". Plaats de kritiek daarnaast - begin mei geuit op de radio, vermoedelijk door een ingenieur van RWS – dat de werkelijke technische kennis van/inzichten op waterwerken is wegbezuinigd door economen en juristen.

Zijn standpunt; in opdracht van politici formuleren economen en juristen uitstekend overeenkomsten, rekenen perfect de kostprijzen, terugverdientijden en winsten uit; maar hebben geen oog voor slijtage, noodzaak tot onderhoud, renovatie en vernieuwing. De missende praktische ervaring leidt ertoe dat essentiële infrastructuur op hetzelfde moment het einde van hun technische levensduur bereikt. Op de korte termijn (politieke) budgetten gespaard en schijnwinst geboekt, op de (middel)lange termijn de problemen verschoven naar de volgende generatie c.q. volgende kabinetten. Adagio: "na ons de zondvloed".

Ons dossier in dit nummer: soevereiniteit, wordt ook teruggevonden in de artikelen van het CBS ("Geen project, maar principe:...") en de gemeente Oss ("Besturen in de mist: ..."). Veelzeggende titels!

Ons tweede dossier: competentie wordt gevoed door Stephan Corporaal c.s., waarbij zij ingaan op de "... cybercompetentietekorten in Europa". Dit aan de hand van het Europese CADMUS project en de richtinggevende 'learning communities' bij het MKB, zie het kader aldaar. Ook Jolanda ter Maten gaat in op de vaardigheid van mensen, specifiek op het leiderschap ('De firewall die we vergeten te bouwen:..."). Een geheel andere vermogens- dan wel kwaliteitsorde brengt Ronald Eygendaal op tafel met zijn "Veilig in het verkeer met Open Source" bijdrage.

Tot slot als dessert het derde dossier: Quantum perikelen - de artikelen van TNO en de Algemene Rekenkamer. Zij adresseren quantumveilige PKI c.q. de quantumdreiging voor de Rijksoverheid.

'Moge de competentie oftewel de vaardigheid dan wel de ervaring met jullie zijn' bij het nuttigen van het leesvoer in dit nummer, of zoals Oscar Wilde zo treffend schreef/zei: "Ervaring is de naam die we aan de som van onze fouten geven." Ik wens ons redacteuren en de lezer, vele fouten toe!

Chris

Veel leesplezier en graag tot de volgende uitgave.

IN DIT NUMMER

Auteur: Etienne Lemmens (1958) is sociaal en economisch historicus, zelfstandig onderzoeker en lid/voorzitter van drie gemeentelijke rekenkamers. Naast onderzoeker is Etienne bestuurssecretaris van de Vereniging van Rekenkamers en voorzitter van de Raad van Toezicht van Stichting de Tussenvoorziening, onder andere voor daklozenopvang in Utrecht en omgeving. Etienne Lemmens is bereikbaar via: etienne.lemmens@rekenkamers.nl

Informatiebeveiliging bij gemeenten

Wat 25 rekenkamerrapporten onthullen

Gemeenten beheren enorme hoeveelheden persoonsgegevens van hun inwoners – van belastinggegevens en bijstandsdossiers tot jeugdzorgrapportages en schuldhulpverleningstrajecten. De bescherming van die gegevens is niet alleen een technische opgave, maar raakt aan het fundament van het vertrouwen van burgers in de overheid. De afgelopen jaren hebben diverse lokale rekenkamers onderzocht hoe het met die bescherming is gesteld. Hun bevindingen zijn alarmerend consistent.

Voor dit artikel zijn 25 rekenkamerrapporten over informatiebeveiliging en privacy bij gemeenten geanalyseerd, gepubliceerd tussen 2021 en begin 2025. De rapporten beslaan gemeenten van uiteenlopende omvang – van kleine plattelandsgemeenten als Rhenen en Baarn tot steden als Eindhoven en 's-Hertogenbosch. Wat opvalt is niet zozeer de diversiteit in bevindingen, maar juist de opvallende gelijkluidendheid. Er tekenen zich rode draden af die vragen oproepen over de digitale weerbaarheid van het lokaal bestuur. Tot slot ga ik in op wat de Vereniging van Rekenkamers doet ter ondersteuning van de leden op het gebied van informatiebeveiliging.

De aanpak: hoe rekenkamers te werk gaan

De rekenkamers hanteren vrijwel allemaal dezelfde onderzoeksaanpak. Het vertrekpunt is een documentenanalyse van het geldende beleid, gevolgd door interviews met sleutelfunctionarissen zoals de CISO, de **F**unctionaris **G**egevensbescherming (FG), Privacy Officer(s) en betrokken lijnmanagers. Als gemeenten op ICT en informatieveiligheid samenwerken in een **S**hared **S**ervice **C**entrum (SSC) of op basis van een gastheerschap, dan worden deze partners ook betrokken in het onderzoek. De meeste rekenkamers toetsen de organisatie langs de assen: mens, proces en techniek en maken gebruik van volwassenheidsmodellen om de stand van zaken te objectiveren.

Veel rekenkamers huren een extern onderzoeksbureau in voor de uitvoering van het onderzoek, een klein aantal voert het zelf uit. Tien van de 25 rekenkamers gaan een stap verder en zetten ethische hackers in om de beveiliging in de praktijk te testen. De ingezette testen variëren breed: van externe en interne penetratietesten, Active Directory-audits en wifi-pentesten tot social engineering in de vorm van phishingcampagnes, smishing en mystery guest-bezoeken aan het gemeentehuis. Meerdere rekenkamers rapporteren dat ethische hackers erin slaagden om via nagemaakte e-mails inloggegevens van medewerkers – en soms raads- en collegeleden – te bemachtigen of om fysiek ongehinderd beveiligde kantoren en technische ruimten te bereiken. De keuze om ethische hackers in te zetten maakt de bevindingen en conclusies concreet en onweerlegbaar; het verschil tussen beleidsanalyse en een daadwerkelijke inlooptest is voor een gemeenteraad onmiddellijk invoelbaar.

Rode draden: vijf terugkerende tekortkomingen

Uit de analyse komen vijf rode draden naar voren die in vrijwel alle rapporten terugkeren. Samen vormen zij het beeld van een sector die enigszins worstelt met de overgang van papieren beleid naar daadwerkelijke beheersing van informatieveiligheid in het kader van risicomanagement.

De meeste gemeenten scoren op volwassenheidsmodellen tussen niveau 1 (ad hoc) en niveau 2 (herhaalbaar) op een vijfpuntsschaal. Om daadwerkelijk 'in control' te zijn, wordt over

Rode draad	Kernbevinding
Verouderd beleid	Beleid voldoet niet aan BIO en AVG, is te abstract of niet geëvalueerd
Ontbrekende PDCA-cyclus	Risicomanagement is ad hoc; de check- en act-fase ontbreken
Bewustwording onvoldoende	De menselijke factor is de grootste kwetsbaarheid; trainingen zijn niet structureel of verplicht
Raad onvoldoende geïnformeerd	Informatie is te technisch, te summier of niet gericht op sturing en de rol van de raad
Regie op derden zwak	Onvoldoende controle op ketenpartners, SSC's en leveranciers

Meerdere rekenkamers constateren dat gemeenten nog onvoldoende zijn voorbereid op wat komen gaat.

het algemeen minimaal niveau 3 (gedefinieerd) aangehouden. Opvallend is het verschil tussen afdelingen: teams die jarenlang met privacygevoelige informatie werken, zoals Burgerzaken en het Sociaal Domein, tonen vaker een hoger risicobewustzijn dan de rest van de organisatie. Dat zijn ook medewerkers die te maken hebben met strenge landelijke beveiligingseisen rond Suwinet en DigiD – een indicatie dat toezicht wél werkt.

De IB-professional: gewaardeerd maar geketend

Uit de rekenkamerrapporten blijkt dat de vakinhoudelijke expertise van CISO's, FG'n en Privacy Officers breed in de gemeentelijke organisaties wordt gewaardeerd, maar hun organisatorische positie knelt vaak op drie punten.

In de eerste plaats betreft het de positionering en onafhankelijkheid. Rekenkamers adviseren herhaaldelijk om de CISO en FG onafhankelijk van de lijn te positioneren, dus buiten de ICT-afdeling, bijvoorbeeld bij Control of als rechtstreekse adviseur van de gemeentesecretaris. Wanneer zij 'verstopt' zitten in de ICT-organisatie, wordt informatiebeveiliging ten onrechte als een louter technische kwestie gezien en is de afstand tot het bestuur te groot. In kleinere gemeenten vindt regelmatig geen functiescheiding plaats en worden rollen vaak door dezelfde persoon vervuld. Rekenkamers ontraden combinaties, omdat het kan voorkomen dat de toezichthouder toeziet op beleid dat hij zelf mee heeft ontwikkeld.

Het tweede knelpunt is het mandaat. CISO's missen in enkele gemeenten de bevoegdheid om beveiligingsmaatregelen daadwerkelijk af te dwingen. Hun adviezen kunnen soms door lijnmanagers overruled worden. Sommige rekenkamers bepleiten een mandaat en een eigen budget voor de CISO om de noodzakelijke onafhankelijkheid te waarborgen.
En ten derde, is het gebrek aan capaciteit en continuïteit. Functies worden voor te weinig uren ingevuld, er is geen achtervang bij ziekte of vertrek en de krappe arbeidsmarkt maakt werving bijzonder lastig. Het gevolg is een vicieuze cirkel: doordat de lijnorganisatie onvoldoende volwassen is, wordt de CISO overspoeld met operationele ad-hoc-vragen en komt deze niet toe aan de strategische en toezichthoudende taken. Informatieveiligheid blijft zo 'het technische feestje van de CISO', terwijl het eigenaarschap bij de proceseigenaren in de lijn hoort te liggen.

De klok van NIS2 tikt

In de rapporten uit 2024 en 2025 komt de NIS2-richtlijn prominent naar voren als gamechanger voor gemeenten. Deze Europese richtlijn wordt in Nederland vertaald naar de Cyberbeveiligingswet, die gemeenten definieert als aanbieders van essentiële diensten onder strengere beveiligingsnormen vallen met een wettelijke zorg- en meldplicht voor incidenten. De **B**aseline **I**nformatiebeveiliging **O**verheid (BIO) wordt doorontwikkeld naar de BIO2 om aan de Europese eisen te voldoen; en het voldoen aan die normen wordt wettelijk verplicht.

De implicaties voor gemeenten zijn ingrijpend. Waar de meeste gemeenten momenteel op volwassenheidsniveau tót 3 opereren, vereist de Cyberbeveiligingswet een doorgroei naar niveau 4 (gemanaged). De verantwoordelijkheid voor informatiebeveiliging wordt expliciet bij het bestuur gelegd. Er komt proactief toezicht vanuit de Rijksinspectie Digitale Infrastructuur (RDI), bovenop het huidige horizontale toezicht via de gemeenteraad. En de invoering brengt aanzienlijke taakverzwaring en extra kosten met zich mee.

Meerdere rekenkamers constateren dat gemeenten nog onvoldoende zijn voorbereid op wat komen gaat. In sommige onderzoeken uit begin 2024 werd genoteerd dat er op dat moment 'weinig aandacht' aan NIS2 werd besteed. Als gemeenten er nu al niet in slagen om aan de bestaande BIO-normen te voldoen, ligt er nog een behoorlijk grote uitdaging om te gaan voldoen aan de aanzienlijk strengere eisen van de Cyberbeveiligingswet.

De gemeenteraad: kadersteller op afstand

Een van de meest opvallende rode draden betreft de positie van de gemeenteraad. De raad is formeel verantwoordelijk voor kaderstelling en controle van het beleid, maar vult deze rol volgens de rekenkamers op informatiebeveiliging nauwelijks in. Er zijn nog steeds colleges die het onderwerp primair als bedrijfsvoering beschouwen en raden zien vaak voor zichzelf weinig politieke keuzeruimte. In de praktijk stelt de raad zelden zelf strategische kaders of ambities vast en doet het college dat op basis van landelijke normen.

De informatiepositie van raadsleden wordt door rekenkamers als structureel tekortschietend gekwalificeerd. De raad wordt geïnformeerd via de planning-en-controlcyclus en de jaarlijkse ENSIA-verantwoording – documenten die als te summier, te technisch en onvoldoende sturingsgericht worden ervaren. Vaak komen de opmerkingen over informatieveiligheid uit de managementletter van de accountant alleen ter sprake in een auditcommissie, maar komen niet aan bij de voltallige raad. Er is weinig inzicht in de maatschappelijke effecten van het beleid. De aandacht voor het thema piekt vrijwel uitsluitend na grote hackincidenten bij andere gemeenten, zoals bij de gemeenten Hof van Twente of Buren of recenter een bedrijf als Odido, en ebt daarna weer weg. Jargon en afkortingen vormen een extra barrière en de kloof in kennisniveau tussen raadsleden is groot.

Raadsleden blijken bovendien zelf een kwetsbare schakel. Pentesten tonen aan dat zij soms gevoelig zijn voor phishing en niet altijd de beveiligde gemeentelijke mailaccounts of de tweefactorauthenticatie gebruiken. Rekenkamers doen concrete aanbevelingen: laat de raad expliciet ambities en het gewenste beveiligingsniveau vaststellen, zet de auditcommissie in als vooruitgeschoven post, geef de externe accountant een gerichte IT-auditopdracht en organiseer verplichte bewustwordingssessies voor raadsleden.

Privacy in het sociaal domein: een spanningsveld

Verschillende rekenkamers zoomen specifiek in op het sociaal domein, waar gemeenten grote hoeveelheden bijzondere persoonsgegevens verwerken in jeugdzorg, Wmo en participatiewet. Hier tekent zich een inherente spanning af tussen de integrale aanpak, waarbij teams informatie delen voor betere hulpverlening en de strikte regels van de AVG. Medewerkers ervaren die regels als belemmerend bij complexe casussen of vroegsignalering.

Structurele tekortkomingen zijn de gebrekkige regie op ketenpartners die namens de gemeente persoonsgegevens verwerken, het achterblijven van verplichte DPIA's op risicovolle processen, en fysieke kwetsbaarheden op locaties waar cliëntgesprekken plaatsvinden. Denk aan afluisterbare spreekkamers en papieren dossiers omdat systemen niet aan elkaar gekoppeld kunnen worden. Rekenkamers adviseren om het privacybeleid te herijken met praktische handvatten voor de specifieke dilemma's in het sociaal domein en de spanning tussen dienstverlening en privacy expliciet bespreekbaar te maken.

Kritiek op het landelijke stelsel

Hoewel rekenkamers formeel hun rapport adresseren aan de eigen gemeenteraad, richten diverse rapporten hun pijlen ook op het landelijke kader. Zij constateren dat het door Rijk en VNG opgetuigde systeem van BIO en ENSIA dermate complex is dat het, vooral bij kleinere gemeenten, leidt tot onduidelijkheid over rollen en taken. Een terugkerende kritiek is dat ENSIA-audits toetsen of het juiste instrumentarium aanwezig is, maar niet of dit daadwerkelijk bijdraagt aan de veiligheid van inwoners: het gevaar dreigt van het maken van vinklijstjes in plaats van het bevorderen van veiligheid. De opzet van de nieuwe BIO2 lijkt meer aandacht te besteden aan de werking van het informatieveiligheidsbeleid dan alleen het bestaan en opzet van het beleid.

Daarnaast signaleren rekenkamers dat individuele gemeenten te klein zijn om effectief te onderhandelen met grote leveranciers. De aanbeveling is om via de VNG en **I**nformatie **B**eveiligings **D**ienst (IBD) collectief meer gewicht in de schaal te leggen. Voor regionale ICT-samenwerkingsverbanden (SSC's) geldt dat de governance vaak te licht is ingericht en de onderlinge afspraken over aansprakelijkheid bij grote incidenten niet goed geregeld zijn.

Vragen die blijven hangen

Deze analyse levert een beeld op dat zowel herkenbaar als ook enigszins verontrustend is. De bevindingen zijn geen verrassing voor wie in het vakgebied werkt, maar de consistentie ervan over tientallen gemeenten heen maakt ze lastig te negeren.

De centrale vraag is er een van tempo en schaal. Nederland loopt weliswaar achter op de invoering van de Cyberbeveiligingswet en deze nadert wel snel. Maar de meeste gemeenten opereren op een volwassenheidsniveau dat zelfs aan de huidige normen niet voldoet. De CISO's en FG'n die de transitie moeten begeleiden, missen vaak mandaat, capaciteit en organisatorische onafhankelijkheid. De gemeenteraden die de kaders moeten stellen, beschikken niet over de informatie om dat effectief te doen. En het landelijke stelsel dat richting

moet geven, wordt door de rekenkamers als te complex en te weinig effectief beoordeeld.

Wat deze verzameling rekenkamerrapporten uiteindelijk laat zien, is dat informatiebeveiliging bij gemeenten niet alleen een technisch probleem is dat met enkel technische oplossingen kan worden opgelost. Het is een governancevraagstuk, een kwestie van eigenaarschap, verantwoording en politieke prioritering. Het is mijn ervaring bij de afdronk van de rapporten over informatieveiligheid dat de professionals, in sommige gevallen eerst huiverig ten aanzien van een rekenkameronderzoek, uiteindelijk zeer tevreden zijn met het effect. Zij ervaren dat het rekenkamerrapport het onderwerp op een goede manier bij de raad onder de aandacht brengt, de bestuurlijke bewustwording stimuleert en dat zij daardoor op de juiste tafels hun punten kunnen agenderen.

De Vereniging van Rekenkamers

Dan is natuurlijk de vraag of alle rekenkamers het zelf netjes voor elkaar hebben op het gebied van informatiebeveiliging? Daar durf ik mijn hand niet voor in het vuur te steken. Probleem is dat rekenkamers niet altijd goed geoutilleerd zijn met voldoende middelen en menskracht. De rekenkamers in de grotere steden en provincies beschikken vaak over een professioneel apparaat dat hen in staat stelt om de zaken op orde te hebben, ook op het gebied van informatieveiligheid en privacy. Maar de grote meerderheid betreft rekenkamers met een beperkt budget, met leden die het rekenkamerwerk als (kleine) bijbaan uitvoeren en niet beschikken over uitgebreide ondersteuning van een secretariaat.

De Vereniging van Rekenkamers (VvR) tracht alle rekenkamers zo goed mogelijk te ondersteunen in hun werkzaamheden. Dat doet de vereniging onder andere door opleidingen, cursussen en kennisdeling. Ook over het stelsel van toezicht op de uitvoering van de Cyberbeveiligingswet (Cbw) heeft de vereniging meegedacht. De VvR nam deel aan de begeleidingscommissie van een onderzoek dat werd uitgevoerd in opdracht van de Vereniging Nederlandse Gemeenten (VNG), het InterProvinciaal Overleg (IPO) en de Unie van Waterschappen (UvW). De onderzoeksvraag was hoe het horizontale en verticale toezicht van de Cbw bij decentrale overheden ingericht zou kunnen worden en of decentrale rekenkamers daar een rol in zouden kunnen vervullen. Het antwoord op die laatste vraag is dat, gelet op de wijze waarop de rekenkamerfunctie wettelijk is ingericht, deze hierop geen

De Vereniging van Rekenkamers tracht alle rekenkamers zo goed mogelijk te ondersteunen in hun werkzaamheden

structurele rol kunnen vervullen. Wel een incidentele rol, door periodiek onderzoek te doen.

