INFORMATIEBEVEILIGING
MAGAZINE



DOSSIERS

- Onderzoek & rapportage: het Rijk in de Cloud
- Analyse van hacks: determinisme versus kansberekening
- Organisatie fitheid

JAARGANG 26 - 2026 - EDITIE 4

Hoe stuur jij op security in de board room?

Kijk op **cisomasterclass.nl** om uit te vinden hoe je daar grip op krijgt en schrijf je in voor de masterclass op 28, 29 en 30 september 2026.

Kennis brengt je naar de top, skills zetten je aan het stuur!



CISO masterclass

www.cisomasterclass.nl info@cisomasterclass.nl 079-360 4268

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

creative commons

Tenzij anders vermeld valt de inhoud van dit tijdschrift onder een Creative Commons Naamsvermelding-gelijkeDelen 3.0 Nederland Licentie (CC BY-SA 3.0)

ISSN 1569-1063

Uitdagend!



Chris de Vries

Wij Nederlanders komen voort uit een natie van zeevaarders, maar langzamerhand zijn veel maritieme zegswijzen vergeten zo niet verloren gegaan. En zo bracht het artikel van Robert Blokker mij het essayboek: "Herzien Bestek" van C.J.E. Dinaux (ISBN 90 254 6357 6 / 1974) in herinnering. Als tiener las ik graag literatuur en nog steeds geldt dat.

Het artikel van Robert is een uitdaging en een proeve van bekwaamheid om ons huidig bestek te herzien. Wat was ook alweer bestek? Dat kan zijn:

1. het exact vastleggen wat een aannemer (van huis of schip) moet bouwen, hoe dat gebeurt en onder welke voorwaarden en/of

2. plaatsbepaling en loden op zee.

Het oogmerk is in ieder geval dat men niet van koers afraakt en daar aankomt waar men wil aankomen. En dat vereist regelmatig verifiëren van de actualiteit (weer & wind) en dus een kort bestek bijhouden (gevolg: koersaanpassing).

Robert doet dat met abstractie, natuur- & behoudswetten, wiskunde, ijk-symmetrie en diverse andere begrippen waarbij hij een deterministische aanpak adviseert boven een benadering gebaseerd op kansberekening. Raad niet naar de intentie van de 'hacker', maar zoek die, gebaseerd op terug te vinden sporen. Vandaar de titel van zijn artikel: "De aanvaller verraadt zichzelf".

Het is geen gemakkelijk artikel; regelmatig moet teruggegrepen worden op vergeten kennis van de middelbare school en is herlezen nodig om zeker te zijn dat het gelezene begrepen is. Al sinds onze eerste uitgave ziet InformatieBeveiliging Magazine als één van haar doelen, dat de lezer uit zijn comfortzone komt en over de grenzen van ons specialistisch vak. Niet vaak, maar bij tijd en wijle!

Verder is er een lezenswaardig artikel van Xander Bordeaux & Ruud Wissenburg vanuit de Algemene Rekenkamer ingaande op het nieuwe beleid van "Het Rijk in de cloud". Maarten Albregts gaat in op: "De onzichtbare aanval op onze vertrouwde SaaS-workflows" en schrijft Reza Razai over de fitheid van onze organisatie in relatie met de fitheid van de CISO of FG.

Ronald Eygendaal heeft het in zijn lezenswaardig blog over leeftijdsverificatie op sociale media en spreekt daarbij onze verantwoordelijkheid als ouders & opvoeders aan, terwijl onze voormalige Hoofdredacteur Nicole van Deursen enthousiast ingaat op het boek "From heatmaps to histograms", een aanrader dus.

De titel van dit voorwoord is "Uitdagend", de betekenis: demonstratief, provocerend, tergend of tartend dan wel: verleidelijk, stout, prikkelend en sexy. Naast begrippen als: fier, zelfbewust, prikkelend en stimulerend zal dit magazine van alles wat hebben en daardoor vertrouwen wij erop dat het een magazine is vol van 'tips & tricks', die onze mentale en fysieke fitheid aanspreekt.

Chris

Rectificatie IB.3-2026 *In aansluiting op het artikel van Jolanda ter Maten inzake: "De firewall die we vergeten te bouwen. Over leiderschap, mensen en de blinde vlek in informatiebeveiliging " (IB.3- 2026 pagina 28 t/m 31) hebben wij geconstateerd dat er een typefout is gemaakt in de auteursgegevens. Het juiste e-mailadres van de auteur is als volgt: info@jolandatermaten.com*

IN DIT NUMMER

03 Voorwoord en inhoudsopgave
04 Het Rijk in de cloud: digitale soevereiniteit onder druk
11 Vogelvrijverklaarde
12 "Ik vaar blind op mijn CISO!" : en vier andere overtuigingen die de digitale weerbaarheid niet vooruithelpen
16 De onzichtbare aanval op onze vertrouwde SaaS-workflows
22 De aanvaller verraadt zichzelf. Waarom we de intentie kunnen lezen, niet raden.
29 De ontwikkeling van authenticatie: van wachtwoorden naar passkeys
30 Een organisatie wordt nooit fitter dan de experts die haar bewaken
34 Leeftijdsverificatie op sociale media platforms = onzin
35 In korte broek naar digitale onafhankelijkheid
36 Boekreview: From Heatmaps to Histograms

Auteur: Xander Bordeaux en Ruud Wissenburg zijn IT-onderzoekers bij de Algemene Rekenkamer. Zij zijn bereikbaar via voorlichting@rekenkamer.nl

De Algemene Rekenkamer onderzoekt of de rijksoverheid publiek geld zinnig, zuinig en zorgvuldig uitgeeft. Onze wettelijke taak is het controleren van de inkomsten en uitgaven van het Rijk en hierover rapporteren wij één keer per jaar aan het parlement op Verantwoordingsdag (derde woensdag in mei). Op basis van ons oordeel kan het parlement besluiten of hij decharge verleent aan het kabinet. Daarnaast rapporteren we afzonderlijke onderzoeken aan het parlement zodat Kamerleden kunnen bepalen of het beleid van een minister doeltreffend is. Voor meer informatie: www.rekenkamer.nl en bekijk ons dashboard Doelen & Resultaten op blikopnederland.rekenkamer.nl

Het Rijk in de cloud

Digitale soevereiniteit onder druk



Dit artikel is gebaseerd op het onderzoek Het Rijk in de cloud – Donkere wolken pakken samen, uitgevoerd door de Algemene Rekenkamer over het cloudgebruik bij de rijksoverheid. De onderzoeksresultaten zijn in 2025 gepubliceerd waarbij de nadruk ligt op kansen, risico's en – bij de toetsing – op de bevindingen rond digitale soevereiniteit, continuïteit en gegevensbescherming. De auteurs van dit artikel hebben beiden aan dit onderzoek meegewerkt.

Cloud als strategische keuze, niet slechts een technische

De migratie van applicaties van de rijksoverheid naar de cloud is geen IT-project, maar een strategische herpositionering van: digitale macht, afhankelijkheden en verantwoordelijkheden. Het rapport Het Rijk in de cloud – Donkere wolken pakken samen (1) beschrijft hoe de rijksoverheid in relatief korte tijd grootschalig gebruik is gaan maken van public cloud-diensten, terwijl de governance, risicobeheersing en strategische sturing daar niet in gelijke mate in zijn meegegroeid.

Voor wie zich bezighoudt met informatiebeveiliging en digitale weerbaarheid is dit rapport bijzonder relevant. Het legt bloot dat cloudgebruik niet alleen draait om kosten, innovatie en efficiëntie, maar vooral om fundamentele vragen rond soevereiniteit, controle, continuïteit en bescherming van publieke waarden. Vragen die niet alleen bij (public) cloud gesteld moeten worden maar eigenlijk bij (overheids)uitbesteding in het algemeen.

Het onderzoek richt zich op de praktische invulling van het rijksbrede cloudbeleid (herzien in 2022) en specifiek op de mate waarin ministeries zicht hebben op hun cloudgebruik en bijkomende risico's. Daarnaast zijn in het onderzoek drie belangrijke public cloud contracten onderzocht op de borging van drie kernprincipes: digitale soevereiniteit, continuïteit van dienstverlening en gegevensbescherming.

De conclusies zijn zorgwekkend: de rijksoverheid heeft beperkt zicht op zijn cloudgebruik, maakt onvoldoende strategische risicoafwegingen en waarborgt in het drietal onderzochte contracten de kernprincipes onvoldoende.

Vanuit beveiligingsperspectief is vooral de bevinding rond soevereiniteit fundamenteel: het Rijk heeft zich afhankelijk gemaakt van een beperkt aantal, grotendeels Amerikaanse hyperscalers, zonder altijd helder te hebben welke structurele risico's dit meebrengt. Voor velen was dit wellicht niet een verrassende uitkomst. Echter, het onderzoek heeft wel mede de maatschappelijke discussie aangejaagd en voor grotere politieke interesse gezorgd. Interesse die zich niet meer beperkte tot de technische maar vooral ging over de strategische afwegingen.

De context: waarom dit onderzoek noodzakelijk was

De cloud push

In ons onderzoek beschrijven wij hoe IT-ontwikkelingen de rijksoverheid richting cloud duwen. Leveranciers bieden hun producten steeds vaker uitsluitend als cloudoplossing aan. Microsoft 365 is daarvan het meest duidelijke voorbeeld: klassieke on-premise versies verdwijnen of worden niet langer doorontwikkeld met nieuwe functionaliteit. Voor ministeries ontstaat hierdoor een praktisch dilemma: vasthouden aan verouderende systemen zonder innovatie of meegaan in cloudmigratie met nieuwe afhankelijkheden.
Vanuit beveiligingsoptiek is dit geen neutrale beweging. De keuze voor cloud is in veel gevallen geen vrije strategische afweging, maar een reactie op marktdynamiek. De onderhandelingspositie van individuele ministeries is daarmee per definitie beperkt.

Beleidsontwikkeling en onderzoeksaanpak

Tot 2022 was public cloud binnen de rijksoverheid niet toegestaan. Toch hadden verschillende ministeries al eigen beleid ontwikkeld waarin public cloud onder voorwaarden werd geaccepteerd. De behoefte was urgent en de druk vanuit leveranciers groot. In 2022 werd het rijksbrede cloudbeleid herzien: public cloud werd toegestaan, mits onder strikte voorwaarden en niet voor zeer vertrouwelijke informatie. In het onderzoek van de Algemene Rekenkamer hebben wij twee voorwaarden uit het beleid getoetst; ministeries moeten zicht hebben op hun eigen cloudgebruik en er moeten risicoafwegingen zijn gemaakt.

Daarna hebben wij uit de inventarisatie van het cloudgebruik drie belangrijke cloudcontracten onderzocht op maatregelen die risico's beheersen op het gebied van: soevereiniteit, continuïteit en gegevensbescherming.

De vraag in het onderzoek was eenvoudig maar fundamenteel: "Wordt aan de geselecteerde voorwaarden voldaan en worden de drie onderzochte risico's voldoende afgedekt?" De bevindingen moesten het cloudgebruik demystificeren en met de praktijkervaring input geven voor een herziene versie van het overheidsbeleid dat in 2025 stond gepland.

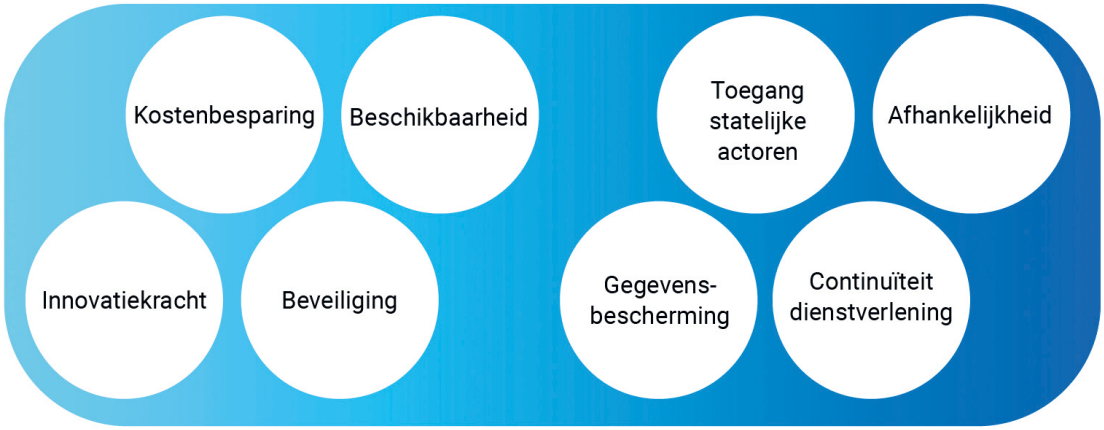
Kansen van cloud: realiteit en relativering

In het onderzoek wilden we niet alleen de risico's benoemen maar ook ingaan op kansen bij cloudgebruik. Vanuit een securityperspectief verdienen deze kansen echter enige nuance.

Kostenbesparing en schaalbaarheid

Cloudtechnologie maakt elasticiteit mogelijk: in theorie kan capaciteit eenvoudig naar behoefte worden opgeschaald of afgeschaald. Dit voorkomt investeringen in ongebruikte

Kansen en risico's van cloud; afhankelijk van de wens en cloudvorm kunnen kansen risico's zijn en vice versa



hardware. Maar de praktijk is complexer:

- licentiemodellen zijn vaak ingewikkeld;
- pay-per-use kan bij verkeerd gebruik tot kostenexplosies leiden;
- cloudtransformatie vereist nieuwe expertise en governance;
- schaalbaarheid is sterk afhankelijk van de mogelijkheden die de applicatie architectuur en infrastructuur biedt (pas bij cloud-native goed mogelijk).

Zonder volwassen cloudontwikkelomgeving en configuratiebeheer is kostenbesparing geen vanzelfsprekendheid.

Beschikbaarheid en redundantie

De grote cloudproviders bieden hoge beschikbaarheidseisen en een geografisch verspreide infrastructuur aan. Vanuit continuïteitsperspectief is dit enorm aantrekkelijk. De drie grootste cloudproviders (hyperscalers) zijn Amerikaanse bedrijven die zo'n 65% van de wereldwijde cloudmarkt bezitten. Door het gebruik van hyperscalers worden echter nieuwe risico's geïntroduceerd:

- concentratie van overheidsdata bij slechts enkele aanbieders;
- systeemrisico's bij grootschalige verstoringen;
- geopolitieke afhankelijkheden.

Beschikbaarheid op microniveau (per applicatie) kan toenemen, terwijl risico's op macroniveau groeien.

Beveiliging en expertise

Hyperscalers investeren miljarden in cybersecurity. Zij beschikken over gespecialiseerde teams, geavanceerde monitoring en snelle patching. Voor veel ministeries overstijgt deze capaciteit de eigen mogelijkheden. Dat is een reëel voordeel. Maar er is een belangrijke paradox: hoe groter de concentratie van gevoelige data, hoe aantrekkelijker het doelwit. Een succesvolle aanval op een hyperscaler of een misconfiguratie in een gedeeld platform kan enorme impact hebben. Security op schaal vergroot ook de impact van falen op schaal. Dit heeft in de praktijk ook al geleid tot grote incidenten, dus is ook een realistisch risico.

Innovatiekracht

Cloud is de basis voor AI, data-analyse en moderne digitale dienstverlening. Zonder cloud dreigt technologische achterstand. Toch rijst de vraag: mag innovatie afhankelijk worden van niet-Europese technologiebedrijven die onder buitenlandse wetgeving vallen? Hier raakt innovatie direct aan soevereiniteit.

De kern: digitale soevereiniteit – meer dan datalocatie

Het rapport heeft digitale soevereiniteit gedefinieerd als het vermogen om autonoom te beslissen en handelen over essentiële digitale aspecten van economie, maatschappij en democratie. Dit begrip is in het onderzoek geconcretiseerd in normen over:

- inzicht in datalocatie;
- afspraken over overdracht buiten de EER;
- right-to-audit;
- interoperabiliteit;
- portabiliteit en exitstrategie.

Het publieke debat versmalt soevereiniteit vaak tot "data in Europa". Het rapport laat zien dat dit te simplistisch is. Estland en Oekraïne kozen er bewust voor om overheidsdata buiten hun eigen grondgebied op te slaan om bij oorlog staatscontinuïteit

te waarborgen. Soevereiniteit kan dus ook betekenen: spreiding van afhankelijkheden. De kernvraag is niet waar data fysiek staat, maar:

- wie kan toegang afdwingen?
- wie bepaalt de spelregels, welke wetgeving is van toepassing?
- kan de overheid overstappen?
- kan zij audits uitvoeren en onafhankelijk afspraken laten toetsen?

Het gaat dus niet alleen om fysieke locatie, maar ook om controleerbaarheid en handelingsvermogen.