Om de onderzoeksfunctie van rekenkamers te ondersteunen brengt de Vereniging van Rekenkamers jaarlijks twee metadossiers en meta-analyses over verschillende onderzoeksonderwerpen uit (zie rekenkamers.nl/meta). Een paar jaar geleden heeft de vereniging via een metadossier een grote hoeveelheid rekenkamerrapporten over informatiebeveiliging ontsloten. Daarmee kunnen rekenkamers leren van andere rekenkamers hoe een onderzoek op dat terrein uitgevoerd kan worden. De Vereniging denkt nog na over een meta-analyse op informatiebeveiliging, waarin de onderzoeksresultaten van de verzamelde rapporten naar een hoger analyseniveau worden getild. In dit artikel is al een aanzet daartoe te vinden.

Tevens heeft de vereniging een vraagbaakfunctie en we zien dat daar veel vragen binnenkomen over de wettelijke verplichtingen, onder andere met betrekking tot AVG, de Wet Open Overheid (WOO) en de Archiefwet. Een paar jaar geleden is een dossier aangelegd waarin veel vragen op het gebied van de AVG worden beantwoord. Over de Cyberbeveiligingswet komen nog relatief weinig vragen binnen. Hier ligt een taak voor de vereniging om rekenkamers te ondersteunen bij hun eigen informatieveiligheid. Zo is de VvR zich onder andere aan het oriënteren om een gezamenlijke FG-functie voor rekenkamers in te richten en een beveiligde mail- en webpaginafunctie voor rekenkamers te organiseren.

Auteur: Zoëlle Yusufi is redacteur van InformatieBeveiliging Magazine. Dit diepte-interview met Ron Kolkman, CIO bij Rijkswaterstaat (RWS) gaat in op de fundamentele keuzes achter onze digitale infrastructuur. Samen ontleden zij de wisselwerking tussen technologische vooruitgang én de noodzaak voor strategische autonomie binnen de overheid. Zoëlle Yusufi is bereikbaar via: zoelle.yusufi@rvo.nl

Wat blijft werken als het erop aankomt?

Rijkswaterstaat over digitale weerbaarheid

In een wereld waar digitalisering steeds meer verweven is met geopolitieke belangen, is digitale soevereiniteit voor overheden cruciaal. Ron Kolkman, sinds 2022 CIO en hoofdingenieur-directeur van de Centrale Informatievoorziening bij Rijkswaterstaat, leidt een ambitieus project: de ontwikkeling van een soevereine cloud voor de Nederlandse overheid. Als CIO van Rijkswaterstaat heeft hij een sleutelrol in het strategisch vormgeven van de toekomst van informatievoorziening in de publieke sector.

In dit interview deelt Ron Kolkman zijn visie op digitale onafhankelijkheid, de rol van kunstmatige intelligentie (AI), en de geopolitieke risico's die de digitale infrastructuren van overheden beïnvloeden. Hij leidt het aanjaagteam Cloud, dat werkt aan een veilige, betrouwbare cloudinfrastructuur voor de overheid en wil daarmee de afhankelijkheid van niet-Europese leveranciers verminderen. Wat zijn de technologische keuzes die gemaakt moeten worden? Hoe kijkt Ron Kolkman naar de uitdagingen van vandaag en de digitale toekomst van Nederland? Lees verder voor inzichten van een van de leiders in de digitale transformatie van de publieke sector.

Digitale weerbaarheid staat bij veel organisaties hoog op de agenda. Toch blijft één vraag in de praktijk vaak onderbelicht: werkt het ook echt als het misgaat?
Niet in een dashboard. Niet in een auditrapport. Maar het werkt op het moment dat systemen uitvallen, leveranciers wegvallen of besluitvorming onder druk komt te staan.
Juist daar ligt de waarde van de lessen uit de praktijk van Rijkswaterstaat. In een tijd van AI, geopolitieke spanningen, groeiende afhankelijkheden en toenemende regeldruk laat de organisatie zien dat digitale veiligheid meer vraagt dan compliance. Het vraagt om vakmanschap, een goede relatie met je leveranciers en bestuurlijke keuzes.

Lessen uit ervaring, niet uit beleid

Ik heb aan de start van mijn loopbaan ergens gewerkt waar een computervirus uitbrak en we 17.000 computers handmatig moesten resetten. Dat gaf heel veel stress. Toen heb ik in de praktijk ervaren hoe belangrijk het is om je IT op orde te hebben. Die awareness wordt steeds belangrijker. IT is al lang geen ondersteunende functie meer, maar een randvoorwaarde voor continuïteit, reputatie en vertrouwen.
Wie ooit een grote verstoring heeft meegemaakt, weet dat voorkomen altijd goedkoper is dan herstellen. Een crisis vergeet je nooit meer, sommige lessen leer je niet uit beleid, maar uit ervaring.

''Meer dan wetenschap omtrent te beschermen belangen''

Digitale weerbaarheid begint met een eenvoudige vraag:"Wat mag nooit uitvallen"?
Voor de ene organisatie zijn dat klantprocessen, voor de andere financiële systemen of zorgverlening. Voor Rijkswaterstaat gaat het om vitale infrastructuur zoals: bruggen, tunnels en waterkeringen. Daarbij sturen IT-systemen soms direct op fysieke processen. Digitale continuïteit is daarmee ook maatschappelijke continuïteit.
De les is breder toepasbaar: elke organisatie moet weten waar de kroonjuwelen zitten, welke processen kritiek zijn en hoe die doorgaan als technologie tijdelijk niet beschikbaar is. Dat is de kern van business continuity management.

Life-cycle management is strategisch relevant

Niet elk cruciaal onderwerp klinkt spectaculair. Life-cycle management is daar een goed voorbeeld van. De boodschap is helder: systemen, software en infrastructuur tijdig onderhouden, vervangen en vernieuwen is geen technisch detail, maar een bestuurlijke noodzaak.
Bestuurders hoeven geen technici te zijn, maar moeten wel begrijpen dat uitstel op dit terrein later veel grotere risico's veroorzaakt. Verouderde technologie leidt tot:

- hogere kans op storingen
- meer beveiligingsrisico's
- oplopende kosten
- minder wendbaarheid
- grotere afhankelijkheid van leveranciers

Zoals scherp werd gezegd:"Life-cycle management moet doorgaan."

Van 'uitbesteding tenzij' naar regie

Rijkswaterstaat maakt een belangrijke koerswijziging door. Jarenlang lag veel nadruk op uitbesteden aan de markt. Dat model heeft voordelen, maar kent ook grenzen.
Wie zelf onvoldoende kennis behoudt, verliest het vermogen om (bij) te sturen en te toetsen. Daarom investeert de organisatie nadrukkelijk in eigen vakmensen en regiefuncties.
Niet omdat alles intern moet gebeuren, maar omdat publieke organisaties altijd zelf moeten kunnen beoordelen of continuïteit, veiligheid en kwaliteit voldoende zijn geborgd.
De vergelijking met de bekende "oranje jas langs de weg" maakt dat tastbaar. Als je niet meer buiten staat, verlies je gevoel met wat daar gebeurt. Voor IT geldt hetzelfde. Je kunt goed regie voeren als je weet en ziet wat er gebeurt.

Daarnaast moet bestuur en management een goed beeld hebben van de uitdagingen van de uitvoering. Technische teams zien risico's vaak eerder dan de top van de organisatie. Het is belangrijk dat signalen goed doorkomen. Als dit niet gebeurt dan kan dit risicovol zijn. Zeker wanneer waarschuwingen over achterstallig onderhoud, afhankelijkheden of life-cycle management te lang blijven liggen. Daarom is één principe cruciaal: bestuur en uitvoering moeten elkaars taal begrijpen. Digitale kennis hoort daarmee niet alleen bij de CIO, maar in de volle breedte van het bestuur.

''De belangrijkste maatregel zit niet in techniek''

Volgens Ron is dit cruciaal. Wanneer technici jarenlang signa-

leren dat het life-cycle management achterblijft, maar daar bestuurlijk geen actie op volgt, ontstaat er een kloof tussen ‘’boven de wolken‘’ en ‘’onder de wolken.‘’

Bestuurders hoeven geen servers te bouwen of code te schrijven, maar zij moeten wel over voldoende IT-kennis beschikken om de juiste vragen te stellen, investeringen af te wegen en risico’s te begrijpen. De CIO verwoordt het scherp: het streven zou moeten zijn dat digitale kennis vanzelfsprekend is op bestuursniveau. De vraag is of er dan nog een CIO nodig is.

Naast processen en techniek benoemt Ron Kolkman een vaak onderschatte factor: leiderschap. De echte vraag is niet alleen welke controls of rapportages er zijn, maar hoe leidinggevenden omgaan met signalen over technische kwetsbaarheden vanuit de werkvloer. ‘’Luisteren we voldoende naar specialisten wanneer risico's worden gemeld? Worden waarschuwingen serieus genomen of komt de aandacht pas wanneer systemen al zijn uitgevallen? Wanneer medewerkers het gevoel hebben dat signalen worden genegeerd, stoppen zij op termijn met melden. Juist dan worden risico’s het gevaarlijkst.‘’ Het is belangrijk om vaker actief op de werkvloer aanwezig te zijn om signalen op te vangen en te waarderen.
De oproep is helder: ‘’Omarm het probleem‘’

AI, geopolitiek en digitale soevereiniteit

De digitale werkelijkheid wordt complexer. Kunstmatige intelligentie, cloudplatforms en internationale leveranciers creëren nieuwe kansen, maar ook nieuwe afhankelijkheden.
Zoals treffend werd gezegd: “De impact van leveranciers uit niet-Europese landen en de afhankelijkheid daarvan is groter dan we hadden gedacht. Dat noodzaakt tot nieuwe bestuurlijke vragen” waaronder:

- waar staat onze data?
- wie beheert kritieke technologie?
- onder welke wetgeving vallen leveranciers?
- kunnen we overstappen als dat nodig is?
- wat gebeurt er als toegang, prijzen of voorwaarden veranderen?

Dat is de kern van digitale soevereiniteit: niet alles zelf doen, maar wel begrijpen waarvan je afhankelijk bent, welke risico’s je accepteert en welke alternatieven je hebt.
Het Europese soevereiniteit framework geeft daar hele goede handvatten voor. Daarnaast moet je weten met welk bedrijf je zaken doet.
"Een sterke relatie met leveranciers is daarom voor mij belangrijk". Jaarlijks nemen we onze belangrijkste leveranciers mee 'de vloer' op, langs onze civiele constructies en waterbouwkundige werken. Zo ervaren zij zelf de impact van hun dienstverlening op de Nederlandse samenleving. Zo creëren we juist wederzijds begrip en gezamenlijke verantwoordelijkheid.

”Zonder weerbaarheid en slagvaardigheid schiet zelfs de beste strategie tekort”

Een van de belangrijkste beslissingen die bestuurders vandaag kunnen nemen is het gesprek aangaan over wendbaarheid. Rijkswaterstaat ziet dat snelheid van handelen binnen de overheid onder druk staat. Procedures, regels en aanbestedingstrajecten zijn vaak complex en tijdrovend.
Terwijl digitale risico’s zich snel ontwikkelen, duurt besluitvorming soms te lang. Vandaag ontstaat een probleem, maar een oplossing organiseren kan maanden duren.
Zoals het treffend werd verwoord:”Vandaag is het aan de hand en er moet morgen iets gebeuren.” Wendbaarheid is nu een veiligheidsvraagstuk.”

Wat kunnen andere organisaties morgen doen?

De lessen van Rijkswaterstaat zijn relevant voor elke sector. Stel je als security-expert en bestuur daarom vragen zoals:

- weten wij wat onze kroonjuwelen zijn?
- begrijpen wij onze belangrijkste afhankelijkheden?
- is life-cycle management structureel op orde?
- hebben wij voldoende eigen kennis om regie te voeren?
- worden signalen van specialisten serieus genomen?
- hebben wij scenario’s en exitplannen als iets uitvalt?
- kunnen wij snel genoeg besluiten en handelen?
- begrijpt het bestuur de taal van IT voldoende?

De nieuwe bestuurlijke werkelijkheid

Niet techniek, niet een extra rapportage en ook niet nóg een control realiseren, maar bestuurlijk bewustzijn wordt gevraagd. Jarenlang gingen organisaties uit van vanzelfsprekende beschikbaarheid van technologie, stabiele markten en beheersbare afhankelijkheden. Die werkelijkheid bestaat niet meer.
De afhankelijkheid van niet-Europese leveranciers blijkt groter dan gedacht. AI, geopolitiek en digitale soevereiniteit zijn geen losse thema’s meer, maar grijpen op elkaar in. Bestuurders hoeven geen technoloog te worden, maar moeten wél begrijpen waar afhankelijkheden ontstaan, welke risico’s daaruit voortkomen en welke keuzes vandaag nodig zijn om morgen wendbaar te blijven.

De vraag is niet óf digitalisering strategisch is. De vraag is of organisaties snel genoeg meebewegen met een werkelijkheid die al veranderd is. Wie de afhankelijkheden niet begrijpt, kan de toekomst ook niet besturen.

Auteur: Zoëlle Yusufi is redacteur van InformatieBeveiliging Magazine. Dit diepte-interview met Wenny Bruysters-Verbossen, CIO bij de gemeente Oss, snijdt door de rapportages en regeldruk heen, op zoek naar de menselijke maat in de IDRS-verslagleggingsstandaard alsook hoe digitalisering écht waarde levert voor de inwoner. Zoëlle Yusufi is bereikbaar via: zoelle.yusufi@rvo.nl

Besturen in de mist

hoe IDRS richting geeft in een complexe digitale werkelijkheid

Voor veel publieke organisaties ligt de grootste digitale uitdaging niet alleen in techniek, maar in sturing. Hoe maak je complexe digitale vraagstukken bestuurlijk begrijpelijk? Hoe voorkom je dat rapportages zich opstapelen zonder dat ze leiden tot betere keuzes? En hoe zorg je dat digitalisering uiteindelijk zichtbaar waarde oplevert voor inwoners?

Wenny Bruysters is CIO bij de gemeente Oss en werkt dagelijks op het snijvlak van technologie, dienstverlening en bestuur. Vanuit een gemeente met bijna 100.000 inwoners ziet zij hoe de behoefte aan grip groeit, terwijl capaciteit, tijd en overzicht onder druk staan.
In haar visie kan de NOREA-standaard: International Digital Reporting Standards (IDRS), helpen om versnipperde verantwoordingsinformatie samen te vatten tot één bestuurlijk relevant verslaggevingsstandaard, geen extra rapportage, maar een instrument voor dialoog en richting.

”De waarde van een rapportage zit niet in het papier, maar in het gesprek dat daarna ontstaat.”

In dit interview vertelt Wenny Bruysters waarom digitale weerbaarheid begint bij samenhang en hoe inwoners uiteindelijk het verschil merken wanneer een gemeente haar digitale basis echt op orde brengt.
Digitale weerbaarheid krijgt vaak aandacht vanuit techniek. Denk aan cyberdreigingen, continuïteit, cloudrisico’s en compliance. Dat is logisch. Maar wie naar de gemeentelijke praktijk kijkt, ziet een andere werkelijkheid.

De grootste uitdaging is lang niet altijd technisch. Die zit vaak in de vraag hoe bestuurders, professionals en organisatieonderdelen samen grip krijgen op een steeds complexere, digitale opgave in een steeds complexere wereld.

Juist daarin ligt de waarde van het gesprek met een gemeente met bijna 100.000 inwoners. Waar andere organisaties vooral laten zien hoe je infrastructuur beschermt of afhankelijkheden verkleint, laat de gemeente zien wat vaak beslissend is voor succes: "de menskant van digitale sturing."

IDRS als middel, niet als doel

Gemeenten hebben te maken met een groeiend landschap van wet- en regelgeving, toezicht, audits en verantwoordingsverplichtingen. Elk kader heeft een legitiem doel, maar in de praktijk leidt de stapeling vaak tot versnippering. Informatie staat op meerdere plekken, kent verschillende definities en wordt in verschillende ritmes aangeleverd.

Juist daar ziet Gemeente Oss de waarde van IDRS. De standaard biedt de mogelijkheid om bestaande informatie samen te brengen in één samenhangend beeld. Daarmee verschuift de aandacht van losse documenten naar bestuurlijke betekenis. Dat onderscheid is cruciaal. Een standaard werkt alleen wanneer zij vereenvoudigt. Niet wanneer zij nog een extra laag aan rapportageverplichting toevoegt. IDRS is geen losse toevoeging, maar het middel om samenhang te creëren. Zonder die integrerende werking missen we het doel.

Echte regie vraagt daarom om meer dan een instrument alleen. Het vraagt bestuurlijke afspraken, governance, prioritering en investeringen, die verder gaan dan rapporteren. Van losse signalen naar bestuurlijke betekenis.
Het gemeentebestuur heeft zelden een tekort aan informatie. Wat vaak ontbreekt, is overzicht.
Rapportages komen uit verschillende domeinen: cybersecurity, privacy, leveranciersmanagement, continuïteit, audits en compliance. Elk document kan waardevol zijn, maar samen vormen zij nog niet automatisch een stuurbeeld.
Volgens Wenny Bruysters zit daar de kracht van IDRS: "niet méér informatie, maar samenhang en duiding". Een kleurcode zonder duiding zegt weinig. Een status oranje kan een verbetering zijn ten opzichte van vorig jaar, maar ook een verslechtering. Zonder trend, toelichting en samenhang ontstaat schijnzekerheid, "oranje is dus niet altijd oranje".
Dat eenvoudig inzicht raakt een fundamenteel probleem in veel governanceprocessen: informatie is pas waardevol wanneer zij helpt om betere keuzes te maken. Daarnaast is de opgave van de gemeente niet primair technisch, maar menselijk en bestuurlijk.
Samenhang ontstaat niet alleen doordat informatie wordt gebundeld. Samenhang ontstaat wanneer mensen elkaar begrijpen. Technische experts moeten risico's en keuzes kunnen vertalen naar bestuurlijke taal. Juristen moeten ruimte zien voor uitvoerbaarheid. Bestuurders moeten voldoende digitaal vakmanschap ontwikkelen om de juiste vragen te stellen en keuzes te wegen.
"Digitale verantwoordelijkheid vraagt om digitaal vakmanschap."
Dat betekent niet dat iedere bestuurder technicus moet worden. Wel dat digitalisering niet langer kan worden behandeld als specialistisch neventhema. Het raakt direct aan publieke waarden, dienstverlening, veiligheid, continuïteit en vertrouwen.

Niet nóg een dashboard

In complexe organisaties is de reflex begrijpelijk: meer meten, meer controleren, meer rapporteren. Maar extra dashboards en aanvullende rapportages lossen versnippering niet vanzelf op. Eerder nog zij versterken dat effect. Wanneer nieuwe verantwoordingsvormen bovenop bestaande structuren worden gestapeld, groeit de administratieve last. Medewerkers besteden dan meer tijd aan verantwoorden dan aan verbeteren. De betere vraag is daarom niet: "Wat voegen we toe?" De betere vraag is: *"Wat kan vervallen; wat kan worden samengebracht; welke informatie helpt bestuurders verder om samenhangende keuzes te maken en te sturen op risico's en waarde? Dat bestuurlijk gesprek is bepalend voor scherpere prioritering en effectievere inzet van middelen, en daarmee uiteindelijk voor betere dienstverlening voor de inwoner?"*

IDRS heeft juist ook meerwaarde wanneer het helpt die omslag mogelijk te maken.

De inwoner merkt het verschil wanneer de basis op orde is. Een inwoner hoeft de term IDRS niet te kennen om het effect ervan te merken. Wanneer interne sturing niet op orde is, wordt dat zichtbaar in de praktijk: door trage afhandeling, onduidelijke statusupdates, meerdere loketten voor één vraag of onnodige herhaling van gegevens. Inwoners

verwachten steeds meer transparantie, voorspelbaarheid en gebruiksgemak.
Gemeenten zijn geen webshops, maar de verwachtingen van inwoners worden wel gevormd door hun dagelijkse digitale ervaringen met de gemeente. Daarom is de kernvraag niet alleen hoe een gemeente verantwoordt, maar ook hoe interne sturing zich verder kan vertalen naar betere dienstverlening en opbouwend vertrouwen.

De ketencomplexiteit

De uitdaging wordt groter in domeinen waar meerdere organisaties samenwerken, zoals: jeugdzorg, welzijn, onderwijs, zorg en veiligheid. Daar komen gegevensdeling, privacy, verantwoordelijkheden en verschillende systemen samen. Vanuit inwonersperspectief is de wens logisch: één ingang, één antwoord, één begrijpelijke route. Achter de schermen is de werkelijkheid veel complexer.
Juist in zulke ketens groeit de behoefte aan bestuurlijke grip. Maar grip verkrijgen vraagt mensen die bedrijfsvoering, technologie, wetgeving en maatschappelijke context tegelijk begrijpen. De invulling van dat functieprofiel is schaars. Daarmee raakt Gemeente Oss een breder vraagstuk: de behoefte aan digitale regie groeit sneller dan het aantal mensen dat deze regie kan uitwerken.

Common ground

Als praktisch perspectief noemt Wenny Bruysters: "Common ground." Niet als los ICT-project, maar als manier van denken waarin dienstverlening en informatievoorziening worden ingericht vanuit het perspectief van inwoners. Dat sluit aan op de bredere Nederlandse Digitaliseringsstrategie (NDS): meer gezamenlijk optrekken, kennis bundelen en hergebruik stimuleren.
Tegelijkertijd vraagt de praktijk om realisme. Gemeenten werken met legacy, vervangingstermijnen, schaarse capaciteit en financiële druk. Grote veranderingen worden zelden in één keer gerealiseerd. Digitale professionalisering is daarom geen sprint, maar een meerjarige beweging. "Je kunt niet alles in één keer veranderen. Je moet wel in beweging blijven."

Van structuur naar dialoog

Klassieke bestuursstructuren werken met vaste cycli, formele documenten en besluitvorming achteraf. Digitalisering ontwikkelt zich sneller, iteratiever en vaak domein overstijgend. Daarom pleit Gemeente Oss voor meer dialoog aan de voorkant. Niet alleen rapporteren ná afloop, maar eerder samen betekenis geven aan signalen, risico's en keuzes. Een agile manier van werken en besturen. Dat vraagt een andere bestuursstijl. Minder zenden, meer gesprek. Minder papieren zekerheid, meer gezamenlijke duiding. IDRS kan daarbij helpen, juist omdat het verschillende perspectieven samenbrengt in één bestuurlijk gesprek. ''Niet het document zelf is doorslaggevend, maar het gesprek dat het mogelijk maakt.''

Digitalisering, een maatschappelijke opgave

Volgens Wenny Bruysters is digitalisering allang geen exclusief thema van de ICT-afdeling meer. Het is een maatschappelijke opgave. Die formulering verandert ook de bestuurlijke verantwoordelijkheid. Dan gaat het niet alleen over systemen beheren, maar over inclusie, weerbaarheid, autonomie, legitimiteit en publieke dienstverlening. Bestuurders moeten daarom de samenhang zien tussen wetgeving, cloud, ketens, innovatie, leveranciersafhankelijkheid en publieke waarden. Wie die samenhang mist, stuurt op deelproblemen.
Uit het gesprek komen drie concrete best practices naar voren:

1. Verminder versnippering; door gebruik van IDRS kan je de bestaande verantwoordingsinformatie samenbrengen in plaats van steeds iets nieuws toe te voegen.
2. Investeer in digitaal vakmanschap. Niet alleen bij specialisten, maar ook in colleges, directies en raden.
3. Organiseer het gesprek eerder. Gebruik rapportages niet alleen achteraf, maar als startpunt voor dialoog en bijsturing. Koppel sturing aan de waarde, voor de inwoners, en laat interne verbeteringen zichtbaar bijdragen aan dienstverlening en vertrouwen.

De menselijke maat in sturing

Het debat over digitale weerbaarheid gaat vaak over technologie. Terecht, maar technologie alléén bestuurt niets. Denk in beweging, dit is geen eindig traject, maar een continue, meerjarige koers. De les uit gemeente Oss heeft daarom meer betekenis dan het zijn van één standaard of voor één enkele organisatie. Echt grip verkrijgen ontstaat wanneer informatie begrijpelijk wordt, verantwoordelijkheden helder zijn en mensen het goede gesprek kunnen voeren. IDRS kan daarin een belangrijke rol spelen. Niet als extra verplichting, maar als brug tussen inhoud en bestuur.
Daar begint volwassen digitale sturing. Niet nóg een rapportage, maar een beter gesprek. Niet méér controle, maar meer vertrouwen. Niet alleen systemen verbeteren, maar samen beter besturen. Denk in beweging, digitale professionalisering vraagt om een meerjarige koers, geen eenmalig project.

COLUMN NICOLE

Lippendienst

Toen ik vol optimisme aan dit columnistenbestaan begon in 2024, wist ik dat er een moment zou komen waarop ik moest sprokkelen voor onderwerpen. Telkens als de deadline nadert, ga ik ijverig op zoek naar een recent incident als haakje. En telkens komen dezelfde onderwerpen voorbij: ransomware, bestuurlijke betrokkenheid, datalekken. Het voelt als een reünie van vergane glorie.

Ik heb weleens met vrienden uit de gemeenschap gesproken over cyber fatigue — een soort verzadiging van cybersecurity: de discussies, de vragen, de obstakels. Komt die vermoeidheid door het gebrek aan vooruitgang? Want hoewel er zoveel verandert, heb ik tegelijkertijd het gevoel dat we al tien jaar stilstaan. Dat ik bij elke vermelding van *weerbaarheid, gedeelde verantwoordelijkheid en dreigingslandschap* al achterover leun en begin te gapen.

Ik dacht aan die sleur te kunnen ontsnappen toen ik mijn huidige functie aannam. Nieuwe technologie, nieuwe energie. Maar de *cyber fatigue* blijft mij achtervolgen. Want als ik over iets nieuws begin, geeft mijn publiek aan nog steeds te worstelen met alle oude problemen. En inmiddels is AI niet meer nieuw. Sterker nog: ik bespeur een AI-moeheid. En quantum dreigt aan dezelfde besmettelijke ziekte te bezwijken, nog voor het echt begonnen is.
Waar komt die sleur vandaan? Ik geloof nu dat het de herhaling is die mij doet afhaken — maar niet zomaar herhaling. Het is de herhaling van woorden zonder daden. In het Engels noemen ze dat *lip service*, in het Nederlands *lippendienst*. Onoprechte steun. Lege woorden. Zeggen dat je ergens achter staat, zonder ook maar iets te doen om het te ondersteunen. Een incident voltrekt zich, de commotie laait op, er worden vragen gesteld en beloften gedaan — en een week later is het business as usual.

Wat mij het meest treft, is het contrast. De specialist — de analist, de architect, de beheerder — weet precies wat er moet gebeuren. Die werkt 's avonds door, schrijft het rapport, stuurt de aanbeveling. En dan belandt dat stuk op het bureau van iemand die besluit dat er eerst een businesscase nodig is, dat het past op de agenda van het volgende kwartaal, dat er eerst draagvlak gecreëerd moet worden. Intussen tikt de klok.

Als het gaat om cybersecurity kunnen we een voetbalstadion vullen met mensen die toewijding veinzen. En dan heb ik het niet over de specialisten, maar over de mensen die uiteindelijk beslissen over het geld en het beleid. Zij gaan de straat op als het moet. Zij sturen de brandende e-mail. Zij tekenen de verklaring. En daarna zakken ze weer terug in hun stoel, tot het volgende incident.

Ik geloof dat de lippendienst mijn melatonine is. En zolang woorden goedkoper blijven dan daden, blijf ik gapen.

Dr. Nicole van der Meulen is expert op het gebied van cybersecurity en emerging technologies en werkzaam bij SURF als Cybersecurity Innovation Lead, ns.vandermeulen@gmail.com

Auteur: Zoëlle Yusufi is redacteur van InformatieBeveiliging Magazine. Zij verkent de strategische verschuivingen binnen het ICT-landschap in gesprek met Erik Logtenberg (CIO bij het CBS) over de vraag hoe het Centraal Bureau voor de Statistiek zijn digitale soevereiniteit bewaart in een tijd waarin data en AI de nieuwe geopolitieke krachtenvelden bepalen. Zoëlle Yusufi is bereikbaar via: zoelle.yusufi@rvo.nl

Geen project, maar principe:

hoe het CBS... soevereiniteit werkbaar maakt

Als hoofddirecteur IT en CIO bij het Centraal Bureau voor de Statistiek (CBS) staat Erik Logtenberg aan de lat voor de digitale transformatie van een van Nederlands meest vitale data-instituten. In een tijd waarin data de nieuwe geopolitieke valuta vormt, navigeert hij door het complexe speelveld van technologische soevereiniteit en de opkomst van AI. Voor het Platform voor informatiebeveiliging gaat hij dieper in op wat digitale soevereiniteit werkelijk betekent voor het CBS en de BV Nederland.

"Ik ben een IT'er in hart en nieren"

Die uitspraak zegt meer dan alleen iets over persoonlijke passie. Goed bestuur in het digitale tijdperk vraagt niet alleen algemene managementvaardigheden, maar ook inhoudelijk begrip van technologie. Niet iedere bestuurder hoeft technicus te zijn. Maar organisaties hebben wél leiders nodig die technologische keuzes kunnen doorgronden, alternatieven herkennen en de gevolgen van afhankelijkheden begrijpen.

Van data naar daadkracht

Digitale soevereiniteit klinkt nog als beleidstaal. Iets voor strategiedocumenten, conferenties en overheidsagenda's. Maar in de praktijk is het geen doel op zich, je probeert een bijdrage te leveren aan het grotere geheel.
Nederland is digitaal afhankelijker dan veel organisaties beseffen. En zolang die afhankelijkheid niet concreet wordt aangepakt, blijft weerbaarheid kwetsbaar.

**Digitale soevereiniteit is geen project.
Het is een ontwerpkeuze.**

Jarenlang werden digitale keuzes vooral beoordeeld op kosten, functionaliteit en gebruiksgemak. Die wereld

verandert snel. Alle organisaties moeten digitale afhankelijkheid veel breder bekijken, dit in samenhang met geopolitiek, economische druk en strategische autonomie.

Technologie, data en infrastructuur zijn onderdeel geworden van internationale machtsverhoudingen. Toegang tot diensten, data of platforms is niet langer vanzelfsprekend neutraal. Als een organisatie volledig afhankelijk is van externe partijen voor kritieke digitale processen, ontstaat ook bestuurlijke kwetsbaarheid, de situatie met het Internationaal Gerechtshof (**ICJ**) is een goed voorbeeld van wat er kan gebeuren.

Digitale soevereiniteit is daarom geen doel op zich. Het is een middel om als land en als organisatie sterker te staan wanneer belangen botsen.

Vertrouwen begint bij beschermde data

Voor een organisatie als het CBS is data geen bijzaak, maar een bestaansrecht. Een belangrijk onderscheid daarbij is het verschil tussen onherleidbare uitkomsten en herleidbare brondata. Statistische eindproducten zijn bedoeld voor het feitelijk informeren van de samenleving en om beleid te kunnen maken. Maar microdata of herleidbare datasets vragen maximale bescherming.
Daarom werd bij het CBS al vroeg kritisch gekeken naar waar data thuishoort en onder welke voorwaarden die worden verwerkt. Dat heeft erg geholpen met waar we nu staan.

De kernvraag is niet alleen: waar staat de data? De echte vraag is: wie kan erbij, onder welke wetgeving en wat gebeurt er als omstandigheden veranderen?

Dat vraagt om meer dan technische beveiliging. Het vraagt om bewuste architectuurkeuzes. IT is geen algemene portefeuille; digitale keuzes, echter, raken continuïteit, autonomie, veiligheid, innovatie en publieke waarden. Daarom verdienen vaklieden ook plek aan de top. Niet elk bestuurslid hoeft IT-specialist te zijn, maar onderschat IT niet als een algemene portefeuille. AI, cloud en geopolitiek zijn geen losse dossiers meer, ze kunnen elkaar versterken.

De stille verschuiving

Vroeger kochten organisaties software als product. Je installeerde het lokaal en gebruikte het in je eigen omgeving. Vandaag zijn veel toepassingen geëvolueerd van standaardsoftware tot onlinediensten, verbonden met Cloud-platforms, licentiemodellen en continue synchronisatie. Dat lijkt een technisch detail, maar heeft grote gevolgen.

Wie afhankelijk wordt van online activatie, externe identiteiten, cloudopslag en geïntegreerde AI-diensten, wordt ook afhankelijk van partijen buiten de eigen invloedssfeer. Zelfs zonder nieuw contract kan de afhankelijkheid dus groeien.

Exit-strategie is geen papieren exercitie

Veel organisaties spreken over risicoanalyses. Minder organisaties werken aan realistische exit strategieën. Dat is een verschil, een exit strategie betekent niet dat morgen alles moet veranderen.

In de praktijk is het vooral weten waar je staat: welke afhankelijkheden zijn kritiek? Welke alternatieven heb je, hoe migreer je daarnaartoe en welke kennis en tijd is daarvoor nodig? Het gaat erom dat je die puzzelstukjes en kennis paraat hebt. Zonder dat inzicht blijft een exit-plan theorie. En op het moment dat een crisis ontstaat, ben je te laat.

Open source vraagt een andere mindset

In Nederland werken we als overheid nog te weinig met open source. Open source is geen ideologie, maar een bestuurlijke optie: een strategische en soevereine keuze. Het biedt een fundamenteel ander uitgangspunt, als organisatie ben je niet meer volledig gebonden aan één leverancier. Software kan worden beheerd, aangepast, overgenomen of door een andere partij worden ondersteund als dat jouw keuze is. Dat geeft keuzevrijheid.

Niet elk open source alternatief is direct gelijkwaardig aan gevestigde marktleiders. Maar dat hoeft ook niet altijd. Soms is "goed genoeg" strategisch waardevoller dan "perfect", want volledig afhankelijk. Dat vraagt een andere mindset, minder gestuurd door marketing en meer door lange termijnbelang.

"Neem genoegen met een klein beetje minder. Dan worden alternatieven ineens veel haalbaarder."

Modernisering zonder hyperscalerreflex

Veel organisaties worstelen met legacy, technical debt en verouderde infrastructuur. De verleiding is dan groot om volledige modernisering onder te brengen bij een hyperscaler.

Dat lijkt snel en logisch. Maar Big Tech is niet de enige route. Snelheid is verleidelijk, maar niet altijd de route naar modernisering. Onze weg naar binnen, ons eigen datacenter doorontwikkelen, bewijst dat dit leidt tot een sterkere IT-organisatie. Door open source omarming en slimme herinvestering van licentiegelden in eigen vakmensen, creëren we een cultuur van eigenaarschap.
Teams werken nauw samen en begrijpen hun omgeving beter, doordat de techniek weer écht van henzelf is. Het resultaat is minder vendor lock-in en een hecht team van interne experts die niet meer afhankelijk zijn van externe partijen.

Verslim je Life-cycle Management

Digitale autonomie bereik je niet met een eenmalige 'big bang', maar door slimme keuzes in je bestaande IT-cyclus. Door soevereiniteit te integreren in het bestaande onderhouds- en vervangingsproces, sla je twee vliegen in één klap. Je hebt geen apart project of budget nodig, wat de weerstand in de organisatie drastisch verlaagt. Het stelt teams in staat om stapsgewijs nieuwe kennis op te bouwen, precies op de momenten dat er toch al verandering plaatsvindt.

De transitie naar een soevereine architectuur vraagt echter meer dan techniek alleen. Het succes valt of staat met vijf pijlers. Het begint met een helder verhaal aan de organisatie, gesteund door zichtbaar leiderschap. Geef teams eigenaarschap door ze op te leiden en te begeleiden bij nieuwe keuzes. Bewijs de meerwaarde door kleinschalig te beginnen, te leren en resultaten te tonen voordat je opschaalt. Zo wordt soevereiniteit een structureel onderdeel van je besluitvorming.

AI is kansrijk, maar niet neutraal

Als we kijken naar de inzet van AI, dan is de nuance belangrijk. Niet elke AI-toepassing is hetzelfde. Binnen het CBS blijken vooral traditionele toepassingen veel waarde te leveren, zoals machine learning, patroonherkenning, beeldanalyse en voorspellende modellen.

Bijvoorbeeld het automatisch analyseren van satellietbeelden of het versnellen van dataverwerking. Dat betekent dat het misschien niet perfect is, maar ook daarin vinden we veiligheid, kwaliteit en soevereiniteit belangrijk.
Daartegenover staan generatieve AI-toepassingen, die kunnen weliswaar meer, maar met andere risico's, zoals beperkte uitlegbaarheid, datagebruik buiten de organisatie en onduidelijke herleidbaarheid van uitkomsten.
Voor een organisatie die statistiek als kernactiviteit heeft, is dat cruciaal. Cijfers moeten uitlegbaar, reproduceerbaar en controleerbaar blijven. Daarom is de boodschap helder: gebruik AI waar het waarde toevoegt, maar blijf scherp op governance, herleidbaarheid en data-autonomie.

Een contract is geen controlemaatregel

Het is een misvatting om te denken dat contractuele afspraken met techreuzen voldoende bescherming bieden. Een contract kan belangrijk zijn, maar vervangt geen technische realiteit, geen juridische context en geen architectuurkeuzes. Als data technisch toegankelijk is, processen volledig extern draaien of alternatieven ontbreken, biedt papier beperkte bescherming. Bestuurders moeten dus verder kijken dan clausules alleen. Wie dat verband niet ziet, stuurt straks op symptomen in plaats van oorzaken.

Soevereiniteit is onderhandelingskracht

Digitale soevereiniteit gaat niet over alles zelf doen. Het gaat over voldoende grip krijgen op de belangrijkste belangen, zodat organisaties keuzes houden wanneer het erop aankomt.