Amerikaanse wetgeving: het structurele spanningsveld

Cruciale onderdelen van het soevereiniteitsvraagstuk zijn de Amerikaanse CLOUD Act en de FISA Sectie 702. Amerikaanse autoriteiten kunnen op basis van deze wetten data opvragen bij Amerikaanse cloudproviders, ook wanneer deze data in Europa is opgeslagen. Historisch zijn meerdere afspraken tussen de VS en Europa zoals Safe Harbor en het Privacy Shield door het Europese Hof nietig verklaard. Het huidige EU-US Data Privacy Framework moet nog zijn robuustheid bewijzen onder president Trump.
In de praktijk zouden dergelijke verzoeken vanuit de VS zelden zijn gedaan. Maar juridisch is de mogelijkheid aanwezig. Experts bevestigen dit beeld. Het risico is dus niet verwaarloosbaar of afwezig. Te meer omdat de Amerikaanse inlichtingendiensten volgens FISA helemaal geen gerechtelijk bevel meer nodig hebben om inzage in de data te krijgen. Voor staatsgevoelige data is het formele risico zeer relevant, ongeacht de frequentie.

De toetsing: harde cijfers en zorgelijke patronen

Ons onderzoek maakt zichtbaar hoe het cloudgebruik binnen de rijksoverheid zich in de praktijk heeft ontwikkeld. Cloud wordt inmiddels breed toegepast, maar tegelijkertijd zien we dat de governance rond cloudgebruik nog onvolwassen is. Vooral het ontbreken van overzicht, uniforme definities en structurele risicoafwegingen zijn aandachtspunten.

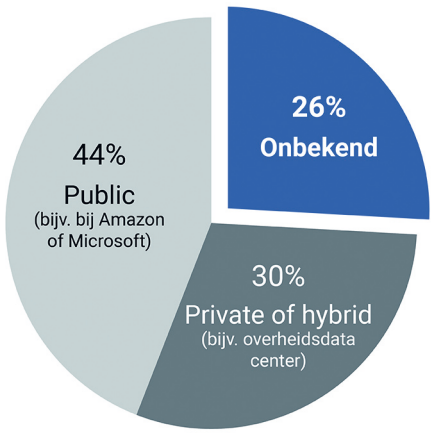
Gebrekkig overzicht

Uit het onderzoek blijkt dat de rijksoverheid in totaal 1.588 clouddiensten in zicht heeft. Deze zijn als volgt verdeeld:

- 700 public cloud-diensten (44%);
- 477 private of hybride cloud-diensten (30%);
- 411 diensten waarvan het type cloud onbekend is (26%).

Voor effectief risicomanagement is een dergelijk overzicht essentieel. Zonder inzicht in gebruikte diensten, leveranciers en dataopslaglocaties is het moeilijk om te sturen op compliance, beveiliging en continuïteit.

Bij een kwart van gerapporteerde clouddiensten is de vorm onbekend



Vanuit het perspectief van digitale soevereiniteit heeft dit directe consequenties. Wanneer niet duidelijk is in welke cloudomgeving data wordt verwerkt, is ook niet altijd bekend:

- waar de data fysiek is opgeslagen;
- welke wetgeving van toepassing kan zijn;
- en welke partijen potentieel toegang hebben tot de gegevens.

Dit maakt cloudgebruik niet alleen een technisch vraagstuk, maar vooral een governancevraagstuk.

Materieel public cloud: geen uniforme definitie

Van de 700 public clouddiensten zijn 126 diensten aangemerkt als 'materieel'. Dit zijn cloudtoepassingen die essentieel zijn voor de uitvoering van primaire overheidstaken, zoals belastinginning, communicatie met burgers of vitale informatievoorziening.
Ministeries hanteren verschillende definities voor het begrip 'materieel'. Sommige ministeries baseren dit uitsluitend op het belang voor primaire processen, terwijl andere aanvullende criteria gebruiken, zoals gevoeligheid van data of maatschappelijke impact bij uitval.
Het gevolg is een inconsistente classificatie van kritieke clouddiensten. Dit heeft meerdere gevolgen:

- risico's kunnen verschillend worden beoordeeld;
- rapportages tussen ministeries zijn moeilijk vergelijkbaar;
- centrale sturing op rijksniveau wordt bemoeilijkt.

Omdat het rijksbrede cloudbeleid vooral betrekking heeft op materieel public cloud-gebruik, leidt deze variatie in definities ertoe dat risico's niet altijd op dezelfde manier worden herkend of beheerst. Voor digitale soevereiniteit betekent dit dat de beoordeling van strategische afhankelijkheden en risico's versnipperd plaatsvindt.

Onvoldoende risicoafweging

Een opvallende bevinding uit het onderzoek betreft de wijze waarop risicoafwegingen plaatsvinden bij cloudgebruik.
Van de 126 materiële public cloud-diensten blijkt bij 84 diensten (67%) geen voorafgaande risicoafweging te zijn gemaakt. Met andere woorden: bij ongeveer twee derde van de kritieke cloudtoepassingen ontbreekt een gestructureerde analyse van de bijbehorende risico's. Een dergelijke risicoafweging zou minimaal moeten ingaan op drie kernprincipes die volgens de Rekenkamer centraal staan bij cloudgebruik door de overheid:

- digitale soevereiniteit – controle over data en systemen;
- continuïteit van dienstverlening – het vermogen om publieke diensten te blijven leveren;
- gegevensbescherming – het beschermen van vertrouwelijke gegevens van burgers en bedrijven.

Wanneer deze afweging niet expliciet plaatsvindt, blijven potentiële risico's buiten beeld en worden mitigerende maatregelen mogelijk niet genomen. Dit kan leiden tot situaties waarin:

- afhankelijkheden van leveranciers onvoldoende worden beheerst;
- continuïteitsrisico's niet zijn onderkend;
- of gevoelige gegevens onvoldoende beschermd zijn.

Contracttoetsing: waar soevereiniteit concreet wordt

Naast de kwantitatieve analyse van cloudgebruik zijn drie materiële public-cloudtoepassingen nader onderzocht.

Beperkte grip op contractuele afspraken

Een belangrijk aandachtspunt uit het onderzoek is de complexiteit van de contractuele structuur rond cloudleveranciers. Contractuele afspraken blijken vaak verspreid te zijn over meerdere documenten, zoals hoofdovereenkomsten, service-level agreements, aanvullende voorwaarden en technische bijlagen.
Daarbij spelen vaak verschillende partijen een rol, waaronder:

- primaire cloudleveranciers;
- integratie- of serviceproviders;
- en onderaannemers binnen de bredere leverancierskeketen.

Deze gelaagde structuur maakt het lastig om volledig overzicht te houden van alle contractuele verplichtingen en verantwoordelijkheden. Wij constateren dat hierdoor in de praktijk:

- niet altijd een volledig overzicht bestaat van contractuele afspraken;
- kennis over specifieke contractbepalingen beperkt kan zijn binnen ministeries;
- inzicht in de volledige leverancierskeketen niet altijd aanwezig is.

Voor digitale soevereiniteit is dit een belangrijk punt. Formeel kan controle over data, systemen en processen contractueel zijn vastgelegd, maar wanneer de contractstructuur complex en gefragmenteerd is, wordt praktische controle aanzienlijk moeilijker.

Exitstrategieën en afhankelijkheden

Een tweede belangrijk aandachtspunt betreft de mogelijkheid om van cloudleverancier te wisselen. In theorie vormt portabiliteit – het kunnen migreren van data en systemen – een belangrijk onderdeel van cloudcontracten. In de praktijk blijkt dit echter complex. Bij langdurig gebruik van specifieke cloudplatformen kunnen organisaties afhankelijk worden van de technologie en diensten van één leverancier.
Deze afhankelijkheid kan verschillende oorzaken hebben:

- integratie van cloudservices in bedrijfsprocessen;
- gebruik van leveranciersspecifieke functionaliteiten;
- technische en organisatorische migratiekosten.

Hierdoor ontstaat een situatie waarin overstappen naar een andere leverancier wel mogelijk is, maar in de praktijk ingrijpend, kostbaar en risicovol kan zijn. Voor digitale soevereiniteit betekent dit dat contractueel vastgelegde exit-mogelijkheden niet automatisch leiden tot feitelijke soevereiniteit. Zonder realistische migratiescenario's kan een exit-strategie vooral theoretisch van aard blijven.

Gegevensbescherming

Ook de bescherming van persoonsgegevens en andere gevoelige informatie vormt een belangrijk aandachtspunt bij cloudgebruik.
Wanneer meerdere partijen betrokken zijn bij de verwerking van gegevens, kan het lastig zijn om volledig inzicht te krijgen in:

- waar gegevens precies worden verwerkt;
- welke partijen toegang hebben;
- en hoe controle op naleving van afspraken plaatsvindt.

Voor organisaties die met gevoelige overheidsdata werken, betekent dit dat transparantie binnen de leverancierskeketen cruciaal is. Zonder voldoende inzicht in deze keten wordt het moeilijk om aantoonbaar te voldoen aan eisen rond gegevensbescherming, beveiliging en compliance.

Strategisch leveranciersmanagement: gemiste kans

De rijksoverheid behoort tot de grootste IT-afnemers van Nederland. Vanuit dat perspectief zou zij in principe over een aanzienlijke onderhandelingspositie moeten beschikken tegenover grote cloudleveranciers. Het onderzoek laat echter zien dat deze potentiële schaalvoordelen in de praktijk slechts beperkt worden benut. Cloudinkoop en contractbeheer vinden grotendeels plaats binnen afzonderlijke ministeries of uitvoeringsorganisaties. Hoewel er rijksbrede kaders bestaan voor cloudge-

bruik, is de toepassing ervan niet altijd uniform. Hierdoor ontstaat een situatie waarin verschillende onderdelen van het Rijk vergelijkbare diensten afnemen, maar niet altijd gezamenlijk optrekken richting leveranciers. Deze versnippering heeft directe gevolgen voor de strategische positie van de overheid in een markt die wordt gekenmerkt door sterke concentratie van aanbieders. Juist in een dergelijke marktsituatie is strategisch leveranciersmanagement op rijksniveau van belang. Gezamenlijke inkoop en gecoördineerde contractonderhandelingen kunnen helpen om sterker te sturen op voorwaarden rond bijvoorbeeld:

- audit- en controlemechanismen;
- locatie en bescherming van data;
- mogelijkheden voor migratie of beëindiging van diensten;
- juridische waarborgen rond toegang tot gegevens.

Effectief leveranciersmanagement vraagt niet alleen om technische en juridische expertise, maar ook om rijksbrede regie en coördinatie.

Cloud in geopolitiek perspectief: een structureel dilemma

Digitale infrastructuur is niet langer uitsluitend een technologische of economische kwestie, maar raakt in toenemende mate aan vraagstukken van soevereiniteit en nationale veiligheid. De internationale cloudmarkt wordt gedomineerd door een beperkt aantal grote technologiebedrijven. Veel van deze aanbieders zijn gevestigd buiten Europa. Voor overheden die in toenemende mate afhankelijk zijn van cloudplatformen voor hun digitale dienstverlening, betekent dit dat technologische keuzes ook geopolitieke implicaties kunnen hebben. Daarbij gaat het onder meer om:

- juridische afhankelijkheid, bijvoorbeeld door de mogelijke werking van buitenlandse wetgeving;
- politieke kwetsbaarheid, wanneer geopolitieke spanningen invloed hebben op toegang tot technologie of dienstverlening;
- strategische blootstelling, doordat vitale digitale infrastructuur buiten directe nationale invloedssfeer kan vallen.

Dergelijke afhankelijkheden zijn niet per definitie problematisch, maar moeten wel expliciet onderdeel zijn van de risicoafweging bij cloudgebruik.

Aanbevelingen: richting versterkte digitale soevereiniteit

In het rapport doen we aanbevelingen om de governance rond cloudgebruik binnen de rijksoverheid te versterken. De kern van deze aanbevelingen ligt niet zozeer in het beperken van cloudgebruik, maar in het professionaliseren van de besluitvorming, het toezicht en het leveranciersmanagement rondom cloudtoepassingen.

Uniformeer, concretiseer en handhaaf rijksbreed cloudbeleid
Een eerste aandachtspunt betreft het rijksbrede cloudbeleid. Hoewel er beleidskaders bestaan, blijken deze in de praktijk verschillend te worden geïnterpreteerd en toegepast door ministeries en uitvoeringsorganisaties. De Algemene Rekenkamer adviseert daarom om het beleid verder te uniformeren en te concretiseren, zodat duidelijker wordt welke eisen gelden bij het gebruik van cloudtechnologie.

Daarnaast pleiten we voor het structureel verplicht stellen van risicoafwegingen bij de inzet van cloudoplossingen. De eerder gesignaleerde lacunes – waarbij bij een aanzienlijk deel van de materiële public-clouddiensten geen expliciete risicoanalyse heeft plaatsgevonden – maken duidelijk dat een systematische benadering noodzakelijk is. Risicoafwegingen zouden daarbij niet alleen technische en operationele aspecten moeten omvatten, maar ook vraagstukken rond afhankelijkheden, gegevensbescherming en digitale soevereiniteit.

Ook de rol van de rijksoverheids CIO, de CIO-Rijk komt nadrukkelijk naar voren in de aanbevelingen. Volgens de Rekenkamer kan de centrale regiefunctie worden versterkt door duidelijkere kaders te stellen, de naleving van beleid beter te monitoren en waar nodig actief bij te sturen. Daarmee kan CIO-Rijk een belangrijkere rol spelen in het bewaken van rijksbrede belangen bij cloudgebruik.

Ga meer gezamenlijk optrekken om expertise te bundelen en sterker te staan
Verder wijzen we op het belang van gezamenlijke inkoop en contractbeheer. Door als rijksoverheid-CIO collectief op te treden richting cloudleveranciers kan de onderhandelingspositie worden versterkt en kunnen afspraken over bijvoorbeeld auditrechten, gegevensbescherming en migratiemogelijkheden beter worden geborgd.

Onderzoek nadrukkelijker alternatieve cloudleveranciers
In datzelfde kader adviseren we om nadrukkelijker te kijken naar Europese alternatieven en initiatieven die digitale soevereiniteit kunnen versterken. Hoewel dergelijke alternatieven momenteel nog niet altijd dezelfde schaal of functionaliteit bieden als de grote internationale cloudplatformen, kan strategische ondersteuning van Europese initiatieven bijdragen aan een meer evenwichtige markt.

Tot slot benadrukken we het belang van realistische exit-strategieën. De mogelijkheid om van leverancier te wisselen of cloudgebruik te beëindigen vormt een essentieel onderdeel van digitale soevereiniteit. In de praktijk blijkt echter dat dergelijke strategieën vaak onvoldoende zijn uitgewerkt of getest.

Wat CIO-Rijk, ministeries en SSO's moeten doen



Op 3 juli 2026 heeft de Ministerraad ingestemd met de herziening van het rijkscloudbeleid. Na onderzoeken van de Auditdienst Rijk, de Algemene Rekenkamer en vragen en moties uit de Tweede Kamer zijn aanbevelingen en adviezen meegenomen. Rijksorganisaties moeten bij het gebruik van publieke clouddiensten voortaan rekening houden met geopolitieke risico's en afhankelijkheid van één leverancier. De herziening 2026 is een update van het cloudbeleid uit 2022, heeft een breder bereik en bevat diverse aanscherpingen om de rijksoverheid te helpen om beter inzage in de risico's van cloudgebruik te krijgen.

Samen vormen deze elementen de basis voor een meer volwassen benadering van cloudgebruik binnen de rijksoverheid. Cloudtechnologie zal de komende jaren immers een centrale rol blijven spelen in de digitale infrastructuur van de overheid. Juist daarom is het van belang dat technologische innovatie gepaard gaat met sterke governance, transparante risicoafwegingen en strategische regie.

Slotbeschouwing: soevereiniteit als continu proces

Ons rapport schetst geen beeld van een overheid die lichtzinnig omgaat met cloudtechnologie. Wel maakt het duidelijk dat het gebruik van cloud binnen de rijksoverheid in belangrijke mate organisch en pragmatisch is gegroeid, terwijl een volledig geïntegreerd strategisch kader zich nog ontwikkelt.

Ministeries en uitvoeringsorganisaties hebben cloudoplossingen ingezet om digitalisering te versnellen en IT-voorzieningen te moderniseren. Deze ontwikkeling sluit aan bij bredere trends in zowel de publieke als private sector. Tegelijkertijd laat het onderzoek zien dat de governance rond cloudgebruik, met name op het gebied van: overzicht, risicobeheersing en rijksbrede coördinatie, nog niet overal dezelfde volwassenheid heeft bereikt.

Voor professionals in informatiebeveiliging ligt hier een belangrijke les. Digitale soevereiniteit is geen statische eigenschap, maar een continu proces van beheersing, heronderhandeling en strategische positionering. In een omgeving waarin technologie, marktdynamiek en geopolitieke verhoudingen voortdurend veranderen, vraagt soevereiniteit om blijvende aandacht voor governance, contractuele afspraken en afhankelijkheden.

De rijksoverheid staat daarmee voor een fundamentele opgave. Cloud kan worden benaderd als een efficiënt hulpmiddel voor IT-modernisering, maar kan ook worden beschouwd als strategische digitale infrastructuur die vraagt om expliciete regie en langetermijnbeleid.

De 'donkere wolken' waar de rapporttitel op wijst zijn daarmee niet zozeer een voorspelling, maar eerder een signaal. Dit onderstreept dat digitale soevereiniteit geen vanzelfsprekendheid is. Dit vraagt om actieve, gezamenlijke en strategische sturing. Zeker in een omgeving waarin overheidsprocessen steeds afhankelijker worden van cloudinfrastructuur.

Referenties

(1) https://www.rekenkamer.nl/documenten/2025/01/15/het-rijk-in-de-cloud



COLUMN PRIVACY

Mr. Rachel Marbus

Vogelvrijverklaarde

Het zal weinigen ontgaan zijn. De potentiële verkoop van Solvinity en het gevaar dat gegevens van Nederlandse burgers in buitenlandse (USA) handen komt te liggen. Het heeft zich ontpopt tot een ware soapserie met een breed scala aan 'schurken'. We hebben de grote schurken: de kwaadwillende statelijke macht, die met diens tengels in de gegevens kan graaien. We hebben de geniepige schurk: de beleidsverantwoordelijke, die maar wat graag de klokkenluider onder de bus gooit. En we hebben de tot schurk gemaakte: de hoogste privacyambtenaar van het ministerie, die de 'vuile was' buiten hing omdat er grondrechten op het spel staan en niemand leek te luisteren.

Vanuit privacy bezien is het niet eens zo'n vreselijk ingewikkelde zaak. Het gaat om heel gevoelige gegevens van heel Nederland, daar moet je uiterst voorzichtig mee omspringen. En dan moet je dus ook zorgen dat die gegevens niet in buitenlandse handen terecht kunnen komen. Dat is ook gewoon je plicht als overheid. En die plicht weegt dubbel zwaar als je beseft dat burgers geen enkele keuzemogelijkheid hebben; het is verplichte winkelnering. Zonder je DigiD kom je nergens. Lijkt een appeltje-eitje toch?

Dat bleek het dus in het geheel niet en dan al helemaal niet voor die hoogste privacyambtenaar, Pieter van Oordt. Intern had hij alle paden belopen, vergeefs geëscaleerd en alle kaarten uitgespeeld. Dan rest een privacyspecialist weinig anders dan er zoveel op het spel staat. En juist dan weet die privacyspecialist dat naar buiten treden je zeer waarschijnlijk ook de kop gaat kosten. Beroepsmatig kun je ook bijna geen andere keus maken, het zou de integriteit van je beroep aantasten, zou je niet handelen. En denk nu niet dat dit maar een eenmalige gebeurtenis is, ook mij en anderen van mijn privacyvrienden is het overkomen. Je nek uitsteken om de privacy van personen te kunnen borgen, feitelijk dus gewoon je werk doen, en dat met een ontslag of een 'vrijwillig vertrek' moeten bekopen.

Nu wordt niemand graag verteld dat die het bij het verkeerde eind heeft en dat die de wet met voeten treedt. En die boodschap wordt harder en luider naarmate je die blijft negeren – er gaat bijna altijd een lang traject: "wij van privacy adviseren u dat niet zo te doen, maar wel op deze manier", aan vooraf. Maar op een gegeven moment is ook de maat voor privacy vol. En dan gaat het knetteren. Maar vraag je eens af: wat vinden wij er nu eigenlijk van dat mensen die grondrechten beschermen de laan uit gewerkt worden als wat zij te melden hebben bijzonder onplezierig is? We mogen toch gevoeglijk stellen dat dit niet deugt, dat het zaakje stinkt van alle kanten.

En Pieter van Oordt, hoe gaat het nu met zijn carrière? Zijn ontslag is inmiddels aangevraagd. Eigenlijk verdient de overheid een rode kaart, maar die zal wel weer door iemand met macht teruggedraaid worden

Rachel



Auteurs: Marijke Stokkel, senior manager cybersecurity en Robert van Vianen, partner cybersecurity, beiden werkzaam bij BDO Risk Advisory. Zij zijn bereikbaar via: marijke.stokkel@bdo.nl respectievelijk robert.van.vianen@bdo.nl



Ik vaar blind op mijn CISO!

en vier andere overtuigingen die de digitale weerbaarheid niet vooruithelpen

Halverwege de training leunt de CEO achterover en schraapt zijn keel. In een lichte ruimte met hoge ramen zit een groep van twaalf mensen in comfortabele stoelen rond een ovaalvormige tafel. We hebben net uitgelegd hoe cyberaanvallers organisaties zoal binnendringen. De CEO steekt van wal. *"Je kunt investeren wat je wilt, maar er hoeft maar één medewerker te klikken op een phishinglink en alles ligt alsnog plat."* Rond de tafel wordt instemmend geknikt.

Eén klik is zelden einde verhaal

De reactie is begrijpelijk. Organisaties bestaan uit mensen, en mensen zijn niet feilloos. Maar in deze redenering schuilt een aanname die de blik vernauwt. Want het risico wordt zo wel heel sterk bij individuele medewerkers neergelegd, terwijl digitale weerbaarheid breder wordt bepaald.

De afgelopen periode verzorgden wij vanuit BDO Risk Advisory bestuurderstrainingen in het kader van de Cyberbeveiligingswet (Cbw). In die gesprekken zien we telkens hetzelfde: bestuurders zijn betrokken en scherp, maar hanteren soms aannames die de digitale weerbaarheid eerder vertroebelen dan versterken. In dit artikel bespreken we vijf van die aannames en tonen wat organisaties in de praktijk verder helpt.



Aanname 1: ‘Eén klik op een phishinglink en de boel is verloren.’

Deze aanname, zoals verwoord door de CEO, horen we vaker. Sommige bestuurders gaan ervan uit dat één verkeerde klik het hele netwerk onderuit kan halen. Dat is te kort door de bocht. Organisaties werken doorgaans met ‘defense in depth’: een gelaagde manier van beveiligen, met technische, organisatorische en mensgerichte maatregelen. Geen van die maatregelen is op zichzelf waterdicht, maar samen verkleinen ze de kans op een succesvolle aanval aanzienlijk (1).

Neem als voorbeeld een phishingmail. Als een medewerker op een link klikt, met als effect dat ransomware zich installeert, moet er nog veel goed gaan voor de aanvaller. Idealiter wordt de mail al eerder tegengehouden: filters herkennen verdachte afzenders of bijlagen. En zelfs als iemand toch klikt, grijpen andere maatregelen in. Browserbeveiliging kan een malafide website blokkeren en endpointbeveiliging voorkomt idealiter dat schadelijke software wordt uitgevoerd.

Komt een aanvaller toch binnen, dan stopt het daar niet. Zonder openstaande kwetsbaarheden – bijvoorbeeld door achterstallige updates – wordt het installeren van malware een stuk lastiger. Met beperkte toegangsrechten wordt de impact van een aanval begrensd en door netwerksegmentatie verspreidt een aanval zich niet zomaar verder. En als de organisatie een goede logging en monitoring heeft ingericht, worden afwijkingen, zoals onbekende inlogpogingen of vreemd dataverkeer, sneller zichtbaar. Daarmee kan een aanval in een vroeg stadium worden gestopt.

En zelfs in het slechtste geval — wanneer systemen daadwerkelijk worden geraakt — zorgen betrouwbare back-ups ervoor dat data kan worden teruggezet en de organisatie weer op gang komt.

Eén klik is zelden het einde van het verhaal. Het is hooguit het begin van een keten waarin elke verdedigingslaag opnieuw het verschil kan maken. Dit biedt houvast in het gesprek met bestuurders: niet focussen op die ene klik, maar op de vraag welke verdedigingslagen ontbreken of versterkt moeten worden.



Aanname 2: ‘We nemen wel een cyberverzekering, dat scheelt een hoop gedoe.’

Tijdens een training komt de vraag regelmatig op tafel. Zodra bestuurders zicht krijgen op het speelveld van dreigingen en maatregelen, vragen zij zich af of dit risico niet gewoon te verzekeren is, want het scheelt hen een hoop gedoe. De gedachte



Een cyber-verzekering is geen panacee

erachter is begrijpelijk. Een verzekering lijkt een praktische uitweg.

Maar zo simpel is het niet. Verzekeraars stellen hoge eisen aan preventie; zonder aantoonbare maatregelen wordt er bij een incident niet uitgekeerd. Tegelijk is de dekking soms beperkter dan veel bestuurders denken. Risico's als social engineering, CEO-fraude en identiteitsfraude vallen niet altijd binnen de basisdekking en vragen vaak om aanvullende modules. Wat wel en niet gedekt is, verschilt bovendien sterk per aanbieder en polis.

Vanwege de grote toename in cyberaanvallen zijn de premies de afgelopen jaren fors gestegen, terwijl dekkingen juist zijn ingeperkt. Er zijn geregeld uitsluitingen voor veelvoorkomende scenario's zoals ransomware of aanvallen via leveranciers (2). Daar komt bij dat de markt onder druk staat. Uit sommige onderzoeken blijkt dat criminelen actief proberen te achterhalen of een organisatie verzekerd is, bijvoorbeeld door in gecompromiteerde systemen te zoeken naar documenten met termen als insurance of policy. Die informatie kan hun onderhandelingspositie versterken en leiden tot hogere initiële losgeldeisen. Grote internationale datasets laten echter geen eenduidig verband zien tussen het hebben van een cyberverzekering en de uiteindelijke hoogte van losgeldbetalingen. De impact van een verzekering op het verloop van een ransomeware-incident blijkt sterk afhankelijk van: sector, polisvoorwaarden, incidentrespons en het type aanval.

Een cyberverzekering kan helpen, maar is dus geen oplossing op zich. Het blijft een financiële laatste redmiddel. Het vraagt om een nuchtere afweging: past een cyberverzekering bij het risicoprofiel van de organisatie, als aanvulling op – en nadrukkelijk niet ter vervanging van – goede cybersecuritymaatregelen.

Aanname 3. 'Moeten we niet weg bij Microsoft?'

In de Cbw-training zien we dat bestuurders het onderwerp "Moeten we niet weg bij Microsoft?" steeds vaker zelf ter sprake brengen. Zij merken op dat hun organisatie sterk leunt op Microsoft en vragen zich hardop af of dat inmiddels ook een risico is. De aanwezige IT-verantwoordelijke verslikt zich vervolgens bijna in de koffie. Die weet wat zo'n overstap in de praktijk betekent.

Maar de vraag is terecht. Het is goed om kritisch te kijken naar afhankelijkheden. Ongeacht de precieze leverancier wil je als organisatie de regie houden over wat er met je data gebeurt en of je dienstverlening beschikbaar blijft. Geopolitieke spanningen of buitenlandse wetgeving kunnen die regie onder druk zetten. Met als reëel risico dat data wordt opgevraagd of dat toegang tot systemen wordt beperkt of zelfs stopgezet.

Betekent dit dat je moet vertrekken van niet-EU leveranciers? Misschien wel, zeker als je in die systemen werkt met zeer gevoelige data, afhankelijk bent van continue beschikbaarheid en/of een aantrekkelijk doelwit bent in een geopolitieke context. Maar een snelle overstap is complex, kostbaar en risicovol. Voor veel organisaties wegen de voordelen niet op tegen de nadelen. Dan ligt de oplossing in stapsgewijze autonomie. Start met een noodvoorziening in het geval van een storing, versleuteling met sleutels in eigen beheer, een offline

back-up bij een Europese partij en het uitwerken van een realistische exitstrategie (4). Zo krijg je stap voor stap meer grip, zonder direct het hele fundament te hoeven vervangen.

Aanname 4. 'Ze zitten toch al binnen'

Steeds vaker klinkt in bestuurskamers de overtuiging dat aanvallers zó geavanceerd zijn geworden dat verdedigen nauwelijks nog zin heeft. "De Russen en Chinezen zitten toch al binnen." Het klinkt realistisch, maar het werkt ook verlammend. Want waarom zou je dan nog iets doen? Dat aanvallen slimmer en sneller worden, klopt. Aanvallers gebruiken bijvoorbeeld AI om zwakke plekken sneller te vinden en nieuwe exploits te ontwikkelen. Maar in de praktijk ontstaan de meeste incidenten nog altijd niet door spectaculaire nieuwe technieken, maar omdat de basis niet op orde is (5).

Neem de recente datalek bij Odido. Het incident werd door het bedrijf zelf als een 'zeer geavanceerde aanval' beschreven. Een begrijpelijke reflex bij zo'n ingrijpende gebeurtenis. In werkelijkheid kwam de aanval neer op bekende tactieken. Aanvallers deden zich voor als interne IT-medewerkers, ontfutselden inloggegevens en kregen medewerkers zover om multi-factorauthenticatie goed te keuren. Daarmee konden ze inloggen en data ophalen uit het klantcontactsysteem.
De impact was groot — gegevens van miljoenen klanten in verkeerde handen — maar de aanpak was allesbehalve nieuw. Geen zero day, geen technische doorbraak, maar phishing, social engineering en toegangsrechten die te ruim waren ingericht. Eén account gaf toegang tot een enorme hoeveelheid gegevens (6).

Veel incidenten zijn terug te voeren op dit soort tekortkomingen: te ruime toegangsrechten, beperkte monitoring en data die langer wordt bewaard dan nodig. Daarmee geef je een aanvaller, zodra die binnen is, meteen veel ruimte. Dat maakt het perspectief minder fatalistisch. Niet alles is te voorkomen. Maar een passend niveau van basisbeveiliging — patching, toegangsbeheer, monitoring — maakt in de praktijk het grootste verschil. Niet spectaculair, wel effectief.

Aanname 5: 'Ik ben in control want ik vaar blind op mijn CISO'

Aan het eind van onze Cbw-bestuurderstraining leggen we de volgende stelling voor: "Ik ben als bestuurder voldoende in control op het gebied van informatiebeveiliging." Het levert steevast een goede discussie op. Want wat betekent 'in control' zijn eigenlijk? Bestaat dat wel, in een wereld waarin dreigingen zich voortdurend ontwikkelen en kwetsbaarheden deels onbekend zijn?

Cyberaanvallen zijn meestal minder geavanceerd dan wordt beweerd

De reacties lopen uiteen. Sommige bestuurders formuleren het als een streven: je bent nooit volledig in control, maar probeert het zo goed mogelijk te zijn. Anderen zeggen dat ze al blij zijn als ze helder zicht hebben op de pijnpunten en kwetsbaarheden. Van 'in control zijn' is voorlopig nog geen sprake. En heel af en toe zegt iemand: "Ik vertrouw volledig op mijn CISO. Ik geloof dat die de juiste keuzes maakt."

Dat klinkt geruststellend, maar is juist niet de bedoeling. De verantwoordelijkheid ligt namelijk niet bij de CISO, maar bij de bestuurder zelf. Onder de Cyberbeveiligingswet kan die daar zelfs persoonlijk op worden aangesproken. 'In control' zijn betekent niet dat je als bestuurder alles weet, maar wel dat je de risico's overziet, kritische vragen stelt en daar actief op stuurt.

Bovengenoemde aannames zijn menselijk, zeker bij een complex onderwerp als cybersecurity. Maar door ze expliciet te maken, ontstaat ruimte voor een beter gesprek. En dat is precies waar digitale weerbaarheid begint.

Referenties

(1) 'Defense in depth' https://en.wikipedia.org/wiki/Defense_in_depth_(computing)
(2) 'Cyber Insurance 2026: Premiums Doubled, Coverage Halved' https://www.digital-chiefs.de/en/cyber-insurance-premiums-coverage-cfo-calculation-2026/
(3) "Veel bedrijven hebben eigenlijk geen keuze tussen betalen of niet betalen" https://www.ncsc.nl/interviews/veel-bedrijven-hebben-eigenlijk-geen-keuze-tussen-betalen-niet-betalen
(4) 'Digitale autonomie: wat kunnen organisaties nu doen' https://berthub.eu/articles/posts/digitale-autonomie-wat-kunnen-organisaties-nu-doen
(5) 'Organisaties falen op basisbeveiliging: daarom slagen cyberaanvallen nog steeds' https://www.dutchcowboys.nl/cybercrime/organisaties-falen-op-basisbeveiliging-daarom-slagen-cyberaanvallen-nog-steeds
(6) 'Odido hackers kwamen binnen via phishing, deden zich voor als ICT afdeling' https://nos.nl/artikel/2602283-odido-hackers-kwamen-binnen-via-phishing-deden-zich-voor-als-ict-afdeling

Auteur: Maarten Albregts, Security Architect. Bereikbaar via: maarten@syntyra.nl



De onzichtbare aanval op onze vertrouwde SaaS-workflows

Hoe phishing transformeert van malafide links naar trust-manipulatie

Klassieke perimeterbeveiliging en awareness-trainingen richten zich primair op het detecteren van schadelijke linkjes of verdachte domeinnamen. De moderne cloudwereld dwingt aanvallers echter tot een tactische transformatie. Ze breken niet langer in op systemen, maar loggen simpelweg in via legitieme toegangswegen en manipuleren vervolgens menselijke en geautomatiseerde workflows. Dit artikel analyseert deze geraffineerde vorm van trust-manipulatie en introduceert een nieuwe interactionele verdedigingslaag op basis van runtime workflow-provenance.