Zodra organisaties meer controle terugwinnen over hun eigen data, ontstaat ruimte. Ruimte om te onderhandelen. Ruimte om publieke waarden te beschermen. Ruimte om technologie te gebruiken zonder erdoor gevangen te raken.

De echte opgave is daarom niet alleen technisch, maar ook bestuurlijk is het belangrijk om afhankelijkheden tijdig te herkennen, alternatieven te ontwikkelen en moed te tonen om koers te wijzigen; het hoeft niet perfect te zijn, start klein. We staan op een digitaal kruispunt. Kiezen we voor gemak en afhankelijkheid of voor het ongemak van eigen regie? Het vrijblijvende is er nu wel vanaf, de regie is nu aan ons.

Auteur: Ronald Eygendaal schrijft sinds 1999 over informatiebeveiliging, beveiliging van industriële automatisering en elektronische & technisch beveiliging, voor de toonaangevende vakbladen in Nederland en België. Ronald is te bereiken via: ronald@eygendaal-assist.nl

Veilig in het verkeer met Open Source

Er is veel commotie over de grote restyling van Google Maps, met nieuwe AI-functies zoals Ask Maps en Immersive Navigation (3D-beelden, gedetailleerde landmarks en conversatie met de app). Experts waarschuwen dat deze extra visuele prikkels en interacties gevaarlijke afleiding veroorzaken achter het stuur. Ze vrezen cognitieve overbelasting door te veel informatie en scherm-interactie tijdens het rijden.

Verkeersorganisaties zoals Veilig Verkeer Nederland en SWOV uiten stevige zorgen: multitasken in het verkeer is simpelweg onveilig. *Juist daarom kiest een groeiend aantal mensen voor CoMaps als veiliger alternatief.*

CoMaps is een open source navigatie-app die gebruikmaakt van OpenStreetMap. De app wordt ontwikkeld door een grote, onafhankelijke community en heeft geen winstoogmerk. CoMaps is volledig advertentievrij, respecteert je privacy en volgt je niet. De community achter CoMaps ontstond in 2025 uit onvrede over gesloten serveronderdelen en governance-problemen binnen Organic Maps, een andere open source navigatie-app. Als open source project is CoMaps gratis, transparant over financiering en bestuur; en volledig inzichtelijk voor iedereen.

De app verzamelt geen persoonlijke gegevens, doet niet aan tracking en beschermt je privacy maximaal.

Na het downloaden van kaarten werkt CoMaps volledig offline — ideaal in afgelegen gebieden of wanneer je geen databundel hebt. De app biedt gesproken navigatie in het Nederlands voor auto, fiets en wandelen. Via uitgebreide instellingen kun je onder andere: tolwegen, snelwegen, onverharde wegen, veerboten en meer andere zaken vermijden. Technisch gezien is CoMaps volledig open source. De complete codebase — inclusief de routing engine, kaartweergave en zoekfunctionaliteit — staat openbaar op Codeberg en is vrij te auditen of aan bij te dragen.

CoMaps heeft een minimalistisch gebruikersinterface en is daardoor eenvoudig in bediening. Risico's op cognitieve overbelasting en AI overprikkeling zijn daardoor afwezig.

De app gebruikt geen externe servers voor kernfuncties. Routing, zoeken en POI gegevens worden volledig lokaal verwerkt op je toestel, zodra je de .mwm kaarten hebt gedownload (gebaseerd op OpenStreetMap PBF). Privacy is een centraal uitgangspunt. CoMaps verzamelt geen identificerende gegevens, geen telemetrie, geen achtergrond locatie en bevat geen analytics bibliotheken. De app vraagt alleen de strikt noodzakelijke permissies: locatie (voor GPS navigatie) en opslag (voor offline kaarten). Na installatie is geen internetverbinding meer nodig. Bookmarks en tracks worden lokaal opgeslagen. Automatische lokale back ups voorkomen dataverlies, zonder afhankelijk te zijn van clouddiensten.

Al meer dan 6 maanden vertrouw ik volledig op Comaps voor mijn ritjes in het ruraal van Rotterdam. De stem is helder en natuurlijk, en de interface blijft heerlijk overzichtelijk, zelfs in de drukke spits. Na elke rit ben ik nog steeds onder de indruk: accuraat, gebruiksvriendelijk en ervaar rust tijdens het rijden.

Rij veilig, groeten Ronald

Auteurs: Stephan Corporaal is lector Human Capital op Hogeschool Saxion en het Centrum voor Veiligheid & Digitalisering. Mark Ruijsendaal is programmadirecteur bij Security Delta. Mira van Benthem is innovation liaison bij Security Delta. Sjoerd Peters is onderzoeker Human Capital bij Hogeschool Saxion en het Centrum voor Veiligheid & Digitalisering. Mark Dorenbosch is directeur bij het Centrum van Veiligheid & Digitalisering. Derk-Jan Nijman is associate lector LLO op Hogeschool Saxion. Auteurs zijn bereikbaar via s.corporal@saxion.nl

Cybersecurity competenties in Europa:

evidence-based inzichten voor het doorbreken van de kloof tussen onderwijs en arbeidsmarkt

Europa bevindt zich in een fase waarin digitale afhankelijkheid snel toeneemt, terwijl cyberdreigingen complexer en onvoorspelbaarder worden. Organisaties worden hierdoor geconfronteerd met steeds strengere eisen aan hun digitale weerbaarheid, en dat vereist investeringen in cybersecurity competenties. Het Europese project 'CADMUS', dat zich richt op het in kaart brengen van de Europese cybersecurityvaardigheden, laat zien dat het huidige aanbod van opleidingen en trainingen onvoldoende aansluit op de behoeften van de arbeidsmarkt. Zowel in Nederland als in andere Europese landen is er een kloof tussen vraag en aanbod van cybersecuritycompetenties. Het onderzoek toont aan dat organisaties veel behoefte hebben aan risicomanagement, security consulting, informatiebeveiligingsmanagement, systeembeheer en analytische vaardigheden, terwijl het onderwijs vaak nog te weinig inspeelt op deze vraag. Het onderzoek specificeert deze kloof. Op basis daarvan biedt het concrete handvatten om curricula en professionaliseringsroutes beter af te stemmen op de realiteit van de hedendaagse digitale dreigingen.

De digitale transformatie en de snelle opkomst van AI heeft de manier waarop organisaties functioneren fundamenteel veranderd. Een datalek, ransomware-aanval of verstoring van dienstverlening kan niet alleen financiële schade veroorzaken, maar ook leiden tot verlies van publieke vertrouwen en juridische aansprakelijkheid. Tegelijkertijd is duidelijk geworden dat de vraag naar gekwalificeerde cybersecurityprofessionals veel sneller groeit dan het aanbod. Nieuwe wetgeving zoals: NIS2, DORA en de Cyber Resilience Act versterkt bovendien de noodzaak tot aantoonbare digitale weerbaarheid en dwingt organisaties om cybersecurity structureel in te bedden in hun governance- en risicomanagementprocessen. Tegelijkertijd wordt de dreigingsomgeving complexer doordat kwaadwillenden intensief gebruikmaken van automatisering, AI, cloudinfrastructuren, open-sourcecomponenten en supply-chain-aanvallen. Hierdoor verandert niet alleen welke technische competenties nodig zijn, maar ook welke strategische en communicatieve competenties onmisbaar zijn voor moderne cybersecurityprofessionals. Tot nu toe ontbreekt echter nog inzicht in waar de gap tussen vraag van aanbod van cybersecurity competenties momenteel zit.

Grootschalig onderzoek

Tegen deze achtergrond brengt het CADMUS-project de huidige Europese situatie - rondom de vraag van cybersecurity competenties vanuit het mkb en overheidsorganisatie plus het aanbod van deze competenties vanuit opleidingen en trainingen - systematisch in kaart. We benutten daarvoor een unieke gecombineerde methodiek: een trendanalyse, focusgroepen en een systematische analyse van meer dan 400 vacatureteksten en 266 opleidingen en trainingen.

Uitgebreide trendverkenning

Via een trendverkenning zijn twintig invloedrijke Europese en internationale trendrapporten (zie referentielijst) geanalyseerd op het belang van cybersecurity competenties binnen drie clusters: technologische ontwikkelingen, ontwikkelingen in wetgeving en veiligheids- en risicodynamiek.

Focusgroepen

De inzichten uit de trendverkenning zijn gevalideerd en verdiept in zes focusgroepen met 30 internationale experts uit zowel de praktijk als het onderwijs. Publieke organisaties, mkb bedrijven, cybersecurityprofessi-

onals, docenten in het hoger en middelbaar onderwijs en branchevertegenwoordigers reflecteerden op de trendanalyse in deze focusgroepen.

Vacature- en opleidingsanalyse
480 Nederlandse, 41 Cypriotische en 82 Kroatische vacatureteksten uit overheidsinstellingen en mkb – zijn handmatig geanalyseerd en gelabeld volgens het European e-Competence Framework, die is aangepast naar het cybersecurity werkveld. Daarbij hebben we een uitsplitsing gedaan naar niveau (Level e-1 tot Level e-5). Hierdoor ontstaat een fijnmazig beeld van de daadwerkelijke vraag naar competenties in het werkveld. Aanvullend zijn tientallen onderwijsprogramma's, cursussen en trainingen handmatig gelabeld (in totaal 266 initiatieven), eveneens volgens het aangepaste European e-Competence Framework. Dit maakt het mogelijk om de vacatures rechtstreeks te vergelijken met het bestaande onderwijsaanbod en zo vast te stellen waar structurele gaten ontstaan tussen wat organisaties vragen en opleidingen leveren.
Dankzij deze combinatie van databronnen – arbeidsmarktdata, onderwijsscans, trendanalyse en praktijkgerichte expertvalidatie – ontstaat een robuust, multidimensionaal beeld van de huidige én toekomstige Europese cybersecurityvaardigheden.

Uitkomsten trendanalyse

In de trendanalyse identificeerden we drie type trends: regelgeving, technologische ontwikkelingen en veiligheids- & risicodynamiek, met elk een aantal belangrijke competenties.

Regelgeving
De Europese regelgeving rondom cybersecurity wordt aanzienlijk strenger, waarbij organisaties verplicht worden om meer zichtbaarheid te hebben in hun volledige digitale keten, inclusief leveranciers en open sourcecomponenten. De NIS2-richtlijn vergroot het aantal organisaties dat als essentieel of belangrijk wordt beschouwd, waardoor sectoren zoals: digitale infrastructuur, cloudproviders en publieke administratie onder zwaarder toezicht komen te staan. De Cyber Resilience Act (CRA) verplicht leveranciers om security-by-design en security-by-default principes toe te passen in al hun digitale producten. De Digital Operational Resilience Act (DORA) legt financiële instellingen verplichtingen op rond ICT-risicomanagement en streng toezicht op derde partijen. De AI Act introduceert aanvullende eisen zoals transparantie, menselijk toezicht en conformiteitsbeoordelingen voor hoog risico AI-systemen. Organisaties moeten hun compliance processen harmoniseren, omdat verschillende Europese wetten overlappen, variëren in scope en verschillende handhavingstijdslijnen kennen. Tegelijkertijd krijgen toezichthouders meer slagkracht, met hogere boetes en striktere auditvereisten. De EU stimuleert daarnaast interoperabiliteit en standaardisatie, waardoor uniforme API-standaarden en datamodellen verplicht worden om gegevensuitwisseling veiliger te maken.

De vijf meest genoemde competentiegebieden die worden genoemd ,bij deze trend, in de trendanalyses:
- Regulatory literacy en multidomein compliancebeheer
- Leveranciers- en ketenrisicomanagement
- Privacy-by-design en veilig datamanagement
- Incidentrespons binnen de wettelijke kaders
- Vertalen van technische risico's naar bestuurders en juridische stakeholders

Technologische ontwikkelingen
Cybercriminelen maken steeds intensiever gebruik van AI, waaronder modellen zoals FraudGPT en autonome LLM agents die kwetsbaarheden kunnen misbruiken zonder menselijke tussenkomst. Phishing, social engineering en deepfake aanvallen worden overtuigender door synthetische content en geautomatiseerde scripts. Aanvallen verplaatsen zich van traditionele endpoints naar cloud platformen, SaaS applicaties en identiteitsbeheer, waar misconfiguraties en token diefstal een centrale rol spelen. Living off the land en living off trusted sites technieken worden populairder, waardoor aanvallers detectie ontwijken door legitieme tools en diensten te misbruiken. De afhankelijkheid van grote niet EU-cloudproviders verhoogt strategische kwetsbaarheden, terwijl ook edge en IoT apparatuur vaker doelwit worden door zwakke configuraties. Open source software blijft risicovol door supply chain-aanvallen waarbij één kwetsbare library grote systeemimpact kan hebben. Defensief worden AI-oplossingen ontwikkeld om anomalieën te detecteren, patches te automatiseren en dreigingen sneller te isoleren. Tegelijk blijft de menselijke factor een dominante kwetsbaarheid door misconfiguraties, zwakke MFA-implementaties.

De vijf meest genoemde competentiegebieden die worden genoemd ,bij deze trend, in de trendanalyses:
- AI gedreven threat intelligence en analyse
- Cloud en identiteitsbeveiliging (zero-trust)
- Ethisch hacken, pentesten en OT/IoT beveiliging
- DevSecOps en veilig software ontwikkelen
- Incidentdetectie, monitoring en mensgerichte security awareness

Veiligheids- en risicodynamiek
Geopolitieke spanningen leiden tot een escalerend cyberdreigingslandschap waarin statelijke actoren steeds vaker kritieke infrastructuur aanvallen. Supply chains worden complexer en internationaler, waardoor risico's minder voorspelbaar en moeilijker te beheersen zijn. Nieuwe technologieën worden snel geadopteerd, maar vaak zonder voldoende beveiliging, waardoor cybercriminelen deze tools gebruiken om aanvallen geavanceerder en schaalbaarder te maken. Ransomwaregroepen passen dubbel en zelfs drievoudige afpersing toe waarbij diefstal, encryptie en reputatieschade gecombineerd worden. Kritieke operationele technologie omgevingen zoals productie-installaties, logistieke systemen en slimme gebouwen worden frequenter

aangevallen, mede door hun toenemende connectiviteit. Organisaties hebben behoefte aan betere samenwerking tussen publieke en private partijen om dreigingsinformatie te delen en sneller te reageren. Internationale standaarden en harmonisatie zijn dringend nodig om consistent cyberbeleid mogelijk te maken tussen verschillende regio's. De combinatie van geopolitiek, technologie en complexe ketens maakt risicobeheer minder lineair en vereist wendbare, strategische security governance.

De vijf meest genoemde competentiegebieden die worden genoemd ,bij deze trend, in de trendanalyses:

- Analyse van tactieken, technieken en procedures van diverse dreigingsactoren
- Crisis- en incidentrespons in multidimensionale aanvalsscenario's
- Samenwerking met CERTs, ISACs en publieke partners
- Business continuity, resilience en herstelplanning
- Risico gestuurd prioriteren en strategische security governance

Uitkomsten focusgroepen

De experts in de focusgroepen benadrukken dat toekomstige digitale en cybersecurity-competenties sterk verschuiven richting strategisch en proactief handelen. Professionals moeten in staat zijn om AI-gedreven verdedigingsstrategieën te ontwikkelen, technologische trends te duiden en deze inzichten te verbinden met organisatiebrede prioriteiten, zoals wet- en regelgeving, financiële risico's en operationele continuïteit. Daarbij hoort ook het vroegtijdig integreren van security in het ontwerp en de ontwikkeling van systemen en applicaties, waarbij secure-by-design het uitgangspunt vormt.

Daarnaast groeit het belang van technische expertise in combinatie met analytisch vermogen. Het gaat om het beschermen van apparaten en infrastructuren, het uitvoeren van dreigingsmodellering, het inrichten van veilige cloudomgevingen en het verwerken van incidenten via robuuste probleem- en systeemanalyse. Ook krijgen data-gerelateerde vaardigheden een prominentere rol: het omgaan met ethische vraagstukken rondom data, het toepassen van AI voor detectie van afwijkend gedrag en het kritisch beoordelen van algoritmische uitkomsten op bias en betrouwbaarheid.

Tot slot wordt de menselijke en organisatorische dimensie steeds belangrijker. Professionals moeten complexe cyberrisico's kunnen vertalen naar begrijpelijke taal voor bestuurders en externe partners, en organisatiebrede bewustwording stimuleren. Daarnaast vraagt de toenemende reguleringsdruk – zoals NIS2 – om sterke competenties in risicomanagement, compliance en governance, inclusief het adresseren van ethische aspecten en afhankelijkheden in de digitale keten. Cross-functioneel samenwerken binnen en tussen organisaties vormt hierin een cruciale vaardigheid.

De experts in de focusgroepen prioriteerden de volgende competentiegebieden:

1. Strategische cybersecurity-en AI-aligned besluitvorming (AI-enabled defence, digitale soevereiniteit, koppeling met juridische/financiële prioriteiten)
2. Secure-by-design denken en ontwerpen (veiligheid vroeg in het ontwerp integreren, veilige componentkeuze)
3. Technologische trendmonitoring en snelle adaptiviteit (nieuwe dreigingen en technologieën kunnen interpreteren en toepassen)
4. Threat modelling en secure systems management (beveiligde API's, cloud-configuratie, fysieke/IoT-systemen beveiligen)
5. Risicoanalyse & NIS2-compliance (prioriteren van risico's, handelen in complexe publieke context)
6. Communicatieve vaardigheid om complexe cyberrisico's te vertalen voor bestuurders en niet-technische stakeholders (board-level communicatie, begrijpelijke duiding en samenwerken over organisatorische en disciplinaire grenzen heen (intern én met externe leveranciers; ketenafhankelijkheden begrijpen).

Behoeften cybersecurity competenties

Uit de vacature-analyse blijkt dat voor wat betreft mkb-organisaties de top vijf van meest gevraagde competenties als volgt is:

D.12. Security Consulting (9,74%)
C.4. Problem Management (6,77%)
C.5. Systems Management (5,78%)
B.5. Documentation Production (5,45%)
B.1. Application/Product Development (4,62%)

De percentages refereren naar het percentage vacatures waarin de competentie werd benoemd. Mkb's richten zich sterk op het creëren en ontwikkelen van producten en applicaties voor interne of externe stakeholders. Daardoor zijn competenties zoals probleemoplossing, systeembeheer en documentatieproductie essentieel voor de dagelijkse werkzaamheden van mkb's. Zodra een applicatie of product ontwikkeld is, worden daarnaast consultatieve vaardigheden belangrijk.

De top vijf competenties voor professionals in de publieke sector is:

D.12. Security Consulting (9,74%)
D.7. Science and Analysis (7,26%),
E.4. Relationship Management (6,44%)
A.7. Technology Trend Monitoring (6,27%)
C.4. Problem Management (4,95%)

Overheidsinstellingen richten zich doorgaans op het ontwikkelen van beleid over uiteenlopende onderwerpen, waardoor analytische vaardigheden en het kunnen volgen van technologische trends essentieel zijn. Bovendien doen overheidsorganisaties, naast interne expertise, regelmatig een beroep op externe consultants. Dit vergroot de behoefte aan security consulting en relatiebeheer binnen deze sector.