Wat is 'Provenance'?

De term provenance is oorspronkelijk geleend uit de kunstwereld, waar het de gedocumenteerde herkomstgeschiedenis van een kunstwerk beschrijft om de echtheid te bewijzen (wie had het schilderij in bezit voordat het in het museum belandde?).

Vertaald naar de browser betekent workflow-provenance de digitale stamboom van een actie. Het beantwoordt niet de vraag; wat er op dit moment op het scherm te zien is, maar hoe de gebruiker daar exact terecht is gekomen. Is een OAuth-inlogknop verschenen omdat de gebruiker zélf handmatig een applicatie opstartte of is deze geruisloos getriggerd door een automatische redirect vanuit een externe chat? Binnen de informatica wordt dit fundamenteler gedefinieerd aan de hand van open standaarden (zoals het W3C PROV-model), die causale relaties tussen data en entiteiten in kaart brengen. Die voorgeschiedenis bepaalt de betrouwbaarheid van het huidige moment. Workflow-provenance gaat daarmee fundamenteel verder dan een traditionele link-interceptor of URL-filter; het reconstrueert de asynchrone causale keten van oorzaak en gevolg binnen de live sessie.

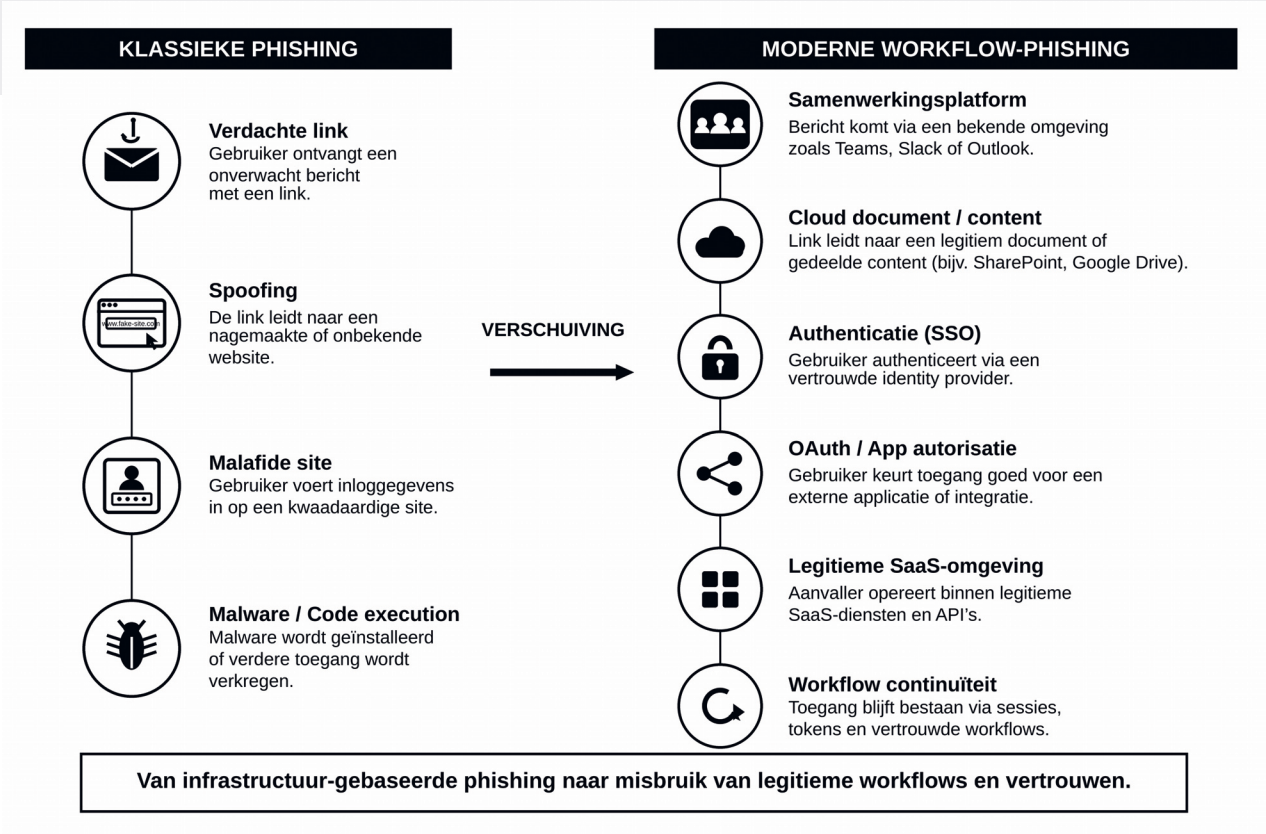
De frictieloze paradox

Een medewerker ontvangt via Microsoft Teams een ogenschijnlijk routine verzoek van een leverancier om aanvullende projectdocumentatie te controleren binnen Atlassian Confluence. De link opent in een vertrouwde browsersessie op een net zo vertrouwde werkplek. Zodra het document opent, vraagt een geïntegreerde viewer via een legitieme Microsoft 365 OAuth-flow om aanvullende verificatie. De medewerker accordeert de pop-up. Voor de gebruiker voelt dit als een frictieloze vervolgstap, maar in werkelijkheid krijgt een malafide applicatie op de achtergrond volledige toegang tot cloudbestanden en mailboxfunctionaliteit.

Waar traditionele phishingaanvallen draaien om duidelijk verdachte artefacten, opereren moderne incidenten steeds vaker binnen legitieme, bestaande trust-relaties en bedrijfsprocessen. Dit type misbruik van proces- en API-ketens was onder meer zichtbaar tijdens de Salesloft Driftcampagne (augustus 2025). Daarbij stalen aanvallers OAuth-tokens van een vooraf goedgekeurde integratie om data te exfiltreren uit honderden Salesforce-omgevingen van ruim 700 organisaties. Er was geen sprake van een inbraak op het platform zelf: de toegang verliep volledig via een legitieme vertrouwensrelatie, waardoor het verkeer nauwelijks te onderscheiden was van regulier gebruik. Organisaties konden zien dat de integratie toegang had, maar niet wat deze ermee deed; terwijl de cross-vendor keten toegang mogelijk maakte naar onder meer Google Workspace. Deze verschuiving wordt onderbouwd door het *Global Incident Response Report van Palo Alto Networks Unit 42: social engineering blijft de absolute hoofdvector voor initiële toegang, maar aanvallers infiltreren door gebruik te maken van bestaande rechten binnen lopende workflows.*

Enterprise-omgevingen zijn er bewust op ingericht om gebruikers zo soepel mogelijk door applicatieketens te loodsen. Single sign-on en cross-app-integraties halen bewust elke drempel weg. Psychologisch gezien houdt dit design, wat psycholoog Daniel Kahneman (2011) 'Systeem 1' noemt, de gebruiker in een modus van snel, intuïtief en automatisch denken op basis van routine (1).

Omdat er geen hobbels zijn, treedt er een effect op dat inherited trust (overgeërfd vertrouwen) wordt genoemd. De gebruiker neemt het legitieme basisvertrouwen van het startpunt onbewust mee naar elke opvolgende redirect, puur omdat de visuele ervaring vloeiend blijft (1). De gezonde achterdocht die nodig is om over te schakelen naar het tragere, analytische denkvermogen ('Systeem 2') wordt door het frictieloze design effectief 'gesust'. Moderne phishing maakt geraffineerd misbruik van deze blinde vlek door een misleidende trust-transitie te forceren.



Figuur 1: Phishingmutatie binnen moderne SaaS-ecosystemen. (Bron: VIGIL Onderzoek)

De browser als runtime-omgeving

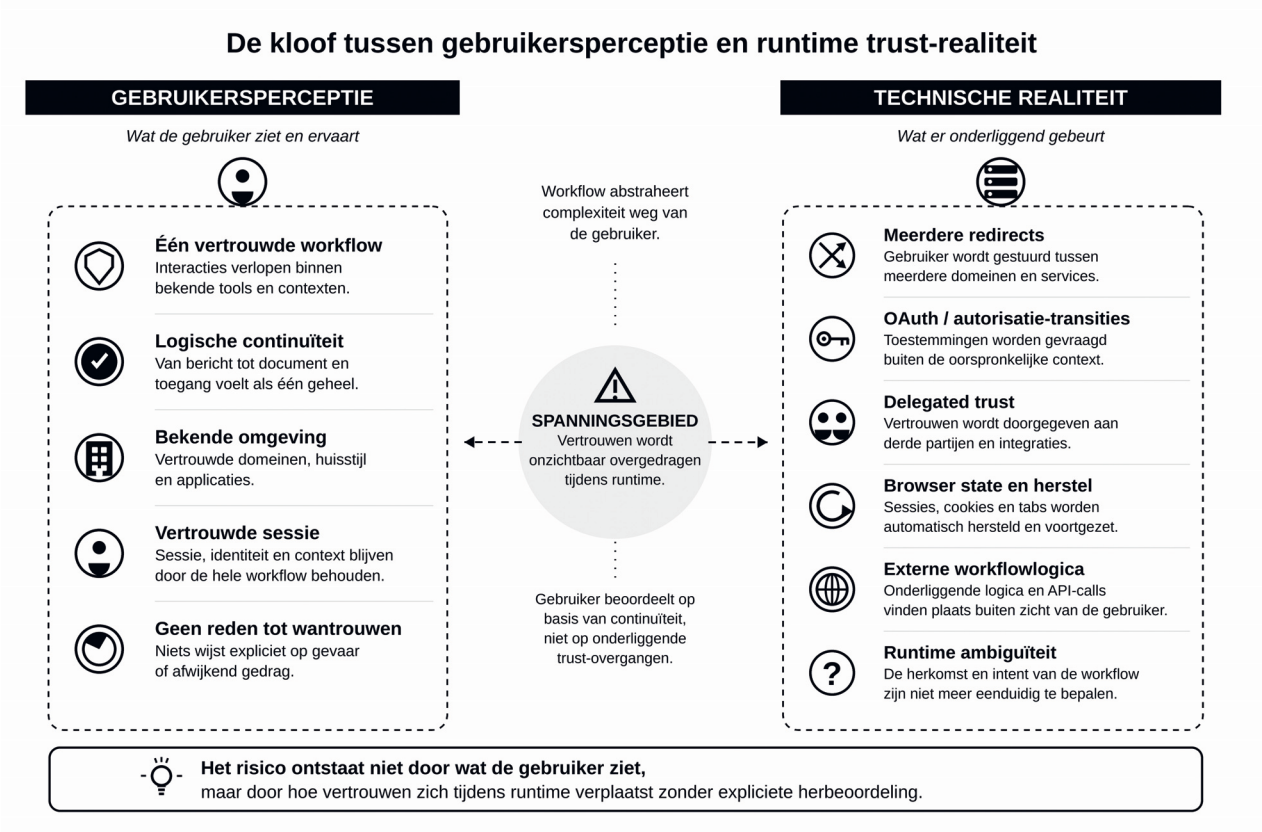
In deze realiteit functioneert de browser als een centrale runtime-omgeving waarin identity flows en applicatie-integraties asynchroon samenkomen. Veel processen bestaan uit een reeks automatische redirects en token-uitwisselingen op de achtergrond. Vanuit technisch perspectief vinden er meerdere trust-overgangen plaats, maar vanuit gebruikersperspectief voelt het als één doorlopende interactie.

Moderne webbrowsers functioneren daarbij allang niet meer uitsluitend als neutrale viewers van webpagina's. Door de opkomst van SaaS-platformen, OAuth- en SSO-ketens, single-page applications (SPA's), client-side redirects en geïntegreerde applicatieworkflows zijn browsers geëvolueerd tot complexe runtime-omgevingen waarin vertrouwensovergangen voortdurend plaatsvinden. Tijdens de ontwikkeling van het VIGIL-onderzoeksproject bleek dat browsers sterk zijn geoptimaliseerd voor gebruiksgemak, sessiecontinuïteit en frictieloze interactie, terwijl herleidbaarheid van workflow-context en navigatie-oorsprong juist steeds diffuser wordt.

Runtime-context raakt versnipperd over redirects, externe applicatieovergangen, achtergrondnavigaties, browser-herstelmechanismen en client-side routing. Hierdoor wordt het voor zowel gebruikers als beveiligingsmechanismen steeds moeilijker om betrouwbaar vast te stellen waarom een navigatie plaatsvindt, vanuit welke context deze is ontstaan en of een vertrouwensgrens ongemerkt is overschreden.

Hierdoor ontstaat een fundamenteel gat in de traditionele verdediging: device trust is niet gelijk aan action trust. Een organisatie kan haar endpoints perfect beheren en strakke MFA-policies afdwingen, maar zodra de gebruiker binnen die goedgekeurde sessie een kwaadaardige interactie autoriseert, faalt het perimeter-denken.

Deze kwetsbaarheid wordt versneld geïndustrialiseerd door de opkomst van generatieve AI. De échte AI-dreiging ligt op dit moment in het vermogen van aanvallers om de context van lopende zakelijke interacties feilloos te interpreteren. Onderzoek van Microsoft Threat Intelligence en OpenAI (2024) bevestigt dat geavanceerde statelijke actoren, zoals de Russische groep Midnight Blizzard, Large Language Models (LLM's) actief misbruiken om de interne communicatiestructuren en workflows van slachtoffers te analyseren. AI stelt kwaadwillenden hiermee in staat om volautomatisch



Figuur 2: het spanningsgebied. (Bron: VIGIL Onderzoek)

uiterst geloofwaardige, interactionele triggers in een bestaande workflow te injecteren. Workflows vormen daarmee steeds vaker het primaire aanvalspad (2).

Van statische detectie naar runtime reassessment

Als risico's niet meer ontstaan bij het allereerste contactmoment, maar pas gaandeweg de interactie zelf, vraagt dat om een andere verdedigingsfilosofie. We moeten verschuiven van statische detectie vooraf naar runtime reassessment tijdens de live interactieflow. Een van de mogelijkheden daarbij ligt in het selectief introduceren van subtiele 'micro-frictie' voor de gebruiker op het moment dat trust-condities fundamenteel wijzigen of minder transparant worden.

Binnen het VIGIL-onderzoeksproject is daarvoor een eerste VIGIL Gate-prototype ontwikkeld in de vorm van een geavanceerde browserextensie. In plaats van uitsluitend de eindbestemming van een navigatie te beoordelen, probeert het systeem runtime-context en trust-overgangen binnen de actuele interactie flow te interpreteren. Zodra er een kritieke trust-transitie plaatsvindt, zoals het openen van een OAuth-consentflow, analyseert het prototype contextsignalen rondom de navigatie en recente workflowcontinuïteit. Door de interactie vervolgens kort te onderbreken met een procesgerichte melding, krijgt de gebruiker aanvullende context om de trust-transitie bewuster te beoordelen ("Systeem 2").

Identiteit als weefsel: de rol van de identity fabric

De noodzaak van runtime reassessment raakt direct aan de manier waarop organisaties hun toekomstige Identity & Access Management (IAM) inrichten. In de security-architectuur van morgen wordt identiteit niet langer benaderd als een reeks losse inlogpoorten, maar als een samenhangend netwerk: de zogenaamde Identity Fabric. Dit model, door analistenbureaus zoals KuppingerCole en Gartner gedefinieerd als de toekomst van gedistribueerd

De roadmap van VIGIL: van extensie naar infrastructuur

Om de visie van runtime trust-transitie-interpretatie te realiseren, wordt het huidige VIGIL Gate-prototype (een vergevorderde MVP ('Minimal Viable Product') in de vorm van een browserextensie) verder ontwikkeld en publiek beschikbaar gesteld voor evaluatie. Dit moet inzicht geven in hoe 'micro-frictie' en contextuele waarschuwingen bijdragen aan bewuste besluitvorming van gebruikers tijdens veiligheidsrelevante interacties binnen moderne digitale workflows.

De blinde vlekken van Big Tech

Hoewel cloud-giganten als Microsoft en Google met initiatieven zoals Continuous Access Evaluation (CAE) en dedicated enterprise-browsers (zoals Chrome Enterprise Premium) serieuze stappen zetten richting realtime beveiliging, blijven deze commerciële oplossingen in de praktijk vaak beperkt tot hun eigen ecosystemen en omgevingssignalen. Dit brengt een tweetal fundamentele gaten met zich mee:

- **De 'Vendor Lock-in' en de fragmentatie van workflow context:** gevestigde platformen begrijpen context uitstekend binnen hun eigen ecosysteem (van Teams naar SharePoint), net zoals Google dat doet binnen Workspace. Zodra een workflow echter cross-vendor gaat (bijvoorbeeld wanneer een gebruiker start in Teams, doorklikt naar Confluence, en autoriseert via een Google Identity), breekt de context-keten volledig.
- **Omgevingsrisico versus interactioneel risico:** huidige enterprise-oplossingen kijken primair naar omgevingsfactoren ("Komt dit verzoek van een bekend device? Is het IP-adres logisch?"). Wat zij fundamenteel missen, is de exacte interactionele stamboom binnen de browsertabbladen; oftewel hoe de gebruiker psychologisch is misleid om op die specifieke autorisatieknop te drukken.