Analyse opleidingen

Uit de analyse van de onderwijsmarkt blijkt dat de volgende competenties het meest aan bod komen in opleidingen, cursussen en trainingen:

E.8. Information Security Management (60,24%)
E.3. Risk Management (41,77%),
C.5. Systems Management (41,37%)
D.7. Science and Analysis (39,36%)
B.3. Testing (33,73%).

Opleidingen, zoals bachelor- en masterprogramma's, hebben doorgaans een minimumduur van één jaar. Omdat deze opleidingen voornamelijk afkomstig zijn van universiteiten en hogescholen, is het logisch dat D.7. Science and Analysis (25,70%) tot de top vijf behoort: studenten moeten analytisch kunnen denken en schrijven om goed (academisch) onderzoek te doen. Daarnaast behoren B.1. Application/Product Development (29,72%), C.5. Systems Management (22,89%), E.8. Information Security Management (22,89%) en A.5. Architecture Design (21,29%) tot de belangrijkste competenties in dergelijke programma's.

Kortlopende cursussen en trainingen vertonen een vergelijkbare focus. Het enige verschil zit in C.5. Systems Management (cursussen: 12,05%) versus E.6. Quality Management and Compliance (trainingen: 7,63%). Een belangrijk doel van cursussen en trainingen is het behalen van specifieke certificeringen. Zo sluiten CISM en CISSP nauw aan bij respectievelijk information security management en systems- en problem management.

Gap cybersecurity competenties

De gecombineerde inzichten uit de vacatureanalyse, trendrapporten, literatuurstudie en focusgroepen bieden een uitgebreid overzicht van benodigde en gevraagde cybersecurity competenties. Via een geavanceerde analyse zijn deze uitkomsten gecombineerd tot een gewogen analyse waarin het verschil tussen vraag en aanbod van cybersecurity competenties is geconcretiseerd. Daartoe zijn de uitkomsten van de vacature-analyse en de analyse van de opleidingen gewogen op basis van de uitkomsten van de trendanalyse en de focusgroepen. Een uitgebreide verantwoording daarvan is beschikbaar in het CADMUS onderzoeksrapport op: www.cadmus-project.eu

De tabel op pagina 25 geeft een samenvatting van de belangrijkste verschillen tussen de vraag naar competenties—gebaseerd op de vacatureanalyse, landenrapporten, trendanalyse en focusgroepen—en het aanbod van competenties in onderwijsprogramma's. We specificeren per competentie en ook per competentieniveau:

- **Groen** markeert de belangrijkste prioriteiten voor investeringen in het onderwijsaanbod, waar de vraag naar competenties groter is dan het aanbod.

- **Rood** geeft de gebieden aan waar het aanbod in het onderwijs groter is dan de vraag.

We specificeren gaps tussen aanbod en vraag van cybersecurity dus als volgt: hoe groter het percentage in de tabel, hoe groter het verschil tussen vraag naar competenties en aanbod van onderwijs. Een gap zien we daarmee als kans om te investeren om onderwijsaanbod uit te breiden.

Overzicht van de Gap-analyse per niveau, zie pagina 25.
Gebaseerd op landendata, literatuuronderzoek, trendanalyse, focusgroepen en vacatureanalyse (n=606) en aanbod van opleidingen en trainingen (n=249).
Groen = Kansen voor het onderwijs: de vraag overtreft het aanbod van huidige onderwijsprogramma's.
Geel = Het onderwijs sluit aan bij de vraag.
Oranje/Rood = Overschot: het aanbod van huidige onderwijsprogramma's is groter dan de vraag in vacatures, nu en in de toekomst."

De vijf belangrijkste kansen voor het uitbreiden van het onderwijsaanbod zijn de competenties 'D.3. Onderwijs- en Trainingsaanbod', 'D.9. Personeelsontwikkeling', 'C.4. Probleembeheer', 'D.1. Ontwikkeling van Informatiebeveiligingsstrategie' en 'E.3. Risicobeheer'. Voor deze competenties is de vraag groter dan het aanbod in de huidige onderwijsprogramma's. Dit suggereert dat de belangrijkste prioriteit voor het onderwijs niet per se de meer technische competenties zijn, maar eerder de strategische en bedrijfskundige competenties.
Wanneer we de data echter uitsplitsen per niveau, zien we dat 'C.4. Probleembeheer', 'C.5. Systeembeheer', 'B.3. Testen', 'E.3. Risicobeheer' en 'E.6. Kwaliteitsmanagement en Compliance' ook tot de meest significante tekorten behoren. Deze gegevens benadrukken de noodzaak van een niveau-specifieke benadering bij het bepalen waar te investeren in nieuwe onderwijsaanbiedingen.
De gap-analyse laat zien dat er slechts een kleine kloof is op gebieden zoals 'A.2. Service Level Management', 'A.4. Product/Service Planning', 'A.9. Innovatie', 'D.11. Behoefte-identificatie', 'D.8. Contractmanagement', 'D.4. Inkoop', 'D.6. Digitale Marketing', 'B.1. Applicatie- & Productontwikkeling' en 'D.2. Ontwikkeling van Kwaliteitsstrategie'. Hier lijkt de vraag naar competenties goed aan te sluiten op het aanbod. Deze competenties komen in de trendanalyse en focusgroepen ook niet naar voren als gebieden waarvan grote veranderingen worden verwacht. Daarmee lijken vraag en aanbod in deze domeinen goed in balans."

Competence/ Proficiency level	GAP in % Level e-1	Level e-2	Level e-3	Level e-4	Level e-5	Overall	Rank Overall
A.1. IS and Business Strategy Alignment				-2%	1%	-4%	24
A.2. Service Level Management			0%	0%		-1%	9
A.3. Business Plan Development			-2%	-1%	-1%	-4%	25
A.4. Product/ Service Planning		-4%	-1%	0%		-6%	27
A.5. Architecture Design			-5%	2%	7%	-12%	34
A.6. Application/ Product Design	0%	-5%	-9%			-17%	40
A.7. Technology Trend Monitoring			-6%	2%	1%	-7%	28
A.8. Sustainability Management			-3%	0%		-3%	22
A.9. Innovating				-2%	0%	-3%	19
A.10. User Experience		-4%	-5%	-1%		-10%	32
B.1. Application/ Product Development	5%	1%	-12%			-20%	41
B.2. Component Integration		-6%	-8%	2%		-16%	37
B.3. Testing	16%	18%	9%	17%		-1%	10
B.4. Solution Deployment	-4%	-2%	-9%			-15%	36
B.5. Documentation Production	2%	1%	-7%			-8%	29
B.6. ICT Systems Engineering			-4%	8%		-10%	30
C.1. User Support	-3%	0%	-1%			-4%	23
C.2. Change Support		0%	-2%			-2%	16
C.3. Service Delivery	0%	-1%	-2%			-3%	20
C.4. Problem Management		23%	22%	21%		10%	3
C.5. Systems Management	24%	22%	10%			-1%	12
D.1. Information Security Strategy Development				4%	5%	3%	4
D.2. Quality Strategy Development				-2%	0%	-1%	14
D.3. Education and Training Provision		25%	21%			23%	1
D.4. Purchasing		-1%	0%	0%		-1%	13
D.5. Sales Development		0%	0%	0%		0%	6
D.6. Digital Marketing		0%	0%	0%		-1%	8
D.7. Science and Analysis		10%	-4%	3%	13%	-17%	38
D.8. Contract Management		0%	0%	0%		0%	7
D.9. Personnel Development		16%	13%	16%		11%	2
D.10. Information and Knowledge Management			-1%	1%	3%	-3%	21
D.11. Needs Identification			-9%	-2%	0%	-12%	33
D.12. Security Consulting			0%	2%		-3%	18
E.1. Forecast Development			-4%	-1%		-4%	26
E.2. Project and Portfolio Management		-9%	-6%	-2%	-1%	-17%	39
E.3. Risk Management		19%	13%	16%		0%	5
E.4. Relationship Management			0%	5%		-2%	15
E.5. Process Improvement			-9%	-3%		-12%	35
E.6. Quality Management and Compliance		16%	4%	12%		-2%	17
E.7. Business Change Management			0%	5%	5%	-1%	11
E.8. Information Security Management		4%	2%	5%		-22%	42
E.9. Information Systems Governance				-7%	2%	-10%	31

Wat betreft de competenties 'A.5. Architectuurontwerp', 'C.4. Probleembeheer', 'B.4. Oplossingsimplementatie', 'C.5. Systeembeheer', 'E.9. Governance van Informatiesystemen', 'E.6. Kwaliteitsmanagement en Compliance', 'B.3. Testen', 'E.3. Risicobeheer' en 'E.8. Informatiebeveiligingsmanagement' is er duidelijk meer aanbod in onderwijsprogramma's dan vraag vanuit werkgevers. Deze kloof is echter op de korte termijn niet problematisch, omdat verschillende van deze competenties in de focusgroepen en trendanalyses worden benadrukt als domeinen die in de nabije toekomst juist belangrijker zullen worden.

Een belangrijk aandachtspunt vanuit de data is dat gespecialiseerde technische vaardigheden zoals reverse engineering, virusanalyse en secure coding-methoden essentieel zijn binnen het cybersecuritydomein, ondanks het feit dat ze niet officieel worden gecategoriseerd als aparte functies of competenties binnen het ECSF. Deze vaardigheden zijn cruciaal voor functies zoals threat hunters, malware-analisten en exploit-ontwikkelaars—experts die opereren op de meest fundamentele niveaus van cyberverdediging en -aanvallen.

Nederlandse situatie

Voor Nederland zijn de vijf grootste gaps en daarmee de prioriteiten voor investeringen in opleidingen:

1. Probleembeheer (C.4., niveau 4)
2. Systeembeheer (C.5., niveau 1)
3. Risicobeheer (E.3., opvallend genoeg is er een grote kloof voor de niveaus 2, 3 en 4)

De competentiekloof C.4. Probleembeheer is cruciaal voor de stabiliteit, veiligheid en veerkracht van digitale infrastructuren, zeker nu Nederlandse organisaties hun digitale transformatie versnellen. De groeiende complexiteit van ICT-systemen vergroot de behoefte aan professionals die incidenten structureel kunnen analyseren en herhaling kunnen voorkomen. Binnen cybersecurity is probleembeheer een kerncompetentie, omdat het risico's beperkt, terugkerende kwetsbaarheden vermindert en een proactieve dreigingsaanpak mogelijk maakt. Daarmee draagt het direct bij aan zowel operationele continuïteit als digitale weerbaarheid.

C.5. Systeembeheer vormt de tweede belangrijke kloof. Trendanalyses, literatuur en focusgroepen tonen aan dat veilig configureren, monitoren en onderhouden van complexe ICT-infrastructuren onmisbaar is geworden. Goed systeembeheer voorkomt misconfiguraties, ondersteunt tijdig patchen en maakt continue monitoring en effectieve incidentrespons mogelijk. Hierdoor is systeembeheer een fundamenteel onderdeel van moderne cybersecuritystrategieën.

Daarnaast is E.3. Risicobeheer een structurele competentiekloof op meerdere niveaus (e2–e4). In een omgeving met toenemende cyberdreiging stelt deze competentie professionals in staat risico's systematisch te identificeren, prioriteren en mitigeren, en middelen doelgericht in te zetten. Tot slot benadrukken analyses het belang van E.4. Relatiemanagement: het vermogen om technische risico's begrijpelijk te vertalen naar zakelijke stakeholders is een essentiële randvoorwaarde voor effectieve cybersecurity.

Conclusies en aanbevelingen

De analyses van vacatures, trendrapporten en focusgroepen tonen glashelder waar de grootste tekorten ontstaan: in governance, risicomanagement, strategisch advies, documentatie, analyse en didactische vaardigheden.

Voor IB-professionals betekent dit dat hun rol strategischer en veelzijdiger wordt. Zij worden steeds meer gezien als sleutelfiguren in digitale weerbaarheid en als verbinders tussen techniek, bestuur en organisatiecultuur. Het onderzoekt toont dat het voor hen steeds belangrijker wordt om de taal van de 'business' te spreken en cybersecurity dreigingen bespreekbaar te maken met niet-technische stakeholders.

Voor opleiders is het een duidelijke opdracht om curricula te vernieuwen, praktijkgericht te werken en meer aandacht te besteden aan soft skills en multidisciplinaire samenwerking. Cybersecurity is niet langer een technisch specialisme; het is een essentie van moderne publieke en private dienstverlening. Het onderzoek biedt een helder kompas om deze transitie te versnellen en om Europese organisaties beter toe te rusten op de digitale uitdagingen van vandaag en morgen.

De conclusies van het onderzoek zijn duidelijk: om de digitale weerbaarheid van organisaties te versterken, is versnelling nodig op drie fronten.

Ten eerste moet het onderwijs meer modulair, praktijkgericht en up-to-date worden. Cyberranges, scenario-trainingen en hands-on oefeningen blijken onmisbaar om studenten en professionals effectief voor te bereiden op realistische situaties.

Ten tweede moeten IB-professionals zich blijven professionaliseren in governance, risicomanagement, consultancy en strategisch advies. In veel organisaties verschuift de rol van de IB-professional richting integrale regisseur van digitale veiligheid, iemand die niet alleen risico's beheert, maar ook beleid vormt, stakeholders verbindt en duurzaam gedrag stimuleert.

Ten derde vraagt de veranderende dreigingsomgeving om meer samenwerking tussen onderwijs, bedrijfsleven en overheid. Kennisdeling en gezamenlijke programma's zijn essentieel om de tekorten op te vangen en het opleidingsaanbod effectief te laten aansluiten op de praktijk. Bijvoorbeeld via praktijkgerichte learning communities waarin kennisinstellingen en organisaties

samenwerken en waarbij leren, werken en innoveren wordt geïntegreerd. Zie het kader "Voorbeeldcase: learning communities in het mkb rondom cybersecurity".

Voorbeeldcase: learning communities in het mkb rondom cybersecurity

Zes MKB-bedrijven uit Oost-Nederland overlegden tussen november 2024 en julli 2025 met elkaar in een learning community, gericht op cybersecurity en NIS2-compliance. In maandelijkse, fysieke sessies deelden deelnemers ervaringen, ontwikkelden zij gezamenlijk beleid, voerden risicoanalyses uit en bepaalden concrete verbeteracties. Tussen de bijeenkomsten pasten bedrijven deze direct toe in de eigen praktijk. Per organisatie namen meestal een ICT-verantwoordelijke en een beslisser deel. Het traject werd begeleid door een facilitator.

Terugkijkend zijn drie succesfactoren doorslaggevend: een veilige en vertrouwde leeromgeving, een sterk actiegericht leerproces; waarbij doen centraal staat, en de inzet van collectieve expertise via partners zoals het Centrum voor Veiligheid en Digitalisering (CVD). Door deze samenwerking en inbedding in het regionale ecosysteem hebben de deelnemende MKB-bedrijven concrete stappen gezet richting versterkte digitale weerbaarheid en NIS2-compliance. In terugblik spelen een drietal factoren een belangrijke rol in het succes. In de eerste plaats betreft dat het voorzien in een vertrouwde en veilige omgeving; bedrijven durven gevoelige informatie over cybersecurity te delen, omdat ze elkaar kennen via het bredere bestaande netwerk. Dit verhoogt openheid en wederzijds vertrouwen. In de tweede plaats gaat het hier om actie te ondernemen, niet alleen om het delen en opdoen van kennis. Waar klassieke kennissessies vaak passief zijn, draait de learning community om actief leren, reflectie en het direct toepassen van inzichten in de eigen organisatie. Hierdoor wordt nieuwe kennis duurzaam verankerd. Als derde en laatste factor wordt verwezen naar collectieve expertise; cyberweerbaarheid is complex, en partners zoals het Centrum voor Veiligheid en Digitalisering (CVD) bieden specialistische kennis en helpen bedrijven de juiste stappen richting NIS2 te zetten.

Geconcludeerd wordt dat door samen te werken in een learning community én gebruik te maken van het regionale ecosysteem, de zes betrokken MKB-bedrijven actief aan een verbetering van hun digitale weerbaarheid hebben gewerkt. Zo hebben ze gerichte stappen richting NIS2-compliance gezet, en bouwen ze aan een veiligere digitale toekomst.

- Doelgericht op NIS2-compliance: samen werken aan het praktisch toepassen van de NIS2-wetgeving om cyberweerbaarheid van MKB-bedrijven structureel te versterken.
- Kleine vaste groep MKB-bedrijven: circa 6 regionale MKB-bedrijven, met per organisatie 1–2 deelnemers (ICT en/of directie) die daadwerkelijk beslissingen kunnen nemen.
- Maandelijkse fysieke werksessies: bijeenkomsten van 1,5–2 uur, fysiek bij IQonIQ, met focus op samen beleid ontwikkelen, risicoanalyses uitvoeren en concrete acties bepalen.
- Sterk actiegericht leerproces: geen kennisconsumptie maar leren door doen; wat wordt besproken, wordt tussen bijeenkomsten direct getest en toegepast in de eigen organisatie.
- Professionele procesbegeleiding: een vaste facilitator bewaakt doel, voortgang en groepsdynamiek en zorgt voor effectieve werkvormen en gelijkwaardige inbreng.
- Ingebed in regionaal ecosysteem: onderdeel van een breder netwerk van IQonIQ, TechYourFuture en CVD, waarin vertrouwen, expertise en ondersteuning rond cyberveiligheid centraal staat

Referenties

- Almeida, F. (2025). Comparative analysis of EU-based cybersecurity skills framework. Computers & Security, 151(1), 1-10.
- Cedefop. (2020). Vocational education and training Europe 1995-2035: Scenarios for European VET systems. Publications Office of the European Union. Retrieved from https://www.cedefop.europa.eu/files/3083_en.pdf.
- Cisco. (2024). Cyber Threat Trends Report: From Trojan Takeovers to Ransomware Roulette.
- Digital Skills and Jobs Platform. (2023). Digital Experts: a deep-dive. Retrieved from https://digital-skills-jobs.europa.eu/en/latest/briefs/digital-experts-deep-dive-0.
- PTvT/Dialogic. (2024). Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity. Retrieved from https://open.overheid.nl/documenten/c0ac3595-28e3-43df-aa85-7d9e8a426c25/file.
- World Economic Forum. (2025). Global Cybersecurity Outlook 2025.