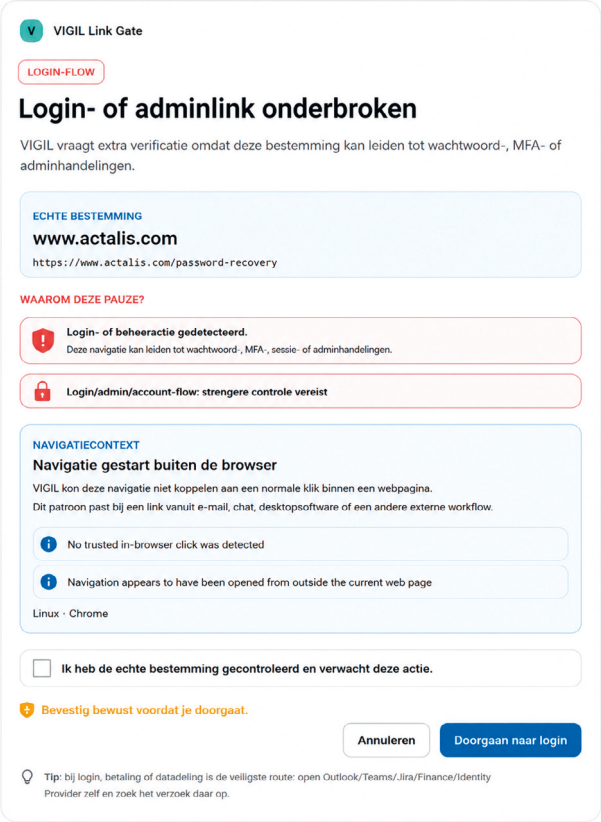
Het VIGIL-onderzoek vult hier een gat door zich specifiek te richten op de leverancier-overstijgende, interactionele stamboom (provenance) van de live workflow zelf.

De stip op de horizon

De ultieme (nu nog theoretische) stip op de horizon is een native integratie waarbij deze runtime-logica inherent onderdeel wordt van de Identity Providers (IdP's) en de Identity Fabric. Wanneer de identiteitsinfrastructuur zélf in staat is de interactionele provenance van een autorisatie-verzoek te beoordelen, is een losse extensie op de endpoint op termijn overbodig. De verdediging tegen workflow-hijacking is dan een ingebakken, (merk onafhankelijk) basiselement van de cloudomgeving geworden. Met een dergelijke oplossingsrichting ligt de nadruk niet langer op het voortdurend waarschuwen van gebruikers, maar op het ondersteunen van gebruikers op de momenten waarop eerder opgebouwd vertrouwen ongemerkt tegen hen kan worden gebruikt.

identiteitsbeheer, streeft naar één geïntegreerde identiteitslaag over alle cloud- en SaaS-omgevingen heen (3,4). Technische standaarden zoals CAEP (Continuous Access Evaluation Profile) maken het mogelijk om risicosignalen in realtime tussen platformen uit te wisselen. Om trust-manipulatie effectief te kunnen bestrijden, zal deze Identity Fabric echter ook verrijkt moeten worden met context over gebruikersinteracties en workflowgedrag. Daarmee verschuift het zwaartepunt steeds meer naar Continuous Adaptive Trust.

SaaS-ecosystemen bestaan steeds vaker uit ketens van onderling vertrouwde identity-relaties, waarbij vertrouwen automatisch tussen platformen, applicaties en OAuth-gebaseerde integraties wordt doorgegeven.



Figuur 3: Micro-frictie' leidt naar Systeem 2 denken.(Bron: VIGIL Onderzoek / Screenshot prototype)

De belangrijkste implicatie hiervan is dat provenance wel eens een zeer belangrijke security control kan worden. Zonder inzicht in de herkomst van een actie weten we weliswaar; wie iets doet (identiteit), maar niet waarom het gebeurt (workflow). Deze ontwikkeling sluit ook aan op moderne Zero Trust-principes, waarbij vertrouwen niet langer statisch wordt toegekend op basis van een succesvolle login, maar continu opnieuw wordt geëvalueerd op basis van context, gedrag en interactiepatronen. Pas wanneer we workflow-provenance onderdeel maken van de bredere Identity Fabric, kan de beveiliging worden verbeterd naar een systeem dat continu context en vertrouwensrelaties meeweegt.

Conclusie: een nieuwe interactionele laag

Naarmate bedrijfsprocessen zich verder verplaatsen naar browser-gebaseerde SaaS-omgevingen, zal phishing zich blijven ontwikkelen in de richting van trust-manipulatie binnen legitiem ogende workflows. Moderne organisaties beschikken inmiddels over uitgebreide detectie-, identity- en monitoringmechanismen, maar binnen complexe SaaS-workflows blijft de gebruiker uiteindelijk vaak degene die de interactie contextueel moet interpreteren en beoordelen. Toekomstige phishingverdediging zal daarom waarschijnlijk steeds meer contextbewust en runtime-georiënteerd moeten worden. Niet ter vervanging van bestaande mailfilters, identity controls of endpointbeveiliging, maar als aanvullende laag binnen de bredere Identity Fabric die gebruikers ondersteunt op momenten waarop eerder opgebouwd vertrouwen ongemerkt tegen hen wordt gebruikt.

Het centrale securityvraagstuk verschuift daarmee langzaam van: "Is deze link veilig?" naar: "Past deze interactie nog logisch binnen de workflow waar het vertrouwen oorspronkelijk vandaan kwam?"

Een interessante open vraag is waar deze vorm van contextuele interpretatie uiteindelijk thuishoort. Moderne digitale omgevingen zijn ontworpen voor snelheid en gemak, terwijl phishing-awareness gebruikers juist leert om voortdurend kritisch te blijven. Kunnen we gebruikers blijven vragen om bij elke stap bewust te vertragen of moeten beveiligingssystemen hen ondersteunen op de momenten waarop de context van een workflow daadwerkelijk verandert? Daarmee ontstaat tegelijkertijd een bredere architectuurvraag: ligt die verantwoordelijkheid primair bij de browser, als uitvoeringsplatform van moderne workflows, of zouden Identity Providers en Identity Fabrics dergelijke signalen moeten meenemen in autorisatiebeslissingen? Naarmate digitale ecosystemen verder integreren, lijkt die discussie relevanter dan ooit.

Referenties

(1) Kahneman, D. (2011). Ons feilbare denken: Thinking, fast and slow (Vertaald door L. van Campenhout & R. de Ridder). Business Contact.

(2) Microsoft Threat Intelligence & OpenAI. (2024). Staying ahead of threat actors in the age of AI: Emerging threats in the core of AI. Microsoft Security Research.

(3) Kuppinger, M. (2020). The Identity Fabric: An Architectural Paradigm for Next-Generation IAM. KuppingerCole Analysts Research.

(4) Gartner Research. (2022). Top Strategic Technology Trends: Cybersecurity Mesh & Identity Fabrics. Gartner, Inc.

(5) Voor geïnteresseerden; achtergrondinformatie in Vigil-Gate:

(5.1) Github site met informatie: https://github.com/malb8/VIGIL-research

(5.2) Google Chrome Store met de Vigil-Gate extensie: https://chromewebstore.google.com/detail/vigil-gate/acedlklfcifjopaofgpffloeggbbmjcp

Auteur: Robert Blokker, is ondernemer en h.o.d.n. Noemeos en EOCME. Hij is bereikbaar via: robert@noemeos.com en via: info@eocme.com | www.eocme.com



De aanvaller verraadt zichzelf

Waarom we de intentie kunnen lezen, niet raden

Het probabilistische paradigma dat de hedendaagse cybersecurity beheerst, kan een aantal problemen wetmatig niet oplossen. In dit artikel laat ik zien waarom — en hoe een deterministisch alternatief, gegrond op behoudswetten uit de natuurkunde, de intentie van een actor rechtstreeks uit het sporenmateriaal reconstrueert in plaats van haar te raden.

Beveiliging als achterwaartse kansberekening

De fundamentele kwetsbaarheid van hedendaagse informatie-architecturen is direct herleidbaar tot de absolute dominantie van het probabilistische paradigma binnen de cybersecurity. Binnen dit raamwerk wordt beveiliging noodgedwongen benaderd als een achterwaartse kansberekening: we kijken met de ervaring van toen naar de situatie van nu, hoofdzakelijk op basis van checklists en statistische gemiddelden uit het verleden.
Deze methodologie was historisch terecht, simpelweg omdat er geen natuurwetmatig alternatief beschikbaar was. Zonder een causaal ijkpunt aan de bron is empirische analyse van datastromen de enige valide route om anomalieën te identificeren. Het logische gevolg van deze werkwijze is echter dat zaken die vooraf niet zijn bedacht of niet op de checklist staan, buiten de waarneming vallen.

Het data-integriteitsprobleem

Daarbij komt een tweede operationeel probleem: de kwaliteit en uitbating van de benodigde data. Voor een betrouwbare statistische analyse is volledige data vereist. In de praktijk is die data vaak incompleet of verwrongen. Wat niet direct bruikbaar is, moet worden weggelaten of aangepast, omdat de analyse anders niet correct functioneert. We hebben dan niet meer de beschikking over de werkelijkheid as-is, maar over een statistisch gemiddelde werkelijkheid.

Twee typen problemen — lineair en wicked

Om de aard van deze kwetsbaarheid te begrijpen, moeten we terug naar de basis: wat is een probleem eigenlijk? In de systemische werkelijkheid bestaan er fundamenteel twee typen, elk met een totaal verschillende dynamiek en wetmatigheid.

Lineair:
het eerste type zijn de lineaire, technische problemen. De oorzaak heeft hier een directe, mechanische en aanwijsbare herkomst — een materiaaldefect, een foute coderegel, een defecte hardware-component. Oorzaak en gevolg zijn helder aan elkaar gelinkt. Het probleem is statisch: het verandert niet van vorm of intentie terwijl je het probeert op te lossen. Hier functioneren het probabilistische paradigma en de traditionele cybersecurity uitstekend.

Wicked;
het tweede type zijn de wicked problems. Deze zijn fundamenteel betekenis gestuurd: er zit een levende intentie achter of ze worden gedreven door een vooropgezet doel van een actor. Een wicked problem is vloeibaar en muteert voortdurend. Elke poging om het op te lossen met traditionele middelen verandert het probleem zelf. Er is hier geen lineaire oorzaak-gevolgketen; de dader of dreiging manifesteert zich telkens opnieuw in een andere vorm en op een onverwacht tijdstip. Statische checklists vangen dit niet, omdat de intentie zich aanpast aan de controle die je inricht.

De technische reflex en het verlies van betekenis

De reactie van het dominante paradigma op deze complexiteit is inherent technisch, omdat verondersteld wordt dat er geen alternatieve weg bestaat. Zodra men met de ongrijpbare dynamiek van een wicked problem wordt geconfronteerd, treedt de "technische reflex" op: men valt automatisch terug op wat gemeten en via statistische checklists of p-waarden kan worden gecontroleerd. Juist die poging om de werkelijkheid te versimpelen via achterwaartse data-analyse zorgt ervoor dat de betekenis ineenstort tot louter data. We wissen de context uit om de statistiek te redden.

Dat opschalen kent twee grenzen. Economisch lopen opslag-, compute- en energiekosten op, terwijl de marginale detectie-meerwaarde afneemt (S-curve) — op enig moment houdt het simpelweg op. Wetmatig vernietigt grenzeloze data-accumulatie uiteindelijk de betekenis zelf.

Contextpsychologie en de paradigmaverschuiving

Om de mechanismen achter deze betekenis gestuurde problemen te doorgronden, bleek naast mijn organisatiekundige achtergrond de aanvullende psychologische kennisbasis een verrijking. Dit traject heeft geleid tot de ontwikkeling van Context Psychologie (CP).

CP doet een radicale, paradigmatische heroverweging van hoe de werkelijkheid is opgebouwd. Het vigerende paradigma hanteert een mechanische, opwaartse causale lijn: alles begint bij informatie, daaruit ontstaat materie, en daaruit wordt pas achteraf betekenis afgeleid.

CP postuleert exact het omgekeerde: meaning — betekenis in technische zin — is de fundamentele driver. De werkelijke causale keten verloopt omgekeerd: niet van informatie naar materie en pas daarna naar betekenis, maar van meaning naar informatie naar materie.

Begrippen in gewone taal

Conservation Law of Meaning:
de gedachte dat meaning niet verdwijnt wanneer zij van vorm verandert. De betekenis blijft aanwezig in de sporen, ook als die sporen digitaal, fysiek of tekstueel zijn.

Enactment:
het moment waarop uit alle mogelijkheden één werkelijkheid wordt geselecteerd. Wat eerst nog open lag, wordt dan concreet zichtbaar in handelen, data of sporen.

Lagrangiaan:
precies gezegd is dit het verschil tussen de kinetische en de potentiële energie van een systeem. Dit is een methode om het gedrag van een systeem te bepalen. Daarbij is de integraal over de tijd van de langrangiaan een weergave van de actie van dat systeem. Koppelt dus 'input' aan de 'output'!

Meaning:
betekenis in technische zin. Niet alleen wat iemand "bedoelt", maar het organiserende principe waardoor informatie richting, waarde en samenhang krijgt.

Meaning configuration:
de specifieke betekenisvorm die door Enactment ontstaat. Vanaf dat moment is niet alles meer open; één richting is gekozen en wordt zichtbaar.

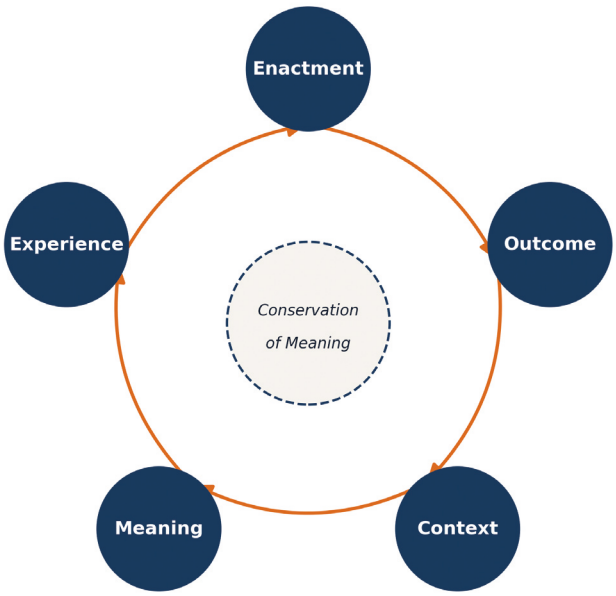
Noemeon:
de kleinste drager van meaning binnen dit framework, vergelijkbaar met de manier waarop een foton licht draagt.

SU(7)-ijksymmetrie:
de wiskundige structuur die binnen het EOCME®-framework wordt voorgesteld om te verklaren waarom meaning behouden blijft over verschillende vormen en niveaus.

Verticals:
de op specifieke sectoren ontwikkelde specialistische hard- & software door (hard/software) bedrijven die zich richten op zeer specialistische sectoren, zoals: gezondheidszorg, financiële dienstverlening, detailhandel, onderwijs, overheid en het producerend bedrijfsleven.

De cyclus van betekenisbehoud

Enactment → Outcome → Context → Meaning → Experience



Afbeelding 1 — Enactment > Outcome > Context > Meaning > Experience. De betekenis blijft behouden over alle transformaties.

Hoe wordt betekenis dan zichtbaar?

Volgens Context Psychology ontstaat meaning niet pas achteraf uit informatie. Meaning is aanwezig als het geheel aan mogelijkheden dat nog openligt: alle mogelijke richtingen, bedoelingen, interpretaties en uitkomsten, die nog niet zijn vastgelegd. Via Enactment wordt uit dat geheel één specifieke meaning configuration geselecteerd. Die configuratie wordt vervolgens zichtbaar als informatie en kan, afhankelijk van het domein, condenseren tot materiële of digitale sporen.

De operationele cyclus, waarin dit gebeurt, is:
Enactment > Outcome > Context > Meaning > Experience > Enactment
Dit is de universele cyclus waarin meaning behouden blijft over alle transformaties (zie afbeelding 1). Het onderliggende mechanisme dat ervoor zorgt dat de patronen zich stabiel herhalen is *memory reconsolidation*.

Een korte verduidelijking is hier op zijn plaats. De terminologie die hierna volgt — Noemeon, SU(7)-ijksymmetrie,

Conservation Law of Meaning — is in het informatiebeveiligingsvakgebied nog niet ingeburgerd. Het deterministische paradigma waaruit deze begrippen voortkomen heeft pas in augustus 2025 zijn formele vorm gekregen en is in oktober 2025 omgezet in een patentaanvraag. De onderliggende ijktheorie ligt momenteel ter peer review bij het American Institute of Physics. De wiskunde zelf grijpt terug op klassieke fysica — en daar begin ik mee.