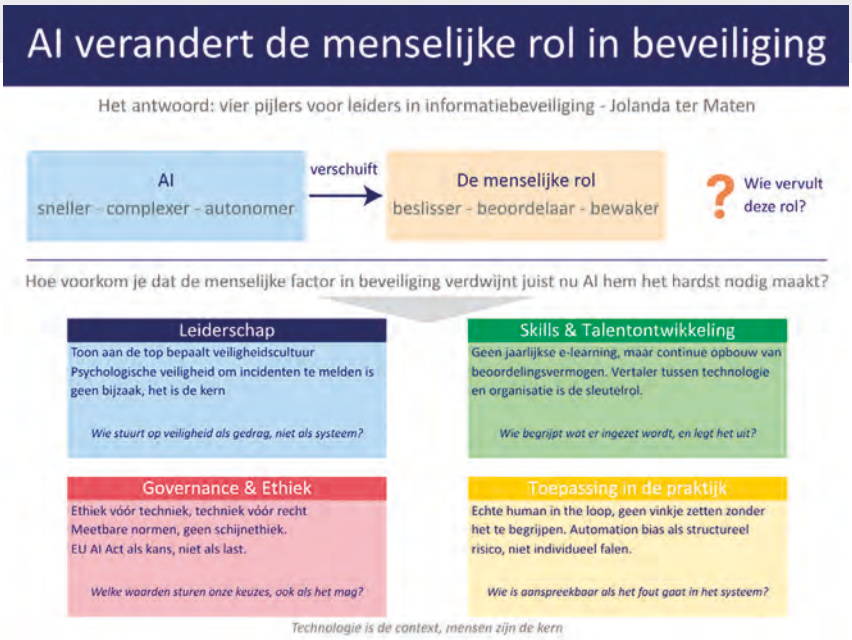
De volledige lijst met referenties is in te zien via: www.cadmus-project.eu

Auteur: Jolanda ter Maten MSc is eigenaar van Jolanda ter Maten – Connecting Knowledge en werkzaam als trusted advisor en mensgerichte AI-strateeg. Zij adviseert toonaangevende organisaties, waaronder de Europese Commissie, Nederlandse ministeries en Defensie, over verantwoord AI-leiderschap en de menselijke dimensie van digitale transformatie. Als keynote spreker staat zij bekend om haar vermogen technologische complexiteit te vertalen naar strategisch en organisatorisch handelen. Haar boek "Modern leiderschap is geen algoritme" verschijnt medio 2026. Zij is bereikbaar via: info@jolandatermaten.co

De firewall die we vergeten te bouwen

Over leiderschap, mensen en de blinde vlek in informatiebeveiliging

AI verandert informatiebeveiliging. Niet alleen omdat het nieuwe aanvalsoppervlakken creëert: deepfakes, geautomatiseerde phishing op schaal, aanvallen die zich in real-time aanpassen aan detectiesystemen. Maar ook, en dat is minder besproken, omdat het de rol van de mens in het beveiligingslandschap fundamenteel opschuift.



Figuur 1: Technologie is de context, mensen zijn de kern

De professional die jarenlang getraind is om patronen te herkennen, werkt nu naast systemen die patronen herkennen met een snelheid en schaal die geen mens kan evenaren. De manager die vroeger een weloverwogen beslissing nam op basis van een rapportage, krijgt nu een algoritmisch advies dat hij in de praktijk zelden echt toetst. En de medewerker die werd getraind op 'klik niet op verdachte links' staat nu tegenover aanvallen waarbij het onderscheid tussen echt en nep nauwelijks nog te maken is.

Dit is niet het einde van de menselijke factor in informatiebeveiliging. Het is het begin van een veel complexere versie ervan. En die complexere versie vraagt om iets wat in de technisch-operationele kern van ons vakgebied nog te weinig aandacht krijgt: een fundamenteel andere manier van investeren in mensen. Vanuit mijn werk met organisaties op het snijvlak van AI, technologie en leiderschap herken ik vier dimensies die daarin het verschil maken.

'AI maakt de mens niet alleen een kwetsbaardere schakel, het maakt hem ook een onzekerder beoordelaar. Dat vraagt om een fundamenteel andere investering in mensen.'

Leiderschap: de toon aan de top bepaalt de cultuur aan de basis

Informatiebeveiliging is een leiderschapsvraagstuk. Niet in de zin dat de CISO meer budget moet krijgen, hoewel dat in veel gevallen ook niet zou misstaan, maar in de fundamentelere zin: de houding van leiders ten opzichte van risico, openheid en verantwoordelijkheid sijpelt door in de hele organisatie.

Ik spreek regelmatig bestuurders die mij vertellen dat beveiliging 'geregeld' is. Ze bedoelen daarmee: we hebben er mensen voor. Maar beveiliging is niet iets wat je delegeert en vergeet. Het vraagt om leiders die zelf begrijpen wat ze inzetten, bereid zijn vragen te stellen waarvan ze het antwoord niet kennen, en een cultuur creëren waarin medewerkers incidenten durven te melden zonder bang te zijn voor de gevolgen.

Dat laatste is crucialer dan het lijkt. Onderzoek laat consequent zien dat de meeste beveiligingsincidenten pas laat worden gemeld, of helemaal niet, omdat mensen bang zijn voor de reactie (1). Een technisch perfecte meldprocedure werkt niet als de psychologische veiligheid ontbreekt om hem te

Figuur 2: De firewall die we vergeten te bouwen

gebruiken. Leiderschap dat veiligheid serieus neemt, begint bij het creëren van ruimte om fouten te benoemen.

Skills & talentontwikkeling: kennis is geen eenmalige investering

De gemiddelde medewerker weet niet hoe een phishingmail werkt. Niet omdat hij of zij onzorgvuldig is, maar omdat niemand het ooit serieus heeft uitgelegd. En de eenmalige e-learning die jaarlijks verplicht moet worden afgerond, telt daarvoor niet.

Effectieve vaardigheidsopbouw rond informatiebeveiliging vraagt om iets anders: inzicht in hoe mensen daadwerkelijk beslissingen nemen onder tijdsdruk. Het menselijk brein reageert op potentieel gevaar in milliseconden, lang voordat de rationele afweging plaatsvindt. Dat is evolutionair gezien slim, maar digitaal gezien gevaarlijk. Wie begrijpt hoe cognitieve shortcuts werken, begrijpt ook waarom awareness-campagnes zo weinig effect hebben als ze louter informatief zijn.

Wat werkt: herhaling, context en oefening in realistische situaties. Niet een jaarlijkse module, maar een doorlopend programma dat aansluit bij de werkelijkheid van de medewerker. En: investeren in de mensen die de vertaalslag kunnen maken tussen technische complexiteit en begrijpelijke werkwijzen. Zij zijn de schakelaar tussen IT en de rest van de organisatie, en ze zijn schaarser dan we denken.

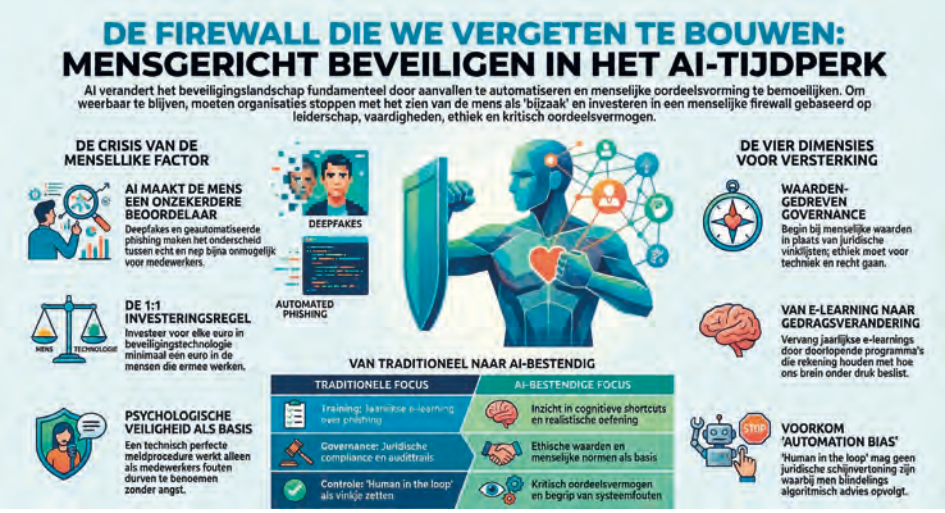
'Het menselijk brein reageert op potentieel gevaar in milliseconden. Wie dat begrijpt, begrijpt ook waarom een jaarlijkse e-learning niet werkt.'

Governance & ethiek: beleid dat begint bij waarden

Met de komst van de EU AI Act (2) en de bredere discussie over digitale regulering staat de vraag naar governance hoger op de agenda dan ooit. Maar governance is meer dan compliancelijsten en audittrails. De fundamentelere vraag is: op welke waarden baseren wij onze keuzes over technologie?

In de praktijk zie ik een patroon dat ik schijnethiek noem: mooie AI-principes op papier, zonder meetbare criteria, consequenties of externe controle (3). Organisaties die zeggen dat ze 'verantwoord' werken met data, maar waarbij niemand precies kan uitleggen wat dat in de dagelijkse praktijk betekent. Dat is geen kwaadwil, het is het gevolg van governance die juridisch is ingericht, maar ethisch leeg is.

Een betere volgorde: begin bij de waarden die uw organisatie wil uitdragen. Wat vindt u acceptabel; niet juridisch, maar menselijk? Vertaal dat naar concrete normen voor de inzet van AI en data. En bouw vervolgens de juridische en technische



Figuur 3: Mensgericht beveiligen in het AI-tijdperk

kaders die die normen ondersteunen. Ethiek gaat voor techniek, en techniek gaat voor recht. Niet omdat recht onbelangrijk is, maar omdat regelgeving per definitie beschrijft wat al bestaat, niet wat eraan komt.

De digitale omnibus (4), die begin 2025 een reeks Europese digitale regelgevingen verzachtte, illustreert het risico van de omgekeerde volgorde. Wanneer compliancedruk wordt verminderd op het moment dat AI-toepassingen in kritieke sectoren groeien, neemt de blootstelling toe terwijl de beschermende kaders zwakker worden. Governance die niet op waarden is gebouwd, is kwetsbaar voor precies dit soort politieke verschuivingen.

Toepassing in de praktijk: de mens die ertussen wil zitten

De vierde dimensie is misschien wel de meest concrete, en tegelijkertijd de meest onderschatte. Het gaat over wat er daadwerkelijk gebeurt op de werkvloer, op het moment dat iemand een beslissing moet nemen over een systeem dat hij niet volledig begrijpt. 'Human in the loop' is een term die inmiddels breed wordt gebruikt in AI-governance. Maar in de praktijk betekent het vaak: een mens die een vinkje zet bij een algoritmisch advies, zonder de context of de capaciteit om dat advies kritisch te beoordelen. Dat is geen menselijke controle, dat is een juridische constructie die de schijn van controle wekt. Echte betrokkenheid van mensen vraagt om iets anders. Het vraagt om mensen die begrijpen wat een systeem doet, wanneer het fouten maakt, en wat de consequenties zijn van specifieke keuzes. Het vraagt om organisaties die automation bias (5), de neiging om algoritmische uitkomsten minder kritisch te beoordelen dan menselijke adviezen, serieus nemen als een structureel risico, niet als een individueel falen. ENISA benoemt dit expliciet als één van de belangrijkste mensgerichte risico's in AI-toepassingen (6). Een praktische vuistregel die ik in mijn werk gebruik: voor elke euro die een organisatie investeert in beveiligingstechnologie, zou minimaal een vergelijkbare investering moeten gaan naar de mensen die ermee werken: hun begrip, hun oordeelsvermogen, hun vermogen om te handelen als het systeem hen in de steek laat. In de huidige praktijk is die verhouding vrijwel altijd omgekeerd. De technologie krijgt het leeuwendeel; de menselijke kant wordt gezien als bijzaak.

'Voor elke euro in beveiligingstechnologie zou een vergelijkbare investering moeten gaan naar de mensen die ermee werken. In de praktijk is die verhouding omgekeerd.'

De firewall die we wél kunnen bouwen

Informatiebeveiliging is mensenwerk. Niet in de betekenis dat technologie er niet toe doet, die doet er wel degelijk toe, maar in de betekenis dat technologie alleen werkt als de mensen die haar inzetten, besturen en er dagelijks mee omgaan, begrijpen wat ze doen en waarom. De vier dimensies die ik beschreef, leiderschap, vaardigheidsontwikkeling, ethische governance en echte menselijke betrokkenheid in de praktijk, zijn geen zachte randvoorwaarden. Ze zijn de kern van wat beveiliging effectief maakt. En ze zijn, in de meeste organisaties die ik ken, structureel onderbelicht. De vraag is niet of we dit kunnen. De vraag is of we bereid zijn te investeren in wat we het moeilijkst vinden: niet de technologie, maar de mensen.

Referenties

(1) Nationale Cybersecurity Strategie 2022-2028, Ministerie van Justitie en Veiligheid, Den Haag, 2022.

(2) Europees Parlement & Raad, Verordening (EU) 2024/1689 inzake kunstmatige intelligentie (AI Act), 13 juni 2024.

(3) NIST, Artificial Intelligence Risk Management Framework (AI RMF 1.0), National Institute of Standards and Technology, 2023.

(4) Europese Commissie, Omnibus I-pakket - Vereenvoudiging van duurzaamheids- en digitale regelgeving, COM(2025) 81 final, februari 2025.

(5) Cummings, M.L., Automation Bias in Intelligent Time Critical Decision Support Systems, AIAA 1st Intelligent Systems Technical Conference, 2004.

(6) ENISA, AI Cybersecurity Risks - Threat Landscape for Artificial Intelligence, Europees Agentschap voor Cybersecurity, 2023.

Auteurs: Manja Koomen en Ivan Veul zijn beiden onderzoekers en Burhan Gün is onderzoeksdirecteur bij de Algemene Rekenkamer. Zij zijn bereikbaar via: voorlichting@rekenkamer.nl

Quantumdreiging voor de Rijksoverheid:

het is tijd om te migreren naar post-quantum cryptografie

Quantumtechnologie staat internationaal hoog op de politieke en technologische agenda. De Verenigde Naties riepen 2025 uit tot het International Year of Quantum Science and Technology. Een symbolisch moment, precies honderd jaar nadat de quantummechanica werd ontwikkeld. Wereldwijd wordt door overheden, universiteiten en bedrijven flink geïnvesteerd in quantumtechnologie. Ook Nederland positioneert zich nadrukkelijk in dit domein.

Voor de Nederlandse rijksoverheid is quantumtechnologie een van de sleuteltechnologieën binnen de Nationale Technologiestrategie. Sleuteltechnologieën zijn essentieel bij het oplossen van maatschappelijke uitdagingen en leveren een bijdrage aan onze economie. Nederland beschikt bovendien over sterke wetenschappelijke expertise op dit terrein, met onderzoekscentra zoals QuTech en het Centrum Wiskunde & Informatica (CWI). Via het Nationaal Groeifonds investeert de overheid tussen 2021 en 2028 minimaal €615 miljoen in de ontwikkeling van quantumtechnologie.

De focus op quantumtechnologie heeft meerdere redenen. Enerzijds gaat het om economische kansen. Quantumtechnologie kan bijdragen aan bijvoorbeeld de ontwikkeling van nieuwe medicijnen, betere batterijtechnologie, optimalisatieproblemen in logistiek en energiegebruik en nieuwe materialen. Anderzijds speelt technologische soevereiniteit een belangrijke rol. Door te investeren in quantumtechnologie kan Nederland (in de toekomst) minder afhankelijk zijn van andere technologische grootmachten.

Tegelijkertijd brengt quantumtechnologie ook nieuwe risico's met zich mee. Met name quantumcomputers vormen een potentiële bedreiging voor de huidige digitale beveiliging. Vrijwel alle digitale communicatie, authenticatie en gegevensopslag maken gebruik van cryptografie. Onze huidige cryptografische systemen zijn ontworpen tegen aanvallen van klassieke computers. Quantumcomputers werken echter volgens een fundamenteel andere rekenlogica en kunnen bepaalde wiskundige problemen veel sneller oplossen. Dat betekent dat een voldoende krachtige quantumcomputer bestaande versleutelingstechnieken kan kraken. Wanneer dat gebeurt, kunnen vertrouwelijke gegevens worden ontsleuteld en kan digitale authenticatie worden ondermijnd. Voor overheden raakt dit direct aan nationale veiligheid, vertrouwelijkheid van staatsinformatie en de betrouwbaarheid van vitale infrastructuur.
De Algemene Rekenkamer onderzocht daarom in het rapport Focus op Quantum bij de rijksoverheid (1) hoe de rijksoverheid zich voorbereidt op deze technologische ontwikkeling. De centrale vraag is: hoe bereidt de rijksoverheid zich voor op de kansen en risico's van quantumtechnologie? In dit artikel kijken we naar de risico's. De scope van het onderzoek is de Nederlandse rijksoverheid: ministeries, hun diensten en zelfstandige bestuursorganen. We hebben hierbij organisaties geselecteerd die verantwoordelijk zijn voor kritieke processen, gegevensverwerking of vitale infrastructuur. In totaal zijn 63 organisaties onderzocht die mogelijk een doelwit kunnen worden van toekomstige aanvallen met quantumcomputers.

Quantumcomputers

Wat zijn quantumcomputers eigenlijk? Quantumcomputers maken gebruik van eigenschappen van subatomaire deeltjes, zoals superpositie en verstrengeling. Waar klassieke computers werken met bits (0 of 1) gebruiken quantumcomputers qubits. Deze kunnen tegelijkertijd meerdere toestanden aannemen. Daardoor kunnen quantumcomputers bepaalde berekeningen veel sneller uitvoeren. Quantumcomputers zijn in het bijzonder goed in het kraken van cryptografie. Sommige cryptografische systemen, zoals RSA en elliptische-curve-cryptografie, zijn gebaseerd op wiskundige problemen waar klassieke computers miljoenen jaren over doen om te kraken. Quantumcomputers kunnen deze problemen echter binnen enkele dagen of uren oplossen met algoritmen zoals dat van Shor (2). Hoewel deze technologie nog volop in ontwikkeling is, staat vast dat de impact groot kan zijn. Quantumcomputers vormen een disruptieve factor voor de huidige informatiebeveiliging. Juist daarom is voorbereiding noodzakelijk, ook al is nog niet precies bekend wanneer krachtige quantumcomputers daadwerkelijk beschikbaar zullen zijn.

De dreiging van quantumcomputers voor de overheid

Cryptografie is de basis van vrijwel alle digitale beveiliging: van internetverbindingen en e-mail tot authenticatie, digitale handtekeningen en toegangssystemen.

Binnen de overheid beschermt cryptografie onder meer:

- Vertrouwelijke informatie van burgers en bedrijven.
- Authenticatie van digitale identiteiten zoals DigiD.
- Communicatie tussen overheidsorganisaties.
- Toegang tot vitale infrastructuur zoals sluizen, bruggen en waterkeringen.
- Echtheidskenmerken van documenten zoals paspoorten.