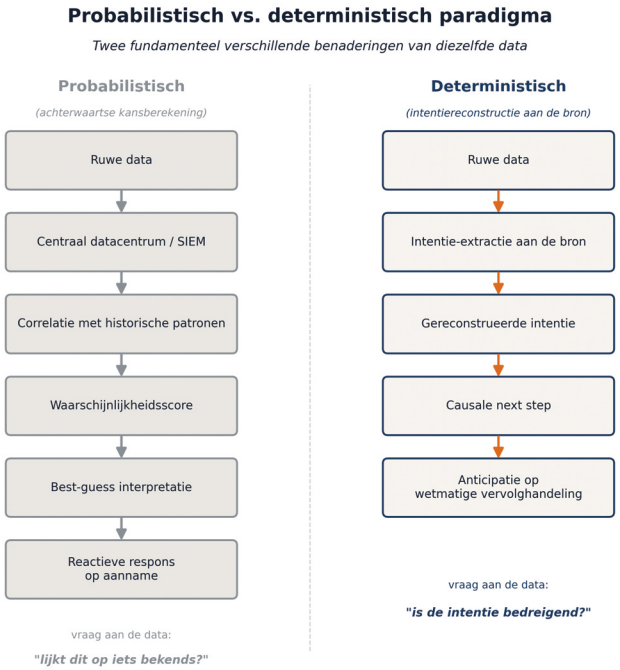
De wiskunde, in herkenbare taal

In de natuurkunde geldt het theorema van Noether: Noether zegt dat bij elke geconserveerde grootheid een wiskundige symmetrie hoort. Bijvoorbeeld: energiebehoud correspondeert met tijd-symmetrie en impulsbehoud correspondeert met ruimte-symmetrie. Datzelfde principe geldt ook voor betekenis.

Omdat meaning behouden blijft over de hele cyclus — de Conservation Law of Meaning — moet er een onderliggende symmetrie zijn. Binnen het EOCME®-framework wordt die symmetriestructuur voorgesteld als een SU(7)-ijksymmetrie (gaugefield). Het deeltje dat deze symmetrie draagt — analoog aan het foton dat het elektromagnetische veld draagt — heb ik het Noemeon genoemd.

Voor de praktijk komt het hierop neer: zoals een foton de informatie van een lichtbron meedraagt door alle media heen, draagt het Noemeon de intentie van een actor mee door alle digitale sporen die hij achterlaat: logs, code, file-artifacts, netwerkverkeer. De intentie gaat niet verloren tijdens transformaties van data; ze blijft wetmatig aanwezig in elk individueel datapunt. Dat is geen filosofie maar een wiskundig gevolg van Noethers stelling toegepast op het betekenisveld.

Elke intentie die in het veld binnenkomt, laat dus onherroepelijk sporen achter. Zoals een dader materiële sporen achterlaat op de plaats van een misdaad of zoals wij sporen van onze intentie achterlaten in tekst, zo laat elke bewuste handeling sporen na in alle producten van wat ik betekenis gestuurd gedrag noem: data, software, foto's, schadepatroon, fysieke producten, tekst. Die intentiesporen worden direct uit de bron gehaald en gevoed aan de deterministische mathematical engine van het analyseprotocol: dit wat ik gemakshalve een protocol noem bestaat uit een serie formules bijeengehouden door een Lagrangiaan, die input met output verbindt.



Afbeelding 2 – Twee fundamenteel verschillende benaderingen van diezelfde data.

De centrale claim voor cybersecurity

Wanneer je nu vanuit het perspectief van de deterministische AI-infrastructuur kijkt, verschuift de vraag die je aan de data stelt fundamenteel (zie afbeelding 2). Waar het probabilistische paradigma vraagt: "lijkt dit op iets dat ik eerder gezien heb in mijn database en wat is dan de meest waarschijnlijke verklaring?" — dus waarmee correleert het — vraagt het deterministische protocol iets heel anders. Het vraagt: "is de intentie achter deze handeling bedreigend, ja of nee?" Het reconstrueert daarmee uit de informatie de betekenis, en deze uitkomst is volledig auditable qua proces en resultaat, en vrij van hallucinaties.

Elk individueel datapunt wordt beoordeeld op intentie; geen enkel datapunt wordt daardoor weggefilterd als ruis. Er gaat dus niets verloren in een statistisch gemiddelde. En omdat de uitkomst een gereconstrueerde intentie is, is de uitkomst geen waarschijnlijkheidsscore. Dit maakt dat op basis van deze uitkomst ook een causale next step kan worden geformuleerd waarop geanticipeerd kan worden. Geen gok over wat er kan gebeuren, maar een afgeleide van wat de actor met deze handeling wil bereiken en dus

logisch als volgende stap zal ondernemen. Dit geeft aan wat de potentie van het deterministische, fundamenteel nieuwe paradigma kan betekenen — niet alleen voor cybersecurity, maar ook voor inlichtingenwerk en situational awareness.

Casus: detectie aan de bron in realtime

Hieronder volgt een representatieve, gecomprimeerde dataset van een verdachte netwerk- en systeemgebeurtenis. Dit is exact het type ruwe data dat in traditionele cybersecurity naar een centraal datacentrum gestuurd moet worden om gecorreleerd te worden met historische gemiddeldes. Traditionele systemen gaan nu rekenen: is die encodedcommand bekend? Is het IP-adres vaker bezocht? Is 4,5 MB uploaden normaal voor deze gebruiker op een donderdagmiddag?

(
{
"timestamp": "2026-05-28T14:02:01Z",
"event_id": 4624,
"source": "Security-Auditing",
"user": "user01",
"ip_address": "192.168.1.45",
"description": "An account was successfully logged on. Logon Type: 3"
},
{
"timestamp": "2026-05-28T14:02:05Z",
"event_id": 1,
"source": "Microsoft-Windows-Sysmon",
"user": "user01",
"process": "powershell.exe",
"arguments": "-nop -w hidden -encodedcommand aW52b2tlLWV4cHJlc3Npb24g...",
"parent_process": "explorer.exe"
},
{
"timestamp": "2026-05-28T14:02:08Z",
"event_id": 3,
"source": "Microsoft-Windows-Sysmon",
"user": "user01",
"process": "powershell.exe",
"destination_ip": "91.198.174.192",
"destination_port": 80,
"protocol": "tcp",
"status": "established"
},
{
"timestamp": "2026-05-28T14:02:15Z",
"event_id": 11,
"source": "Microsoft-Windows-Sysmon",
"user": "SYSTEM",
"process": "powershell.exe",
"target_file": "C:\Windows\Temp\lsass_dump.dmp",
"access": "Write"
},
{
"timestamp": "2026-05-28T14:02:22Z",
"event_id": 3,
"source": "Microsoft-Windows-Sysmon",
"user": "user01",
"process": "powershell.exe",
"destination_ip": "91.198.174.192",
"destination_port": 443,
"bytes_sent": 4529100,
"description": "Large outbound data transfer initiated"
}
)

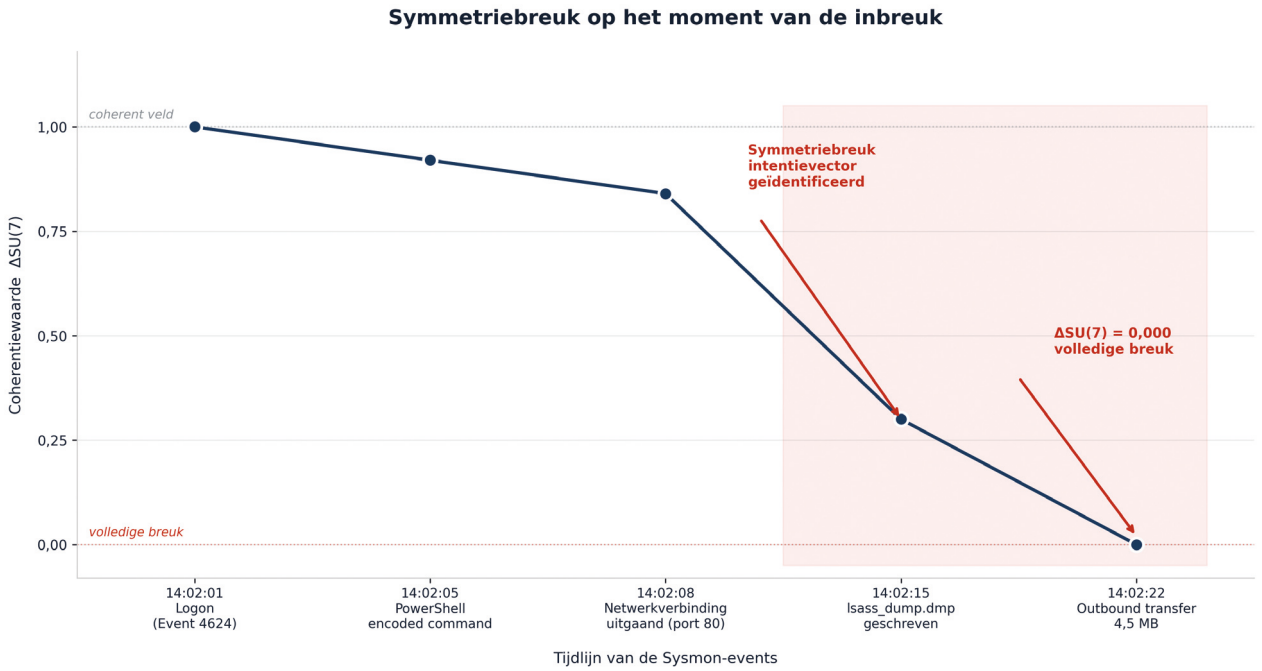
Bij verwerking van deze reeks in het deterministische protocol (werkend op temperatuur 0,0) wordt direct zichtbaar waar de isomorfe (gelijk gevormde) structuur van het betekenisveld vervormt. Op het exacte moment dat het proces switcht van een reguliere netwerkaanroep naar een lokale geheugendump (lsass_dump.dmp) en de daaropvolgende data-exfiltratie, identificeert het systeem de symmetriebreuk aan de bron (zie afbeelding 3).

De invloed van ruis

Ruis verstoort in de deterministische AI-infrastructuur het analyseproces niet. Ruis wordt wiskundig gekenmerkt door het feit dat zij geen outcome-vector bezit. Zonder vooropgezet Outcome (doel) kan ruis het geconserveerde veld niet coherent vervormen, waardoor het deterministische systeem haar direct aan de bron passeert. Alleen informatiestromen met een gerichte betekenisvector kunnen een lokale symmetriebreuk in de SU(7)-structuur veroorzaken. De coherentiewaarde - op het moment van de switch naar de geheugendump - klapt direct naar SU(7) = 0,000; een volledige symmetriebreuk veroorzaakt door de inbrekende intentievector van de actor.

Wat de analyse oplevert

De analyse levert een dossier dat volledig beschrijft wat concreet uit de protocol-pijplijn komt. Dit dossier — auditable qua uitkomst en proces, en vrij van hallucinaties — wijkt in structuur radicaal af van een SIEM-alert. Het dossier bevat de volgende elementen:



Afbeelding 3 — Coherentiewaarde van het veld op de tijdlijn van de events. De waarde klapt naar SU(7) = 0,000 op het moment van de exfiltratie.

- *het exacte breukpunt* — het datapunt of de reeks waar de intentievector het coherente veld binnenkwam. In de Sysmon-casus hierboven; het moment van de switch van netwerkaanroep naar lsass_dump.dmp met daaropvolgende outbound transfer.
- *de gereconstrueerde intentie* — wat de actor met deze keten van handelingen wilde realiseren (credential theft, exfiltratie, lateral movement), afgelezen aan de bron en niet vergeleken met een TTP-database.
- *de evidence chain* — per conclusie de specifieke datafragmenten die haar dragen, volledig traceerbaar tot de individuele logregel.
- *de coherentie-indicator* — een wiskundige waarde (SU(7)) die de mate van symmetriebreuk uitdrukt op het moment van de inbreuk. Geen probability, geen confidence score — een determinant.
- *de causale next step* — gegeven de gereconstrueerde intentie, de logisch te verwachten vervolghandeling van de actor. Input voor actieve anticipatie in plaats van reactieve respons.

Reproduceerbaarheid is gegarandeerd: identieke input levert identieke output, ongeacht het tijdstip of de infrastructuur waarop de analyse draait. Voor audit en het digitaal forensisch onderzoek is dat geen detail maar een eigenschap.

De infrastructuur

Het deterministische karakter van het protocol: pure wiskunde ingebed in harde fysica, geen probabilistische modellen, geen training, geen historische dataset, heeft directe operationele consequenties. Zo zijn er acht gespecialiseerde verticals gebouwd in zes dagen, deze verticals werken van laptop tot serversysteem en van Middenbedrijf tot global enterprise, volledig audit geschikt en hallucinatievrij. Voor iedereen die bekend is met de ontwikkelcyclus van probabilistische AI — waar alleen al het trainen, valideren en uitrollen van één model maanden of langer in beslag neemt — zal het besef er zijn dat dit van een compleet andere orde van grootte is.

Samenvattend

De cybersecurity-praktijk is decennialang opgebouwd rond één centrale aanname: wat we niet eerder hebben gezien, kunnen we niet detecteren. Probabilistische detectie kijkt achterwaarts naar bekende patronen, met als gevolg dat de aanvaller per definitie altijd één onbekende variant vooruit ligt. Het escalatiemodel: meer data, meer modellen, meer rekenkracht; herhaalt deze aanname; het lost haar niet op.

De deterministische benadering verschuift het meetpunt. Niet het patroon dat de aanvaller produceert wordt onder-

Voor wie informatie en intentie tot nu toe als verschillende werelden beschouwde: deze zijn dat niet.

zocht, maar het moment waarop de intentie het coherente veld binnenkomt en de symmetrie breekt. Dat moment is niet statistisch maar wiskundig identificeerbaar, ongeacht of de specifieke handelingen ooit eerder zijn waargenomen. De aanvaller verraadt zichzelf niet door op iets bekends te lijken — hij verraadt zichzelf door het loutere feit van zijn intentie.

Operationeel betekent dit een ander type detectieproduct. In plaats van een waarschijnlijkheidsscore op een gekend dreigingsprofiel levert de analyse een dossier: het exacte breukpunt, de gereconstrueerde intentie, de evidence chain tot op de logregel, de coherentiewaarde en de causaal te verwachten vervolghandeling. Deze elementen verschuiven het werk van het SOC van reactieve respons naar geanticipeerde tegenactie. Voor audit, regelgeving en aansprakelijkheid komt daar het structurele aspect bij: reproduceerbaarheid en hallucinatievrijheid zijn geen ontwerpdoelen, die nog gerealiseerd moeten worden, maar architecturale eigenschappen die niet anders kúnnen zijn.

Voor de CISO en de security-architect zit hier de kern: de fundering onder cybersecurity verandert. Niet de tooling, niet de processen, maar de vraag die je aan je detectielaag stelt. Niet langer "kennen we dit?" — maar "is er intentie?"

Voor wie informatie en intentie tot nu toe als verschillende werelden beschouwde: deze zijn dat niet. De ene draagt de andere mee, natuurwetmatig. Voor cybersecurity betekent dat: we hoeven niet langer terug te kijken om vooruit te zien.

Een uitnodiging tot verdere verdieping

Voor lezers die de wiskundige en theoretische onderbouwing dieper willen verkennen: de ijktheorie, de wet van betekenisbehoud en de empirische validatie op CERN-data alsook de metingen van de kosmische achtergrondstraling, zijn de preprints open access beschikbaar op Zenodo.

Referenties

(1) EOCME® is een geregistreerd merk van Noemeos-EOCME. De grondslagen die in dit artikel besproken worden, zijn open access gepubliceerd op Zenodo (zie hieronder). De onderliggende ijktheorie en de operationele implementatie zijn beschermd door patentaanvraag EP 25 212132.2 (oktober 2025); een internationale PCT-aanvraag wordt in juni/juli 2026 ingediend. De ijktheorie ligt tevens ter peer review bij het American Institute of Physics.

(2) Blokker, R. The Meaning Paradigm: How Context Psychology Unifies Human Behavior, AI, and Organizations. Zenodo. https://doi.org/10.5281/zenodo.19382150

(3) Blokker, R. EOCME: A Meaning-Conservation Framework — Validation on CERN Open Data (v2). Zenodo. https://doi.org/10.5281/zenodo.20135406

(4) Blokker, R. EOCME-CP AI Interaction Infrastructure: A Deterministic Protocol for Human–AI Exchange in Consequential Work. Zenodo. https://doi.org/10.5281/zenodo.19726350

COLUMN LEX

De ontwikkeling van authenticatie
van wachtwoorden naar passkeys

De afgelopen twintig jaar heeft cybersecurity een enorme transformatie ondergaan. Veel hiervan heb ik van dichtbij meegemaakt. In een serie columns duik ik in de ontwikkeling van informatiebeveiliging en belicht ik hoe technologie, bewustzijn en innovatie onze digitale wereld veiliger hebben gemaakt. Dit is deel 1.

Twintig jaar geleden, in 2006, was authenticatie nog een eenvoudig proces. Gebruikers logden in met statische wachtwoorden, die vaak zwak waren en gemakkelijk te raden of te kraken. Systemen gebruikten standaardwachtwoorden zoals "admin" of "123456", waar we nu om lachen. Als je een 'goed' wachtwoord wist te onthouden, paste je dat overal toe. Wachtwoordbeleid bestond niet of werd niet afgedwongen. Wachtwoordbeveiliging bestond uit vaak wachtwoorden vernieuwen. Dit maakte dat de gebruiker wachtwoorden ging opschrijven. Tweefactorauthenticatie (2FA) was complex, met een fysiek token of OTP-lijst en werd alleen toegepast binnen hoogveiligheidsomgevingen zoals banken of militaire systemen.

Authenticatie werd gaandeweg aanzienlijk sterker vooral door de opkomst van smart devices. Een van de grootste verbeteringen was de wijdverspreide adoptie van 2FA, die mogelijk werd gemaakt door de snelle opkomst van smartphones. Waar 2FA in 2006 nog een zeldzaamheid was, is het nu standaard voor de meeste online diensten, van sociale media tot bankieren. Met 2FA moeten gebruikers ook een tweede factor gebruiken, zoals een SMS-code, een OTP-code of een authenticatie-app (zoals Microsoft Authenticator). Door secure elements in smart devices en device-binding technieken werd het mogelijk om de tweede factoren gemakkelijk en veilig te genereren, te koppelen en te gebruiken.

SMS-codes zijn inmiddels al weer verleden tijd, omdat telecom protocollen niet veilig genoeg zijn en SIM-swapping een snelgroeiend probleem werd. Toen de banken mid-2011 een akkoord sloten met de telecombedrijven over SIM-swap notificatie, viel de internetbankieren fraude van tientallen miljoenen euros per jaar vrijwel meteen naar bijna nul.

Ook de biometrische authenticatiemethoden zijn sterk verbeterd, weer mede dankzij smart devices. In 2006 waren biometrische systemen nog duur en onbetrouwbaar, maar tegenwoordig zijn vingerafdrukscanners en gezichtsherkenning gemeengoed op smartphones en laptops. Doordat de biometrische gegevens lokaal in de secure element verwerkt worden ben je gelijk van alle privacy discussies af.

Een andere belangrijke ontwikkeling is de opkomst van wachtwoordloze authenticatie, die ook mogelijk werd gemaakt door smart devices. Technologieën zoals FIDO2 en WebAuthn stellen gebruikers in staat om in te loggen zonder wachtwoorden, door gebruik te maken van device-binding technieken. Smartphones fungeren hierbij als veilige authenticatie-apparaten, die unieke cryptografische sleutels kunnen opslaan en gebruiken. Hier horen ook smart sticks bij, zoals YubiKey.

Ook de beveiliging van wachtwoorden zelf, voor zover die er nog zijn, is verbeterd. Werden wachtwoorden vaak gehasht en gezouten opgeslagen, nu zijn er speciale key derivation protocollen die de computer zwaar belasten tijdens de berekening, wat het kraken van wachtwoorden aanzienlijk bemoeilijkt. Bovendien dwingen veel systemen gebruikers om sterke wachtwoorden te gebruiken, met een combinatie van letters, cijfers en speciale tekens. Deze wachtwoorden moeten ook uniek zijn, hergebruik is uit den boze. De wachtwoordmanager wordt onmisbaar.

Er blijven uitdagingen. Phishing-aanvallen blijven een groot risico, omdat aanvallers gebruikers kunnen misleiden om hun inloggegevens prijs te geven. Over het geheel is de authenticatie in 2026 aanzienlijk veiliger dan in 2006 en het wachtwoord is binnenkort verleden tijd, dankzij de combinatie van: geavanceerde technologieën, betere gebruikerspraktijken, strengere beveiligingsprotocollen en de opkomst van smart devices, die deze innovaties mogelijk maakten.

Lex Borger is security consultant bij Tesorion en oud-hoofdredacteur van IB Magazine. Lex is bereikbaar via lex.borger@tesorion.nl





Auteur: Reza Razai is CEO van Mijn IBP | Cyber Connects. Hij werkte eerder als ethisch hacker, security engineer en CISO. Hij verdiept zich in de vraag hoe je de CISO en de FG ontlast, zodat zij terug kunnen naar hun eigen vak in plaats van naar de rapportage en deelt graag ervaringen over integraal IBP en sectorale kennisdeling. Hij is bereikbaar via: reza.razai@cyberconnects.nl en is ook te vinden op: https://www.linkedin.com/in/reza-razai



Een organisatie wordt nooit fitter dan de experts die haar bewaken

Een verkenning naar de digitale fitheid van de CISO en de FG zelf

Onder de noemer digitale fitheid groeit een beweging die professionals, teams en organisaties helpt om effectiever, veiliger en bewuster met hun werk om te gaan. Vanuit het principe: "eerst de mens, dan de technologie" (1). De kerngedachte is dat digitalisering niet om tools draait, maar om kennis en gedrag en dat goed digitaal gereedschap je lucht, overzicht en focus hoort te geven in plaats van werk. In informatiebeveiliging en privacy kennen we twee experts die ook slachtoffer zijn van het meerwerk uit de verschillende tools, elk vanuit een eigen rol: de CISO als regisseur, die de beveiliging coördineert en bestuur adviseert, en de FG die als toezichthouder op de uitvoering van de AVG wet let. Eén vraag stellen we zelden: zijn die experts zelf nog fit? Of zijn ze, bedolven onder rapportages, audits en compliance-voorbereidingen, allang buiten adem?

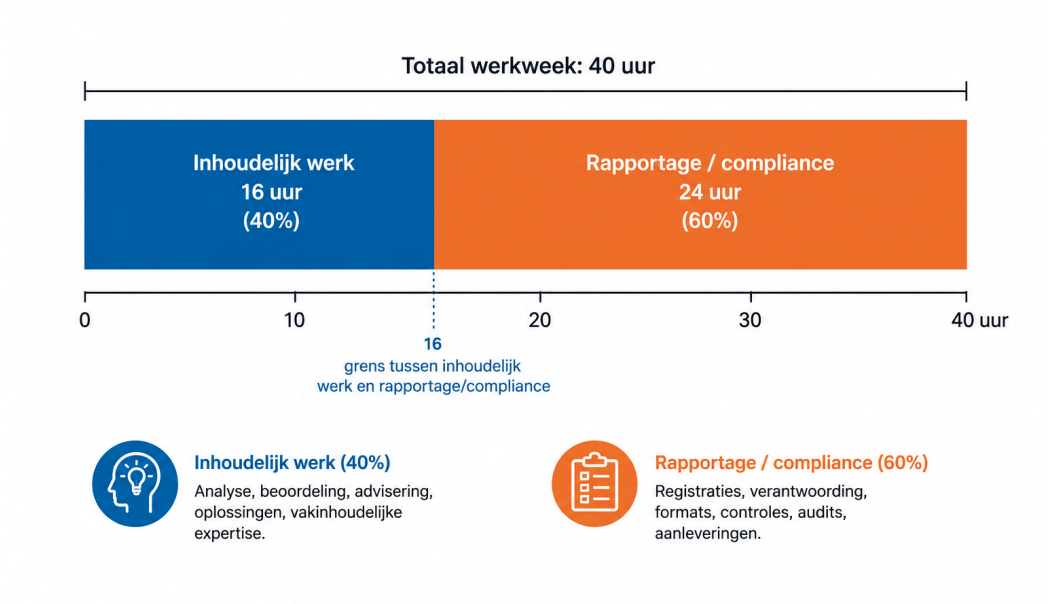
Dit artikel is een korte verkenning van die vraag. Geen sluitend onderzoek, wel een poging om een gevoel dat in het vak breed leeft te toetsen aan beschikbare cijfers en aan ervaringen die elders in voorgaande PvIB uitgaves zijn beschreven. Ik begin met wat het vooronderzoek laat zien, formuleer een paar onderzoeksvragen, analyseer die kort en kom uit bij een mogelijke conclusie. Nadrukkelijk als stelling.

Vooronderzoek

De rol van de CISO is de afgelopen jaren fors breder geworden: databescherming, regelgeving, leveranciersrisico en inmiddels ook AI-governance, het sturen op en verantwoorden van AI-gebruik; het hoort er allemaal bij. In recent onderzoek geeft 96 procent van de CISO's aan: de AI-governance in de hele organisatie te overzien (2) en beheert ruim de helft, tien of meer functies, met een rapportagelijn die steeds vaker rechtstreeks naar het bestuur loopt (3). Tegelijk verschoof het zwaartepunt van het vak van techniek naar aantoonbaarheid: waar securityprofessionals vroeger in architecturen en ontwerpen zaten, zitten ze nu vaker gebogen over gedetailleerde overzichten, overleggen en rapportages (4).

Voor de FG geldt iets vergelijkbaars. Het werk bestaat voor een groot deel uit verwerkingsregisters actueel houden, DPIA's, audits en het zijn van aanspreekpunt. Met de komst van de AI-verordening (de Europese EU AI Act) komt daar meer werk bij. Een Europese, gecoördineerde controle door 25 privacy toezichthouders, met ruim zeventienduizend reacties van organisaties en FG's, wees bovendien op terugkerende knelpunten, waaronder: onvoldoende middelen en onafhankelijkheid van de FG (5). De toezichthouder vraagt dus meer, terwijl de positie vaak begrensder is dan de wet veronderstelt. Die optelsom eist haar tol. In het jaarlijkse 'Voice of the CISO'-onderzoek onder 1.600 CISO's in zestien landen gaf 63 procent aan, het afgelopen jaar burn-out te hebben ervaren of van dichtbij te hebben gezien (6); andere onderzoeken komen op vergelijkbare of hogere cijfers. In de bredere beroepsgroep voelt bijna de helft zich overweldigd door de werklast (47 procent) en uitgeput door het bijhouden van nieuwe dreigingen en technologieën (48 procent) (7).

En de prangende vraag daarachter: levert al die activiteit ook veiligheid op? De signalen wijzen de andere kant op. De digitale basishygiëne, zoals: goede wachtwoorden, updates en toegangsbeheer, verbetert ondanks jaren van aandacht nauwelijks (8). Bij de invoering van de AVG ontstonden vooral stapels beleidsdocumenten in digitale mappen binnen de Big Tech omgevingen, met weinig zichtbare verbetering in de daadwerkelijke beveiliging (9). En 41 procent van de CISO's kan de eigen inspanningen niet koppelen aan aantoonbare risicoreductie (2).



Figuur 1: tijdsverdeling over wel of niet werkprioriteiten

Onderzoeksvragen

Uit dit beeld komen drie vragen naar voren:

1. Waaraan besteden CISO's en FG's hun tijd?
2. Maakt die toenemende rapportage- en compliance-last organisaties ook daadwerkelijk veiliger?
3. Wat doet die onbalans met de expertise en met de mens achter de functie?

Analyse

De eerste vraag doet de cijfers één kant op wijzen: het zwaartepunt is verschoven naar besturen en aantonen. Een functie die zoveel terreinen omvat en steeds vaker aan het bestuur rapporteert (3) en een vak dat zich van ontwerp naar overzicht heeft bewogen (4), laat per definitie minder ruimte voor: de inhoud, architectuur, dreigingsanalyse, advies, privacy- en security-by-design. Bij de FG knelt dat extra, omdat juist het vroegtijdig meedenken bij nieuwe verwerkingen in het gedrang komt zodra de administratieve last de agenda vult (5). De tweede vraag is interessanter. Compliance is niet het probleem: goed uitvoeren, op risico's sturen en er een doorlopend proces van maken draagt degelijk bij (10). Het probleem is de afvinkmentaliteit, waarbij maatregelen worden afgevinkt om te voldoen zonder dat het veiliger wordt: documentatie houdt geen aanvaller tegen (9), training heeft vaak maar een beperkt blijvend effect (8), en het zwaartepunt verschuift naar wat aantoonbaar is in plaats van wat beschermt. Niet voor niets stelt het gedachtegoed van digitale fitheid dat het om kennis en gedrag draait (kijk maar naar de incidenten van de afgelopen tijd en hackersgroep Shinyhunters); niet om het stapelen van tools (1). Als 41 procent van de inspanning niet te koppelen is aan risicoreductie (2), is meer rapportage geen synoniem voor meer veiligheid. Aantoonbaar is niet hetzelfde als veilig.

De derde vraag raakt de kern. Burn-out is een organisatierisico (6,7): uitgeputte professionals maken vaker fouten, zijn minder productief en verlaten vaker het vak, wat de toch al schaarse expertise verder uitholt. Een uitgeputte of ondergewaardeerde expert of een FG die in zijn onafhankelijkheid wordt beknot, levert geen veiliger, fittere organisatie op (5). De conditie van de organisatie hangt dus rechtstreeks samen met de conditie van de mensen die haar moeten bewaken.

Een mogelijke conclusie

Leg deze observaties naast elkaar, en er tekent zich een mogelijke conclusie af. De route naar veiliger organisaties loopt misschien niet via méér rapportage(s), maar via het digitaal fit maken van de CISO en de FG zélf.: Hen de tijd en aandacht teruggeven voor hun eigenlijke vak, zodat compliance een bijproduct wordt van goed beveiligings- en privacywerk, in plaats van het werk zelf. Daarmee passen we het principe van digitale fitheid toe op de experts zelf: eerst de mens, dan de technologie (1).



Figuur 2: het verschil tussen afvinken en effectieve compliance

Wat dat vraagt, laat zich kort samenvatten als:

- geef de expert weer lucht, overzicht en focus;
- ontlast de functie: organiseer de administratieve - en rapportagelaag zo, dat bewijs vanzelf ontstaat uit het werk, niet uit een handmatige eindsprint voor de audit.
- leg het eigenaarschap van risico waar het hoort, bij de lijn en het bestuur, dat onder de Cyberbeveiligingswet (de Nederlandse uitwerking van de Europese NIS2-richtlijn) en de vernieuwde Baseline Informatiebeveiliging Overheid (BIO2) duidelijkere verplichtingen krijgt (10);
- meet en stuur op wat veiliger maakt, niet alleen op wat aantoonbaar is;
- bescherm de mens, want een burn-out is uiteindelijk ook een beveiligingsrisico en
- bewaak de onafhankelijkheid van de FG, daar waar ook of juist de efficiëntie schuilt.

Of dit de juiste conclusie is, laat ik in het midden. Maar als stelling vind ik haar de moeite waard: "Een organisatie wordt nooit fitter dan de experts die haar bewaken." Staan wij toe dat de CISO en de FG zelf buiten adem raken door allerlei tools, dan zijn wij minder veilig.

Tot slot

Daarom leg ik de vraag graag terug bij de lezer, want dit blad spreekt nu eenmaal vrijwel iedere expert in het vak aan. "Hoeveel van jouw week gaat naar inhoud, en hoeveel naar aantoonbaarheid? En wat zou er nodig zijn om jou, als CISO of FG, weer fit te maken voor je eigen vak?" Ik hoor het graag; juist dat gesprek brengt ons verder.

Referenties

(1) Digitale Fitheid, "Eerst de mens, dan de technologie", digitalefitheid.nl (geraadpleegd juni 2026). https://digitalefitheid.nl

(2) Splunk, The CISO Report 2026. https://www.splunk.com/en_us/campaigns/ciso-report.html

(3) Hitch Partners, 2025 CISO Security Leadership Survey. https://www.hitch-partners.com/ciso-security-leadership-survey-results-25

(4) L. Borger, "25 jaar verschuiving in securitymanagement", IB Magazine, jaargang 26, 2026, editie 1, p. 9

(5) EDPB, 2023 Coordinated Enforcement Action — Designation and Position of Data Protection Officers (vastgesteld 16 januari 2024; 25 toezicht-houders, ruim 17.000 reacties). https://www.edpb.europa.eu/system/files/2024-01/edpb_report_20240116_cef_dpo_en.pdf

(6) Proofpoint, Voice of the CISO 2025 (onderzoek onder 1.600 CISO's in 16 landen), 26 augustus 2025. https://www.proofpoint.com/us/newsroom/press-releases/proofpoint-2025-voice-ciso-report

(7) ISC2, 2025 Cybersecurity Workforce Study, december 2025. https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study

(8) M. de Jonge, "Eigen digitale hygiëne: een worsteling, zelfs voor security-professionals", IB Magazine, jaargang 26, 2026, editie 2, p. 4–6

(9) P. Glenstrup, "NIS2-compliance is een voortdurend proces en geen reden tot paniek", IB Magazine, jaargang 26, 2026, editie 1, p. 14–15

(10) E. Becker & K. van der Maarel, "BIO2: een hoger IB volwassenheidsniveau voor de hele overheid", IB Magazine, jaargang 26, 2026, editie 2, p. 18–20

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

Leeftijdsverificatie op sociale media platforms = onzin

Steeds meer overheden pleiten voor leeftijdsverificatie op sociale media platforms, omdat zij verwachten dat dit jongeren beter beschermt tegen schadelijke online risico's. Landen zoals Australië en Frankrijk hebben al leeftijdsgrenzen ingevoerd, vanuit de overtuiging dat sociale media verslaving onder jongeren een groeiend maatschappelijk probleem vormt. In Frankrijk geldt sinds 2024 een minimumleeftijd van 15 jaar, tenzij ouders expliciet toestemming geven.
Binnen de Europese Unie onderzoeken verschillende lidstaten of een minimumleeftijd van 15 of 16 jaar moet worden ingevoerd. Nederland pleit in Brussel voor een Europese minimumleeftijd van 15 jaar, zolang platforms volgens de overheid "onvoldoende veilig" zijn voor minderjarigen. De Europese Commissie verwijst daarbij naar risico's zoals privacy schendingen, algoritmische beïnvloeding en ongepaste content.