Wanneer quantumcomputers cryptografische sleutels kunnen kraken, wordt de betrouwbaarheid van al deze systemen aangetast. Een aanval kan dan bijvoorbeeld leiden tot manipulatie van gegevens, identiteitsfraude of verstoring van vitale infrastructuur.
De dreiging zal vooral afkomstig zijn van statelijke actoren. Quantumcomputers zijn extreem duur en vereisen specialistische infrastructuur. Het is daarom waarschijnlijk dat vooral landen met grote onderzoeksprogramma's als eerste over zulke technologie beschikken. Hoe groot die dreiging precies is, hangt af van de ontwikkeling van quantumhardware. Het

moment waarop een quantumcomputer krachtig (3) genoeg is om bestaande cryptografie te breken wordt vaak aangeduid als Q-day. Wanneer dat moment precies komt, is onzeker. Schattingen variëren van vijf jaar tot meerdere decennia. Die onzekerheid betekent echter niet dat organisaties kunnen wachten. Er zijn drie belangrijke redenen waarom voorbereiding nu al noodzakelijk is:

- Het kraken van cryptografie kan enorme gevolgen hebben voor nationale veiligheid en vertrouwen in de overheid.
- De overgang naar nieuwe cryptografie is complex en kan vele jaren duren. Organisaties moeten systemen inventariseren, software aanpassen, leveranciers betrekken en beleid ontwikkelen.
- Er bestaat nu al een reële dreiging in de vorm van store now, decrypt later-aanvallen. Daarbij verzamelen aanvallers versleutelde gegevens met de bedoeling deze later te ontsleutelen zodra quantumcomputers dat mogelijk maken.

Voor de rijksoverheid zal de impact van een succesvolle aanval groot zijn. Daarom adviseren organisaties zoals de AIVD, het Nationaal Cyber Security Centrum en de Europese Commissie om nu al te beginnen met voorbereidingen. De belangrijkste technische oplossing is het omzetten van bestaande cryptografie naar post-quantum cryptografie (PQC). Dit zijn cryptografische algoritmen die bestand zijn tegen aanvallen van quantumcomputers.

Stappen voor quantumveilige cryptografie

De overgang naar post-quantum cryptografie is geen eenvoudige software-update. Het gaat om een grootschalige transitie die alle onderdelen van een organisatie raakt: infrastructuur, applicaties, inkoop, beleid en governance. Het PQC-migratiehandboek (4) van AIVD, TNO en het Centrum Wiskunde & Informatica beschrijft een aantal kernstappen die organisaties moeten doorlopen.

Quantumrisico's analyseren

De eerste stap is het opnemen van quantumdreiging in het risicomanagement. Organisaties moeten bepalen welke processen afhankelijk zijn van cryptografie en hoe groot de impact van een mogelijke aanval is. Voor veel organisaties is dit een uitdaging. Zij hebben vaak al te maken met andere urgente cyberdreigingen zoals ransomware, kwetsbaarheden of DDoS-aanvallen. Juist daarom is het vanwege de mogelijk grote impact belangrijk om quantumdreiging tijdig mee te nemen in strategische risicoafwegingen.

Cryptografie inventariseren

Een van de meest complexe stappen is het in kaart brengen van cryptografie binnen systemen. Moderne IT-systemen en netwerken bestaan uit honderden componenten en softwarebibliotheken. Elk daarvan kan cryptografische functies bevatten. Organisaties moeten daarom niet alleen hun informatiesystemen inventariseren, maar ook de cryptografische mechanismen die daarin zijn ingebouwd. Zonder deze inventarisatie is een migratie naar PQC praktisch onmogelijk.

Afspraken maken met leveranciers

Een groot deel van de cryptografie binnen organisaties bevindt zich in software en hardware van externe leveranciers. Denk aan cloudplatforms, digitale werkplekken, netwerkapparatuur en applicaties. Organisaties moeten daarom vroegtijdig met leveranciers in gesprek gaan over de ondersteuning van quantumveilige cryptografie. Wanneer leveranciers hun producten niet aanpassen, kan dat leiden tot afhankelijkheidsproblemen of noodzakelijke migraties naar andere leveranciers.

Cryptografiebeleid opstellen

Goed cryptografiebeheer vereist duidelijke governance. Een cryptografiebeleid beschrijft onder meer:

- Welke cryptografie gebruikt mag worden.
- Hoe cryptografische sleutels beheerd worden.
- Welke rollen verantwoordelijk zijn voor cryptografische beslissingen.
- Hoe compliance met regelgeving wordt geborgd.

Binnen de rijksoverheid is cryptografiebeleid al verplicht via de Baseline Informatiebeveiliging Overheid (BIO). Het PQC-vraagstuk maakt deze verplichting nog relevanter.

Migratie aansturen

De migratie naar PQC vereist duidelijke bestuurlijke aansturing. Organisaties moeten een verantwoordelijke aanwijzen, een planning opstellen en capaciteit reserveren. Zonder governance bestaat het risico dat het onderwerp versnipperd raakt tussen IT-teams, securityspecialisten en leveranciers.

Cryptografie vervangen

De laatste stap is het daadwerkelijk vervangen van cryptografie door PQC-algoritmen. Dit zal stapsgewijs gebeuren, waarbij eerst de meest kritieke processen worden aangepakt.
Momenteel zijn nog relatief weinig commerciële producten beschikbaar met PQC-ondersteuning. Daardoor bevinden veel organisaties zich nog in de voorbereidende fase.

Naast PQC wordt ook gekeken naar **Q**uantum **K**ey **D**istribution (QKD), een techniek voor veilige sleuteluitwisseling. Experts zien

deze technologie echter vooral als niche-oplossing. PQC blijft voorlopig de belangrijkste strategie.

De rijksoverheid en de bredere geopolitieke context

Het onderzoek van de Algemene Rekenkamer laat zien dat de rijksoverheid nog aan het begin staat van de voorbereiding op quantumdreiging.
Bij de 63 onderzochte organisaties zien we dat:

- 71% nog niet is begonnen met specifieke maatregelen tegen quantumdreiging.
- Slechts 6% de dreiging heeft opgenomen in risicomanagementprocessen.
- Geen enkele organisatie een tijdslijn heeft vastgesteld voor de PQC-migratie.

Wel werken veel organisaties al aan algemene informatiebeveiliging, bijvoorbeeld via de implementatie van de BIO en de NIS2-wetgeving. Deze trajecten kunnen een basis vormen voor PQC-migraties, omdat ze organisaties dwingen om kritieke processen en systemen te definiëren en verantwoordelijken aan te wijzen.
Quantumspecifieke voorbereidingen blijven echter noodzakelijk. De implementatie van de BIO en NIS2 biedt een fundament, maar organisaties moeten voor quantumdreiging meer doen. Denk aan gedetailleerde inventarisaties van cryptografie, samenwerkingen met leveranciers over PQC en het daadwerkelijk migreren van cryptografie. De omvang en complexiteit van de PQC-migratie mogen niet onderschat worden. Daarom is het voor organisaties van belang om nú te starten, ook als inventarisaties en andere maatregelen niet perfect zijn.

Volgens het onderzoek zijn een gebrek aan capaciteit en expertise, evenals de prioritering van andere IT-vraagstukken de belangrijkste redenen waarom overheidsorganisaties nog niet begonnen zijn met hun aanpak van de quantumdreiging. Voor veel organisaties voelt de quantumdreiging nog als een toekomstprobleem. Cyberaanvallen, kwetsbaarheden en IT-modernisering hebben vaak een hogere urgentie. Juist omdat organisaties hun beperkte middelen moeten verdelen over meerdere IT-dreigingen, is het essentieel dat de dreiging van quantumcomputers wordt meegenomen in risicomanagementprocessen en wordt afgewogen tegen andere dreigingen. Alleen dan kunnen overheidsorganisaties bewuste keuzes maken over de veiligheid van hun netwerk- en informatiesystemen.
Om organisaties te ondersteunen heeft het ministerie van Binnenlandse Zaken het programma **Q**uantum**v**eilige **C**ryptografie **NL** (QvC NL) opgezet. Dit programma richt zich op bewustwording, kennisdeling en ondersteuning bij de migratie naar PQC. Daarnaast speelt ook de Europese Unie een rol. In 2025 publiceerde de Europese Commissie samen met de lidstaten een routekaart voor een gecoördineerde migratie naar post-quantum cryptografie. Deze routekaart benadrukt dat migraties meerdere jaren zullen duren en dat lidstaten tijdig moeten beginnen. De Nederlandse Digitaliseringsstrategie (NDS) noemt quantumveilige cryptografie inmiddels als een strategisch doel voor de overheid. Het kabinet werkt nu aan een Rijksbrede Quantum Strategie. De strategie gaat in op de kansen en risico's van quantumtechnologie en zal naar verwachting in het tweede kwartaal van 2026 aan de Tweede Kamer worden aangeboden.

Een dreiging die nú voorbereiding vraagt

Hoewel quantumcomputers nu nog geen directe inbreuk maken op onze cryptografie, is uitstel geen optie. De migratie naar quantumveilige cryptografie is een complexe en langdurige operatie die alle lagen van de overheid raakt. Voor de rijksoverheid betekent dit dat de focus moet verschuiven van bewustwording naar uitvoering. Organisaties moeten versneld aan de slag met inventarisaties, cryptografiebeleid, governance en samenwerkingen met leveranciers.
Deze uitdaging staat niet op zichzelf. Wereldwijd investeren landen als de Verenigde Staten, China en Europese lidstaten miljarden in quantumonderzoek. Tegelijkertijd bereiden zij zich voor op de beveiligingsrisico's die quantumcomputers met zich meebrengen. Voor overheden gaat het daarbij niet alleen om technologische innovatie, maar ook om digitale soevereiniteit en nationale veiligheid. Als de Nederlandse overheid te laat begint met de overgang naar quantumveilige cryptografie, loopt het risico dat vertrouwelijke informatie in de toekomst alsnog wordt ontsleuteld.

Quantumdreiging is daarmee een typisch voorbeeld van een strategisch informatiebeveiligingsvraagstuk: de impact is onzeker en ligt in de toekomst, maar de noodzakelijke maatregelen moeten vandaag al worden genomen.

Referenties

(1) https://www.rekenkamer.nl/documenten/2026/02/04/focus-op-quantum-bij-de-rijksoverheid
(2) https://en.wikipedia.org/wiki/Shor's_algorithm
(3) De kracht van een quantumcomputer wordt gemeten in het aantal logische qubits. Schattingen lopen uiteen, maar experts denken dat ongeveer 1.000 tot 3.000 logische qubits nodig zijn om veelgebruikte cryptografie te kraken. De grootste huidige quantumcomputers hebben in de orde van 10 logische qubits.
(4) https://www.aivd.nl/documenten/2024/12/3/het-pqc-migratie-handboek

Auteur: Ir. Manon de Vries is senior onderzoeker toegepaste cryptografie bij TNO en docent quantumveilige cryptografie en PKI bij de Security Academy (onderdeel van DNV). Dr. Alessandro Amadori, Dr. Dayana Spagnuelo en Drs. Michiel Marcus zijn medeonderzoekers bij TNO. Prof.dr.ir. Nitesh Bharosa is professor Govtech en Innovatie bij de Technische Universiteit Delft. Prof.dr. Serge Fehr is onderzoeker bij de Cryptografie groep van het CWI en professor bij de faculteit Wiskunde en Natuurwetenschappen van de Leiden Universiteit. Allen nemen deel aan het HAPKIDO project. Hoofdauteur Manon de Vries is te bereiken op manon.devries@tno.nl.

Hybride cryptografie in quantumveilige PKI

Publieke sleutelinfrastructuur (PKI) vormt de ruggengraat van digitaal vertrouwen. Vrijwel elke vorm van digitale beveiliging — van TLS verbindingen tot digitale handtekeningen — vertrouwt op cryptografische sleutels waarvan de authenticiteit (de koppeling tussen cryptografische sleutels en een identiteit) met een PKI stelsel wordt geborgd. De huidige cryptografische algoritmen die onze PKI infrastructuur gebruikt, zijn echter kwetsbaar voor digitale aanvallen die gebruikmaken van quantumcomputers. Het risico dat toekomstige quantumcomputers deze algoritmen kunnen breken, maakt een transitie naar quantumveilige cryptografie noodzakelijk. Voor de nieuwe quantumveilige algoritmen wordt de term **PQC** – **P**ost **Q**uantum **C**ryptografie – gebruikt, als tegenhanger van de klassieke cryptografie.

Figuur 1: De klassieke, quantumveilige en drie hybride versleutelingsvarianten.

Een aantal nieuwe PQC algoritmen zijn inmiddels gestandaardiseerd, maar staan qua volwassenheid alsook implementatie ervaring, en vertrouwen dat de gemeenschap erin heeft, nog niet op hetzelfde niveau als de klassieke tegenhangers. Een kwetsbaarheid in deze nieuwe algoritmes kan leiden tot grote schade. Zelfs als dit een kleine kans vertegenwoordigt, leidt dit tot een hoog risico. Om deze reden adviseren diverse Europese instellingen om niet de huidige cryptografie te vervangen, maar te combineren: klassieke cryptografie én PQC tegelijk. Deze hybride aanpak creëert twee lagen van beveiliging — als één algoritme faalt, blijft het andere overeind.

Het HAPKIDO-project onderzoekt deze hybride transitie zowel vanuit cryptografisch, technisch en organisatorisch perspectief, inclusief praktische implementatie in PKI standaarden, codebibliotheken en operationele processen. Dit artikel focust zich op de opgedane kennis rondom de technische implementatie van hybride cryptografie in PKI.

Hierbij is één van de belangrijkste observaties dat hybride cryptografie op twee manieren kan worden verwezenlijkt. De eerste mogelijkheid is om het algoritme zelf hybride te maken, waarbij onder andere de twee sleutels en handtekeningen worden gecombineerd tot één zichtbare sleutel, één zichtbare handtekening et cetera, zodat het hybride aspect weg geabstraheerd is van de implementatie. De tweede mogelijkheid is om aanpassingen te maken aan protocollen en andere code om een tweede algoritme te kunnen ondersteunen. Bij de experimenten met de laatste variant binnen PKI valt op dat het tweede algoritme vaak optioneel wordt aangeboden, voor compatibiliteitsredenen, waarbij het beveiligingsdoel van twee lagen niet bereikt wordt.

Quantumcomputer versus cryptografie

Cryptografie wordt ingezet voor het verkrijgen van digitale beveiliging. Voorbeelden waar cryptografie een belangrijke rol speelt zijn het versleuteld bezoeken van websites, pintransacties, inloggen bij DigiD en het elektronisch patiëntendossier. Vaak gebruiken dit soort systemen verschillende cryptografische technieken om hun doelen te behalen. Cryptografische versleuteling biedt bijvoorbeeld vertrouwelijkheid, ondertekening waarborgt integriteit, authenticiteit en onweerlegbaarheid. Authenticatie, vaak door middel van cryptografische methoden, biedt zekerheid over met wie er wordt gecommuniceerd; een essentiële voorwaarde voor vertrouwelijkheid en autorisatie, waarbij alleen bevoegde entiteiten toegang mogen hebben tot data of systemen.

De cryptografische algoritmes die hiervoor worden ingezet, zijn gebaseerd op een aantal wiskundige technieken. Er is veel bewijs voor de veiligheid van deze algoritmes, gegeven het type computers dat we tot nu toe kennen en gebruiken.

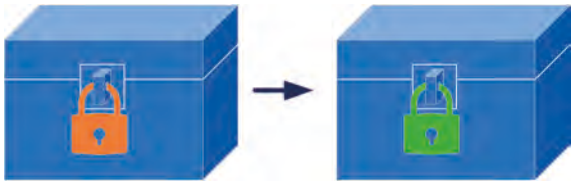
Echter weten we sinds eind jaren 80 (1) dat er een nieuw type computer mogelijk is, die fundamenteel anders werkt: de quantumcomputer. Tegenwoordig is dit niet langer theoretisch, want primitieve versies van de quantumcomputers bestaan en worden actief doorontwikkeld, hoewel de prestaties nog beperkt zijn.
De quantumcomputer brengt nieuwe risico's mee. Indien een quantumcomputer van een bepaalde sterkte wordt gebouwd – vaak gemeten in de hoeveelheid qubits, circuitdiepte en stabiliteit die het ondersteunt - kan het worden ingezet om een aantal veelgebruikte cryptografische algoritmes te kraken (2). Hiermee kan een aanvaller geheime cryptografische sleutels achterhalen om daarmee digitale infrastructuur aan te vallen.

Voor de getroffen versleutelingsalgoritmes betekent dit, dat versleutelde informatie kan worden ingezien: vertrouwelijkheid wordt gebroken. Bovendien raakt dit risico ons al vóór de quantumcomputer het kan ontsleutelen: versleutelde informatie die lang interessant blijft, kan een aanvaller nu al opslaan, om later met de quantumcomputer te ontsleutelen:

dit wordt de store-now-decrypt-later aanval genoemd.
Voor digitale handtekeningen, die vaak gebruikt worden voor authenticatie, is de impact pas merkbaar op het moment dat de quantumcomputer sterk genoeg is ("q-day"): een aanvaller kan zich op dat moment voordoen als zijn doelwit. Dit kan enorme gevolgen hebben, de DigiNotar hack is daar een goed voorbeeld van geweest (3).

Als digitale handtekeningen worden gebruikt om onweerlegbaarheid, integriteit of authenticiteit te waarborgen, kan een aanvaller na q-day de handtekeningen vervalsen: berichten kunnen worden aangepast (software updates of betalingen bijvoorbeeld), en het vertrouwen in digitaal ondertekende documenten wordt ondermijnd.

PQC als antwoord



Figuur 2: Vervanging klassieke versleuteling door PQC versleuteling.

Om dit risico weg te nemen moeten de kwetsbare algoritmes worden vervangen door quantumveilige algoritmes, aangeduid met de parapluterm PQC: Post Quantum Cryptography. Er zijn inmiddels meerdere nieuwe algoritmes ontwikkeld en gestandaardiseerd (4), zowel voor versleuteling als ondertekening.

Waarom hybride?

Figuur 3: Hybride versleuteling.

Vergeleken met de klassieke cryptografie zijn de PQC-algoritmes complexer, de robuustheid tegen onbedoelde informatielekkage in hardware is moeilijker, en de algoritmes hebben - buiten veel academisch onderzoek - niet tientallen jaren aan implementatie-ervaring. Met cryptografie is de gemeenschap doorgaans erg conservatief, omdat een kwetsbaarheid ernstige gevolgen kan hebben en migratie veel werk is. Ondanks het feit dat PQC-algoritmes jarenlang uitvoerig zijn getest en er ondertussen een aantal gestandaardiseerd zijn, zijn niet alle landen voor directe vervanging van een klassiek, kwetsbaar algoritme door een PQC-algoritme: wat als in het nieuwe algoritme toch nog een fout wordt ontdekt?

Daarom adviseren diverse Europese instellingen om niet cryptografie te vervangen, maar te combineren: klassieke cryptografie én PQC samen. Deze hybride aanpak creëert twee lagen van beveiliging — als één algoritme faalt, blijft het andere overeind. Het vertrouwde klassieke algoritme zorgt voor beveiliging tegen traditionele aanvallen terwijl het PQC-algoritme quantum-veiligheid toevoegt.

Er bestaan hybride oplossingen voor zowel encryptie (sleuteluitwisseling) als digitale handtekeningen. Voor encryptie wordt er feitelijk twee keer een sleuteluitwisseling gedaan (al dan niet in één conversatie) en worden de resulterende sleutels veilig gecombineerd (daar zijn zogenoemde combiner functies voor (5)) en vervolgens gebruikt voor encryptie. Bij de digitale handtekening worden er twee handtekeningen gezet op de bron en moeten beide handtekeningen geldig zijn.