De zorgen richten zich vooral op de aard van de inhoud op sociale media. Platforms bevatten regelmatig geweld, pornografie, extremistische boodschappen en andere schadelijke content. Uit het EU Kids Online onderzoek (2020) blijkt dat ongeveer 30% van Europese kinderen tussen 9 en 16 jaar ooit online ongepaste beelden hebben gezien. Beleidsmakers stellen dat leeftijdsverificatie moet voorkomen dat jonge kinderen hiermee in aanraking komen.

Tegelijkertijd is er een hele generatie – grofweg de jongeren geboren na 1995 – opgegroeid met een ongefilterd internet en vrije toegang tot sociale media. Ook mijn eigen kinderen kregen rond hun tiende een mobiele telefoon met wifi internet, zodat zij thuis, onder toezicht van hun ouders, het online domein konden verkennen.

Natuurlijk kwamen ook zij soms onbedoeld terecht op websites met naaktbeelden of ongepaste teksten of beelden. Dat is een logisch gevolg van een open internet. Als ouders spraken we daarover: uitleggen wat ze zagen, duiden waarom het niet passend was en duidelijke grenzen stellen. Dat is opvoeden. Daarnaast beperkten we bewust de tijd die onze kinderen online doorbrachten of deelnamen aan online games. Niet om het internet te verbieden, maar om hen te begeleiden in verantwoord digitaal gedrag.

Onderzoek van onder meer het Sociaal en Cultureel Planbureau (SCP), het Pew Research Center en EU Kids Online laat zien dat de generatie na 1995 in grote meerderheid normaal functioneert: ze volgen onderwijs, werken, onderhouden sociale contacten en gebruiken sociale media zonder structurele problemen.



- Het SCP concludeert dat jongeren "digitaal vaardig en sociaal actief" zijn.
- Pew Research (2023) toont dat 85% van jongeren sociale media gebruikt zonder tekenen van verslaving.
- EU Kids Online vindt dat slechts ongeveer 5–8% van jongeren problematisch gebruik vertoont — vergelijkbaar met andere vormen van mediagebruik zoals gamen of televisie.

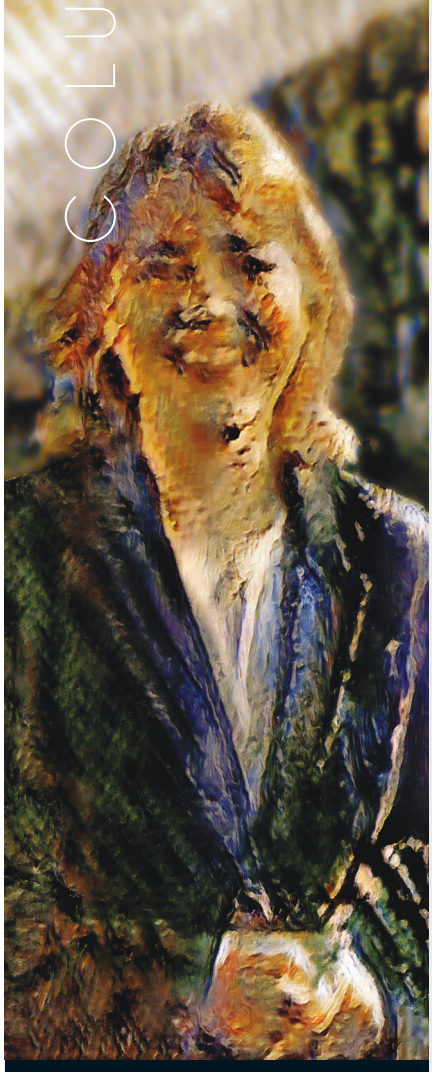
Het idee dat een hele generatie "ontwricht" zou zijn door sociale media wordt door deze data niet ondersteund. De meerderheid gebruikt sociale platforms op een gezonde manier en ontwikkelt geen blijvende negatieve gedragsveranderingen.
Mijn eigen ervaring sluit daarbij aan: met begeleiding, gesprekken en duidelijke grenzen leerden mijn kinderen omgaan met online prikkels. Dat is een normaal onderdeel van opvoeden, niet van risicobeheersing door de overheid.

Daarom voelt een algemeen social mediaverbod of strikte leeftijdsverificatie voor alle jongeren disproportioneel. De praktijk laat zien dat miljoenen jongeren prima functioneren in een digitale wereld. Het bewijs dat een hele generatie hierdoor schade oploopt, ontbreekt — en het bewijs dat zij er juist goed mee om kunnen gaan, is overal zichtbaar.

Groeten Ronald

COLUMN NICOLE

In korte broek naar digitale onafhankelijkheid



Daar zat hij dan, naast me in de collegezaal in Den Haag: in korte broek, zoals beloofd. Bert Hubert was uit Nootdorp komen fietsen. Elektrisch, voor de nuance. Maar tegen deze hitte hielp ook dat niet. Normaal gesproken erger ik me aan mensen die overal opduiken om dezelfde boodschap te verkondigen. Maar voor Bert maak ik graag een uitzondering. Bert is namelijk een soort bedreigde diersoort. Hij doet niet aan fluf en hij fungeert als zeer effectieve bullshitfilter.

Een week na zijn keynote over digitale autonomie kwam het bericht vanuit de Tweede Kamer dat het kabinet wil gaan voor maximale digitale soevereiniteit. Volgens Gartner, die het kabinet een aantal scenario's voorschotelde, was dit scenario het meest kansrijk: een volledig nieuwe, centraal aangestuurde overheidscloud, los van de Amerikaanse cloudaanbieders waar we nu op leunen. Dat klinkt ongetwijfeld goed op papier en krijgt vast de handen op elkaar.

Maar lees je de kleine lettertjes, dan zie je al snel de barsten. Samenwerking met diezelfde markt? Niet uitgesloten. Hoe dat er precies uitziet: wordt nog uitgewerkt. En staatssecretaris Van der Burg zegt er zelf al bij dat het plan alleen kan slagen als genoeg overheidsorganisaties meedoen en hun eigen budget ervoor inzetten. Vertaling: de techniek is het probleem niet. Het containerplatform, de open standaarden, dat komt er heus wel. De vraag is of iedereen ook echt zijn gemak wil opgeven of in ieder geval verminderen.

Als ik dit plan afzet tegen de piramide die Bert die ochtend op het scherm toverde, valt dat op: het gaat niet over kunnen. Het gaat over echt willen. En centrale regie is het soort oplossing waarmee je doet alsof je het probleem aanpakt, zonder dat iemand zelf iets hoeft op te geven — tot het moment dat de rekening en het ongemak echt op tafel komen.

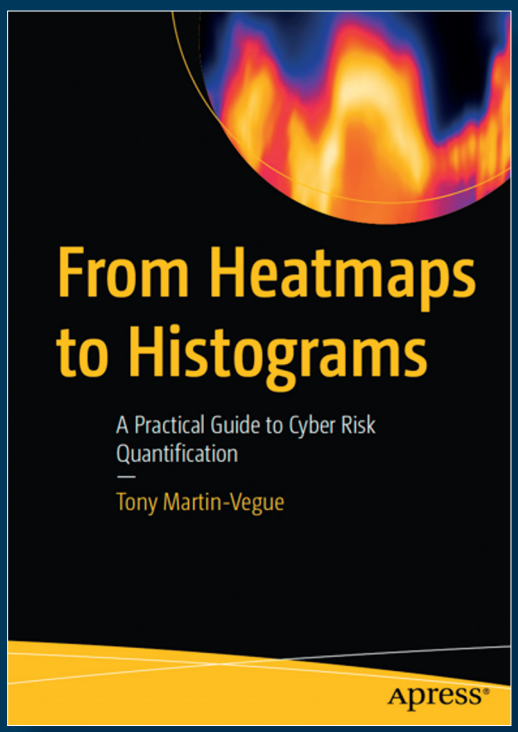
Don't get me wrong. Ik ben zelf zo iemand die nog compleet afhankelijk is, maar ik zeg niet dagelijks dat ik anders wil. Ik ken de risico's, maar neem ze voor lief, uit gemakzucht. De grap of de tragedie — net hoe je het bekijkt — is dat ik daarin niet alleen sta. Verschillende groepen hebben simpelweg geen zin in de verandering die een vertrek bij Big Tech met zich mee zou brengen. Ongemak is iets waar we steeds minder tolerantie voor lijken te hebben. Principes hebben doorgaans een kortere houdbaarheidsdatum dan een pak melk.

Wij willen wel, maar niet genoeg om tegen de stroom in te gaan zwemmen. We willen in airconditioning naar onze bestemming gebracht worden, in plaats van dat we door de hitte in korte broek fietsen en het ongemak van een bezweet t-shirt accepteren.

Bert deed dat laatste. Het kabinet kiest liever voor "wordt nog uitgewerkt." De vraag is niet of het kabinet een piramide — of een cloud — kan bouwen. De vraag is wie van ons bereid is om gewoon te gaan fietsen.

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

Reviewer: Nicole van Deursen, schrijft op persoonlijke titel en werkt als productmanager risicomanagement bij SURF, nicole.vandeursen@surf.nl



Titel boek: **From Heatmaps to Histograms**
A practical guide to cyber risk quantification
Auteur: Tony Martin-Vegue
ISBN: ISBN-13 (pbk): 979-8-8688-2299-5
ISBN-13 (electronic): 979-8-8688-2300-8
https://doi.org/10.1007/979-8-8688-2300-8

BOEKREVIEW

From Heatmaps to Histograms

In dit boek beantwoordt Tony Martin-Vegue precies de vragen waar ik al jaren op zit te broeden: hoe kun je op een op feiten gebaseerde en beleefde wijze uitleggen dat heatmaps beperkingen kennen bij het beschrijven van risico's? En hoe leg je stap voor stap uit hoe risico's te kwantificeren?

’Start where you are. Use what you have. Do what you can.’

De auteur heeft flink wat pagina's nodig om de lezer op te leiden in het zelf kwantificeren van cyberrisico's. Laat dit je, als moderne lezer die houdt van AI-gegenereerde samenvattingen, niet afschrikken! Val je in die categorie: lees dan in ieder geval het voorwoord (vanaf pagina xxii) en hoofdstuk 1. Daar bevindt zich een fundamentele boodschap: *`The distinction between qualitative and quantitative risk analysis isn't just methodological; it's philosophical'*, waarmee de auteur samenvat dat de filosofie: "dat risico's kunnen verdwijnen door beheersmaatregelen en compliance" een andere is dan het ondersteunen van besluitvorming door te werken met onzekerheden. De rol van risicomanagers is niet om allerlei onzekerheden weg te werken, maar om leidinggevenden te helpen bij het nemen van beslissingen, ondanks die onzekerheden. Onzekerheden horen erbij, het zijn geen problemen die je op moet lossen. Dat is een wezenlijk ander uitgangspunt dan dat wat de meeste organisaties gewend zijn. Het hele boek is trouwens ook aardig als je houdt van filosofische zinnen die het goed zouden doen als tegeltjeswijsheden. Neem bijvoorbeeld deze uitspraken: *'Uncertainty is not a bug in the system; it's a feature'* of *'The goal should never be to eliminate all risk, but rather to understand it'*.

In hoofdstuk 2 staat de historische uitleg hoe de benadering van risicoanalyses vanaf 1900 in verschillende richtingen is gaan lopen, waarbij het pad van managementtheorie de richting van kwalitatieve methodes is opgegaan en het pad van besluitvormingstheorie de kwantitatieve analyse doorontwikkelde. De risicomatrix of heatmap is een resultaat van prevalerend management-denken dat complexe systemen kunnen worden versimpeld, opgedeeld, gecontroleerd en beheerst. Echter, cybersecurityrisico's ontstaan uit complexe omgevingen en zijn onderling verweven in ecosystemen. Dat kun je niet 'platslaan', waardoor een matrix de verkeerde tool is.

Dit boek neemt je stap voor stap mee in het uitvoeren van kwantitatieve analyses met behulp van Excel. Je leert om verliezen en kosten te benoemen, waar je data vandaan kunt halen, je gaat forecasten en je doet een Monte Carlo-simulatie. Bovendien worden de cijfers ook weer in verband gebracht met hetgeen waarvoor je het doet: je management helpen een beslissing te nemen.

Bij de technische uitleg wordt regelmatig verwezen naar de bijhorende website waar je materiaal en oefeningen kunt downloaden. Daarnaast bevatten veel hoofdstukken AI-prompts om te ondersteunen bij de uitvoering. En ben je na dit alles nog niet klaar om de heatmap los te laten, in hoofdstuk 6 staat ook nog een voorbeeld van kwantitatieve toevoegingen op je geliefde matrix.

Hoofdstuk 13 en 14 gaan over twee concepten waardoor dit boek mijn favoriete boek van dit jaar is (nerd alert!): expert elicitation en Bayesian reasoning. Tony Martin-Vegue licht toe hoe je workshops met experts kunt inzetten om je data nog betrouwbaarder te maken. Want data zonder menselijke interpretatie is net niet genoeg. Ook beschrijft hij op een heel toegankelijke manier wat Bayesian reasoning is. Want wat je nu weet , is morgen anders. En met Bayes is de cirkel weer rond naar hoofdstuk 2, waarin de geschiedenis van kwantitatieve risicoanalyse werd beschreven vanaf het jaar 1654.

Ik hoop dat het boek mensen over de streep trekt om te gaan oefenen met kwantificeren van risico's en dat ze hun ervaringen delen. De auteur schrijft dat het kwantificeren van cybersecurity tegenwoordig mainstream is, maar ik ben bang dat er in veel organisaties nog wordt gedacht dat het te moeilijk is of dat er geen data is. Ik heb zelf lang gedacht dat kwantificeren vooral was weggelegd voor organisaties met veel ervaring met risicomanagement. Dat zie je ook terug in volwassenheidsmodellen zoals die van NBA-LIO/NOREA waar kwantificeren pas vanaf volwassenheidsniveau 3 wordt genoemd. Na het lezen van dit boek denk ik hier anders over. Je kunt vanaf je eerste analyse al meteen met cijfers aan de slag. Iedereen kan het leren en het staat los van de volwassenheid van je managementsysteem. Het vraagt wel enige inspanning om het te leren en om het continu te blijven verbeteren. AI kan je helpen, maar je moet het nog steeds wel zelf doen. Met de tijd worden jouw analyses steeds beter en zal het nut steeds zichtbaarder worden. Tot die tijd herhaal je dit mantra uit hoofdstuk 2: *'Start where you are. Use what you have. Do what you can.'* De rest zal volgen.



Recht in de doelgroep

100% veilig. 0% spam.

Uw merk, product of dienst onder de aandacht brengen bij dé professionals in de intersectorale branche?
IB-Magazine is hét betrouwbare platform met een sterke, betrokken lezerskring. Geen ruis, geen verspilling — alleen zichtbaarheid waar het telt.

Meer weten?
Mail naar ibmagazine@pvib.nl



INFORMATIEBEVEILIGING
MAGAZINE



VAN VERPLICHTING NAAR ACTIE: WORD NIS2-PROOF MET TRAININGEN

De NIS2-richtlijn stelt strengere eisen 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.

Security Academy - a DNV company: uw partner in cybersecurity, risicobeheersing en business continuity. Leer met praktijkgerichte trainingen alles wat u nodig heeft om te voldoen aan de NIS2.

Training	Locatie	Duur	Prijs
NIS2 Boardroomsessie	Woerden of eigen locatie	4 uur	op aanvraag
NIS2 Certified Professional	Woerden of online	2 dagen	€ 1.675
Lead Auditor ISO/IEC 27001	Verschillende locaties	5 dagen	€ 3.085
Crisis Management Foundation	Woerden of online	2 dagen	€ 1.647
Normkennis ISO/IEC 27001	Verschillende locaties	2 dagen	€ 1.125

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

SECURITY ACADEMY
a DNV company