HAPKIDO

HAPKIDO is een 5-jarig NWO gefinancierd onderzoeksproject over de implicaties en implementatie van Hybride cryptografie: specifiek in het PKI-domein. Het is een consortium van meerdere partijen (TNO, CWI, TU Delft, Logius, KPN, Microsoft en Zynyo) dat zowel de organisatorische, bestuurlijke en technische aspecten onderzoekt van dit onderwerp. Het project test zowel theoretische aspecten, zoals de benodigde eigenschappen van "combiners", als ook praktische aspecten: wat moet er technisch worden aangepast om hybride cryptografie te ondersteunen. Daarnaast wordt de impact op PKI geanalyseerd, ketenafhankelijkheden in kaart gebracht en handvatten gemaakt voor effectieve migratie van PKI naar hybride cryptografie. Dit artikel maakt gebruik van opgedane inzichten over de technische impact van hybride cryptografie.

> Migratie van PKI heeft ook allerlei bestuurlijke en organisatorische stappen en uitdagingen, met allerlei afhankelijkheden binnen het ecosysteem. Die laten we in dit artikel buiten scope. Voor meer informatie over die aspecten, zie https://hapkido.tno.nl.

Wie wil hybride?

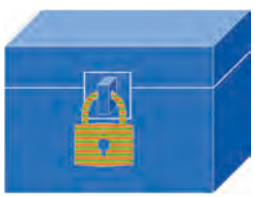
De noodzaak voor hybride wordt niet overal op dezelfde manier gevoeld. Voornamelijk Europese landen raden het aan:

de EU raadt hybride aan, zowel in de recente PQC roadmap (6), als de "Joint statement on PQC" getekend door 21 landen (7). Het Nederlandse PQC Handboek promoot hybride "voor bijna alle protocollen" (8) en Duitsland schrijft hybride verplicht voor (indien mogelijk), ook na de komst van de quantumcomputer (9).

De Verenigde Staten en het Verenigd Koninkrijk staan anders tegenover hybride. Amerikaanse regels staan hybride initieel toe, als tijdelijke maatregel, die later moet leiden tot een tweede transitie met alleen PQC (10), terwijl het Verenigd Koninkrijk noemt dat het soms wellicht nodig is, maar raadt aan het alleen te gebruiken als tijdelijke situatie, en binnen een raamwerk dat makkelijke migratie naar alleen PQC mogelijk maakt (11).

Migratiecomplicaties bij hybride cryptografie

De nieuwe PQC-algoritmes, gestandaardiseerd door het Amerikaanse NIST, zijn "pure" PQC-algoritmes. Om hybride mogelijk te maken wordt daarom doorgaans gekeken naar de plaatsen waar cryptografie gebruikt wordt, zoals cryptografische protocollen en certificaatstandaarden. Dit soort protocollen zijn echter niet ontworpen voor twee algoritmes; het verwacht maar één sleutel, sleuteluitwisseling, handtekening of verificatie. Ondersteuning van hybride kan door aanpassing van deze protocollen, om een tweede algoritme, sleutel et cetera te ondersteunen. Dit is echter geen eenvoudig proces en vereist aanpassingen in veel verschillende standaarden en protocollen. De aanpassing vereist niet alleen het ondersteunen van een tweede algoritme, maar ook aanpassing van validatie of versleutelingslogica. Dit geldt ook voor software en andere producten die cryptografie gebruiken.



Figuur 4: Versleuteling met hybride algoritme.

Een alternatieve manier voor hybride ondersteuning is om niet te focussen op aanpassing van de plek waar cryptografie gebruikt wordt, maar het creëren van een algoritme dat zelf al hybride is. Het lijkt op één enkel algoritme, met één publieke en geheime sleutel, één handtekening, et cetera, maar onder de motorkap worden er twee algoritmes uitgevoerd en veilig gecombineerd. Dit heeft als nadeel dat voor alle relevante combinaties een apart algoritme moet worden gedefinieerd. Voordelen zijn dat deze strategie geen extra aanpassingen vereist voor bestaande protocollen en software, behalve aanpassing aan nieuwe sleutel- en berichtgroottes, wat al moest voor pure PQC. Logica hoeft niet te worden aangepast. Ook voorkomt dit extra complexiteit voor ontwikkelaars: de keuze voor welke twee algoritmes - en hoe deze worden gecombineerd - wordt weggenomen: er is minder kans op misconfiguratie en bijbehorende beveiligingsrisico's.

Beide strategieën zijn voorgesteld in de aanpassing van PKI naar hybride quantumveilige cryptografie, en beide zijn getest in het HAPKIDO project.

PKI als fundament van cryptografische protocollen

Voor ad-hoc netwerken, zoals het internet, levert asymmetrische cryptografie - ook wel "publieke-sleutel" cryptografie genoemd - de functionaliteit om digitaal sleutels uit te wisselen. Welke vervolgens in symmetrische algoritmes wordt gebruikt om confidentialiteit en integriteit van berichten te garanderen of door middel van asymmetrische digitale handtekeningen wordt ingezet voor authenticiteit en onweerlegbaarheid.

Hierbij is het essentieel om zeker te weten dat een bepaalde, publieke sleutel hoort bij een bepaald persoon of bedrijf. Dit wordt vaak opgelost door middel van een certificaat: een certificaat koppelt een identiteit aan een publieke sleutel. Een certificaten autoriteit heeft de identiteit en het bezit van de sleutel gecontroleerd en het certificaat ondertekend om dit te bevestigen. De infrastructuur met bijbehorende rollen, processen en technische protocollen die dit mogelijk maakt is een PKI: Public Key Infrastructuur. Een PKI creëert vertrouwen in het eigenaarschap van cryptografische, publieke sleutels door middel van certificaten en door controles van de identiteit, doelbinding van sleutels, uitgifte van certificaten en revocatie.

Figuur 5: Vereenvoudigde weergave digitaal certificaat.

In een PKI wordt dus ook cryptografie toegepast: hashes en digitale handtekeningen in een certificaat en verschillende cryptografische technieken in ondersteunende PKI-protocollen voor aanvraag, uitgifte en revocatie.

HAPKIDO's ervaringen met hybride cryptografie in PKI

Certificaten ondersteunen traditioneel exact één publieke sleutel en één handtekening. PKI-protocollen verwachten eveneens enkelvoudige algoritmen. Hybride cryptografie past hier dus niet vanzelfsprekend in.

Er zijn momenteel verschillende hybride certificaatstandaarden voorgesteld. Sommige maken het mogelijk om een tweede sleutel en een tweede handtekening toe te voegen. Een andere maakt juist een hybride algoritme om binnen het bestaande sleutel- en handtekeningenveld van de certificaatstandaard te passen. De meeste, ondersteunende PKI-protocollen bieden nog geen ondersteuning voor hybride oplossingen.

Een complicatie in het kiezen voor de beste oplossing voor hybride algoritmes in PKI, is dat het ondersteunen van een tweede algoritme ook voor compatibiliteitsredenen ("backwards compatibility") wordt voorgesteld, niet alleen voor gelaagde beveiliging zoals verlangd in de EU.

Twee algoritmes voor compatibiliteit

Figuur 6: Visualisatie versleuteling met een optionele tweede algoritme.

Het ondersteunen van twee algoritmes in certificaten wordt niet alleen voorgesteld voor de hybride doeleinden die hier beschreven worden: namelijk de reductie van risico's. Er zijn ook voorstellen die een optionele tweede sleutel en handtekening beogen; een klassieke in de standaard velden en een PQC-algoritme in de nieuwe velden. De redenatie is dat dit ook werkt voor systemen die nog geen quantumveilige algoritmes aankunnen en dat die systemen dan - zodra ze er klaar voor zijn - over kunnen schakelen op het quantumveilige algoritme of een combinatie van beide. Voor deze types wordt soms ook de term hybride gebruikt - soms met de verduidelijking "of"-hybride ten opzichte van "en"-hybride.

Het is echter belangrijk deze goed te onderscheiden, omdat deze variant niet de tweelaagsbeveiliging biedt die we hier behandelen. Bij verwarring kan het zelfs leiden tot schijnveiligheid. Ook kan het optioneel aanbieden van een tweede algoritme ten koste gaan van zichtbaarheid in een cryptografische inventaris (wordt de tweede algoritme wel gebruikt?). Tenslotte, indien niet zorgvuldig geconfigureerd, kunnen optioneel-hybride certificaten ook leiden tot "downgrade" aanvallen, waarbij een aanvaller het gebruik van de minst veilige optie forceert. Naar de toekomst kijkende verwachten wij bovendien dat de noodzaak voor certificaten met dit soort compatibiliteit kleiner wordt, door de trend naar kortere levensduur van certificaten.

Binnen HAPKIDO is met beide varianten getest.

De hybride certificaat smaken

Samengevat liggen er nu drie opties op tafel voor hybride certificaten.

Figuur 7: Digitaal certificaat van type composiete sleutels en handtekening (gesimplificeerd).

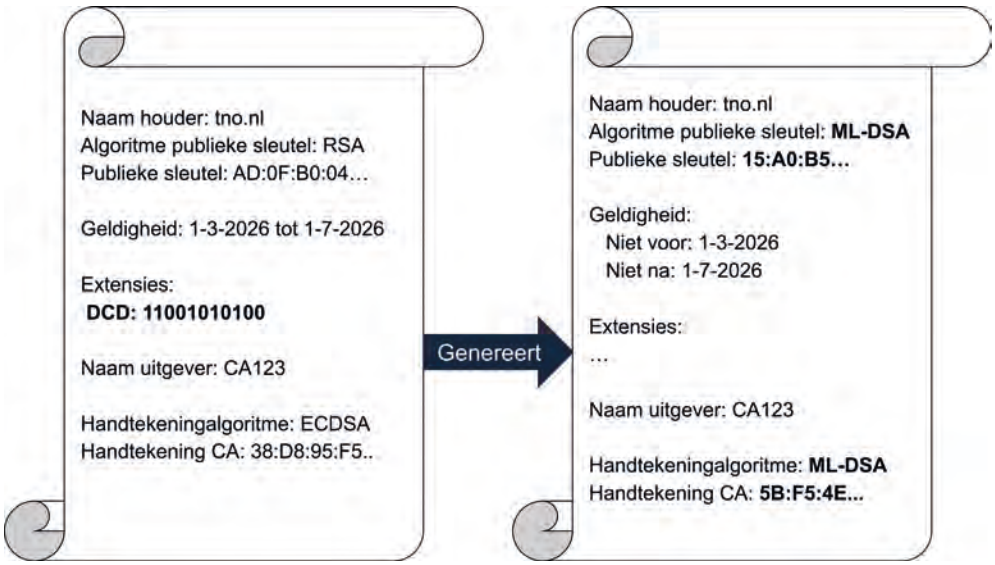
Hybride certificaten via een hybride algoritme
Voorstel naam: Composite
Oplossing: een samenstelling van de twee sleutels in het veld voor de sleutel, samenstelling van twee handtekeningen in het handtekening veld.
Doel: risicoreductie door middel van twee lagen beveiliging.
Status: standaarden zijn nog niet voltooid, maar boeken voortgang voor composite ML-KEM met een klassiek algoritme voor sleuteluitwisseling (12) en voor composite ML-DSA met een klassiek algoritme voor digitale handtekeningen (13).
Voordelen: past binnen bestaande X.509 standaard, geen extra keuzes voor gebruikers van certificaten (engineers, admins) en de manier van combineren ligt vast.
Nadelen: niet "backwards compatible": software moet het "nieuwe" algoritme kennen.

Hybride certificaten via certificaat extensies: Catalyst
Voorstelnaam: Catalyst of Chimera certificaat
Oplossing: tweede sleutel in een extensie binnen het certificaat
Doel: risicoreductie of compatibiliteit, afhankelijk van of de extensie verplicht is ("critical"). In de standaard raden ze aan om hem niet verplicht te maken.
Status: gestandaardiseerd. X.509 standaard ITU-T (14)
Nadeel: standaard bepaalt niet of het als optioneel of verplicht hybride moet worden gebruikt.

Figuur 8: Digitaal certificaat van type catalyst (gesimplificeerd) met tweede sleutel en handtekening in de extensies.

Bij een "critical" (verplichte) extensie
Voordelen: keuze, welke twee algoritmes gecombineerd worden, ligt bij de gebruiker.
Nadelen: niet compatibel met systemen die geen PQC ondersteunen. Verantwoordelijkheid van het veilig combineren van de twee algoritmes ligt bij de software of ontwikkelaar die het certificaat gebruikt, wat de kans op verkeerd gebruikt vergroot.

Bij een "non-critical" (niet verplichte) extensie
Voordelen: compatibiliteit met systemen die nog geen PQC ondersteunen, deze kunnen de extensie negeren. Kan gebruikt worden om over te gaan naar pure of hybride PQC zonder nieuwe certificaataanvraag.
Nadelen: verantwoordelijkheid van het veilig combineren, als ze worden gecombineerd, ligt bij de software of ontwikkelaar die het certificaat gebruikt. Gebruik van het tweede algoritme is niet verplicht: er is dus geen risicoreductie, waarbij dit niet het type hybride is die bijvoorbeeld de EU aanraad. Het past wel bij de Engelse en Amerikaanse aanpak. Verminderde zichtbaarheid van gebruik van PQC: het is moeilijk om te bepalen of een systeem met dit soort certificaat wel of niet quantumveilig is.



Figuur 9: Digitaal certificaat van type chameleon (gesimplificeerd), waarbij vanuit een extensie een PQC-certificaat gegenereerd kan worden.

Hybride certificaten via certificaatextensies: Chameleon
Voorstelnaam: Chameleon (of Delta) certificaat.
Oplossing: hybride via een niet verplichte certificaatextensie, ditmaal is een volledig tweede certificaat geëncodeerd in een extensie. Bij ontbrekende PQC ondersteuning wordt de extensie genegeerd.
Doel: compatibiliteit: optionele hybride
Status: draft, nog niet opgepakt voor standaardisatie.
Voordelen: compatibiliteit, verificatie en creatie is eenvoudiger dan bij catalyst.
Nadelen: gelijk aan de nadelen van catalyst.

Conclusies

Figuur 10: Vereenvoudigde weergave van vijf certificaat types

Hybride cryptografie wordt in Nederland en Europa aangeraden om het restrisico van nieuwe PQC-algoritmes te verkleinen: de combinatie van traditionele en nieuw algoritmes biedt zowel traditionele en quantumveiligheid. Er zijn twee strategieën om hybride te implementeren: als een nieuw hybride algoritme of door middel van aanpassing van protocollen, die cryptografie gebruiken.

Voor PKI zien we daarnaast dat het ondersteunen van twee algoritmes ook voor compatibiliteitsredenen wordt voorgesteld, vaak ook hybride genoemd. Deze verschillende voorstellen, met verschillende doelen, maakt de discussie ingewikkelder.

PKI ondersteunt hybride cryptografie nog niet volledig: nieuwe certificaatstandaarden worden nu voltooid, de ondersteunende PKI-protocollen moeten nog deels worden aangepast.

Duidelijkere terminologie zou de discussie rondom dit onderwerp verbeteren: denk aan tweelaagshybride en optionele-hybride

De discussie hierbij over welke variant gebruikt moet worden is nog niet volledig beklonken. De urgentie om PKI te migreren, omdat veel systemen ervan afhankelijk zijn, vereist een spoedige keuze.

Aanbevelingen

Duidelijkere terminologie zou de discussie rondom dit onderwerp verbeteren: denk aan tweelaagshybride en optionele-hybride.

In het algemeen zijn de argumenten voor hybride algoritmes doorslaggevend: er is geen twijfel over of en hoe algoritmes gecombineerd worden, complexiteit wordt weggehaald voor engineers, en cryptografische protocollen hoeven niet of minder worden aangepast.

Kijkend naar PKI is, vanuit Nederlands en EU perspectief, de composite certificaat oplossing de best passende. Ons advies is, gericht op de cryptografische gemeenschap, om deze te promoten, te standaardiseren en te starten met het aanpassen van ondersteunende PKI-protocollen, zodat deze ook hybride algoritmes gebruiken. Gegeven de verschillen in aanbevelingen tussen de EU en de VS/VK, is het logisch als het initiatief hiervoor vanuit Europa komt.

Voor PKI-beheerders raden we aan te gaan samenwerken met domein- en ketenpartners om te gaan experimenteren met (Hybride) PQC. Voor overige informatie over andere aspecten van PKI-migratie verwijzen we naar het HAPKIDO PKI handboek, dat binnenkort verschijnt.

Referenties

(1) Feynman, R. P. (1986). Quantum mechanical computers. Foundations of physics, 16(6), 507-531.

(2) Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). IEEE.

(3) Hoogstraaten, H., Prins, R., Niggebrugge, D., Heppener, D., Groenewegen, F., Wettinck, J., Strooy, K., Arends, P., Pols, P., Kouprie, R., Moorrees, S., Pelt van, Hu, Y.Z.. (2012). Black Tulip: Report of the investigation into the DigiNotar Certificate Authority breach. 10.13140/2.1.2456.7364.

(4) https://csrc.nist.gov/projects/post-quantum-cryptography

(5) Fehr, S., Huang, Y. H., & Amadori, A. (2023). HAPKIDO Project Report D5. 2. Literature Review: (Quantum-Safe) Cryptographic Combiners and Hybrid Security https://hapkido.tno.nl/publish/pages/4234/hapkido_d5-2.pdf.

(6) https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography

(7) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/-Crypto/PQC-joint-statement-2025.pdf?__blob=publicationFile&v=3

(8) https://publications.tno.nl/publication/34643387/XTdELY16/TNO-2024-pqc-ne.pdf

(9) https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Quantentechnologien-und-Post-Quanten-Kryptografie/quantentechnologien-und-post-quanten-kryptografie_node.html

(10) https://csrc.nist.gov/pubs/ir/8547/ipd

(11) https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography#section_5

(12) https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-kem/

(13) https://datatracker.ietf.org/doc/draft-ietf-lamps-pq-composite-sigs/

(14) https://www.itu.int/rec/T-REC-X.509-201910-I

STRENGERE EISEN OP KOMST DOOR DE NIS2-RICHTLIJN.

De NIS2-richtlijn zorgt voor strengere beveiligingseisen aan uw cybersecurity. Niet alleen technisch, maar ook bestuurlijk. NIS2 legt de zorgplicht voor keten- en leveranciersrisico's bij uw organisatie. Onvoldoende beveiliging in de keten kan directe gevolgen hebben voor omzet, reputatie en klantvertrouwen.

Door de overname van de Security Academy in 2025 bundelt DNV diepgaande cybersecurityexpertise met jarenlange ervaring in risicobeheersing en business continuity. Onze praktijkgerichte trainingen brengen alle NIS2-verplichtingen samen.

Bereid uw organisatie voor op de komst van de NIS2-richtlijn, bezoek **dnv.nl/nis2**

Training	Locatie	Duur
NIS2 Boardroomsessie	Woerden of eigen locatie	4 uur
NIS2 Certified Professional	Woerden of online	2 dagen
Lead Auditor ISO/IEC 27001	Verschillende locaties	5 dagen
Crisis Management Foundation	Woerden of online	2 dagen

SECURITY ACADEMY
a DNV company