Interview met Victor de Pous

Omvang IT-auditing domein groeit explosief en controle blijft cruciaal

14 december 2018

Wilfried Olthof

Al ruim dertig jaar bestaat de Special Interest Group IT en Recht binnen het Nederlands Genootschap van Informatici, tegenwoordig KNVI. De jurist Victor de Pous, medeoprichter en bestuurslid, boegbeeld van die organisatie, volgt de ontwikkelingen en thema's in het digitale domein voortdurend met scherpe blik. Wij kwamen met hem in contact bij de voorbereiding van onze IT-auditorsdag over 'Smart Cities', omdat hij ook over dit onderwerp al enkele studies publiceerde. Daarnaast houdt hij zich veelvuldig bezig met onder meer rechtsaspecten van privacy, cloud computing en software, zoals open source software maar ook 'sjoemelsoftware'. Denk aan de Volkswagenzaak. Hij ziet in zijn werk veelvuldig uitdagingen en kansen voor IT-auditors als 'kwaliteitsbewakers van de digitale samenleving'. Kortom, voldoende aanleiding voor een interview. We spreken elkaar in het Amsterdamse restaurant Dauphine.

Van welke kant komt het gevaar?

'Ik zie enkele majeure trends in de informatiemaatschappij die bijdragen aan het onveilige en onbetrouwbare karakter ervan. De voorbeelden zien we dagelijks in de pers. Commerciële bedrijven zoals Volkswagen, Cambridge Analytica, Facebook, maar ook overheden zoals de Russische geheime diensten FSB en GROe, maken zich schuldig aan malversaties en cybercrime. "De vijand komt uit het stopcontact", luidt een populaire oneliner van onder andere het Openbaar Ministerie, dat al drie jaar geleden een paradigmaverschuiving aankondigde met de verwachting dat in 2021 de helft van alle criminaliteit in ons land computergerelateerd is. Maar de digitale dreiging is breder dan computercriminaliteit.'

> *"De vijand komt uit het stopcontact"*

'Bij de digitale dreiging is de blik veelal beperkt tot beroepscriminelen en georganiseerde misdaad, terrorist of "statelijke actor" (buitenlandse geheime dienst). Het gaat daarbij echter om aanzienlijk meer dan "klassieke computercriminaliteit". Dieselgate heeft laten

zien dat sjoemelsoftware niet alleen wordt ingezet om de Nederlandse fiscus te misleiden via een afroomfunctie in kassasystemen. Een ander voorbeeld is het besturingssysteem Android, dat locatiegegevens registreert, ook wanneer gebruikers hebben aangegeven dit niet te willen. Facebook en onder meer Uber laten zien dat modern ondernemerschap juridisch ontwrichtend kan zijn. Anders gezegd: ook de "bovenwereld" mist deels respect voor rechtsnormen en *regulatory compliance*'.

'Er is een structureel gebrek aan digitale kwaliteit. Zo sterk als cybersecurity in de belangstelling staat in relatie tot computercriminaliteit, zo onderbelicht is doorgaans de aandacht voor (een tekort aan) algemene digitale kwaliteitsnormen. Een recente studie van ENISA, het Europese Agentschap voor Netwerk- en Informatiebeveiliging wijst op de gevolgen. Telecomstoringen in de Europese Unie worden in hoofdzaak veroorzaakt door softwarefouten en defecte hardware en niet door hackers of cyberaanvallen. Zelfs het weer blijkt een relevante storingsfactor. Daarnaast groeit de kwetsbaarheid door digitale afhankelijkheid. Individu, organisatie en maatschappij zijn in feite geheel afhankelijk geworden van de beschikbaarheid, goede werking en doorontwikkeling van de digitale technologie en de gegevensverwerking die daarmee kan plaatsvinden, met alle gevolgen van dien. Zo moest de Luchthaven Schiphol in de nacht van 29 april 2018 letterlijk haar deuren sluiten door de uitval van enkele informatiesystemen. Bovendien zijn we tegenwoordig nog afhankelijker geworden van digitale leveranciers, mede omdat gegevensverwerking in toenemende mate is uitbesteed, dankzij het eclatante succes van cloud computing. Daardoor veranderde ICT grotendeels van "een product" in (een bundeling van) diensten, vaak continu te leveren door derden.'

Welke ontwikkelingen werken onveiligheid in de hand?

'Om te beginnen wordt ICT telkens meer bijzonder. ICT betreft van oudsher ('Electronic Data Processing') en ten principale geautomatiseerde verwerking van gegevens, na het tijdperk van de mechanisatie van de gegevensverwerking. Tegenwoordig gebeurt dat met of, en in toenemende mate, zonder menselijke tussenkomt, inclusief *machine-to-machine* communicatie en andere zelfstandig werkende toepassingen die bovendien zelflerend van karakter kunnen zijn, voorzien van geavanceerde kunstmatige intelligentie op basis van enorme hoeveelheden gegevens uit verschillende bronnen (big data). Dat zijn fysieke apparaten, machines, voertuigen andere uniek identificeerbare objecten met ingebedde elektronica en netwerk-connectiviteit, waarmee in realtime gegevens kunnen worden verwerkt. Bij het Internet of Things (IoT) gaat het om de onderlinge verbinding van deze objecten, die in samenhang met digitale diensten autonoom fungeren als hulpmiddel of middel voor besluitvorming.'

> *Ik zie de IT-auditor als cruciale kwaliteitsbewaker*

'Een andere ontwikkeling die gevaren meebrengt is dat ICT meer dan ooit mede persoonlijke digitale technologie is geworden, in de vorm van pc, tablet, smartphone en andere devices en allerlei (software-)diensten (apps). In relatie tot nieuwe manieren van plaats- en tijdonafhankelijk werken, vertaalt deze trend zich ook in *bring-your-own-device*. Werknemers gebruiken voor hun arbeid digitale producten en diensten van de zaak, van zichzelf en van derden. Deze trend van "schaduw ICT" heeft twee onderbelichte, doch verstrekkende gevolgen voor ieder bedrijf of overheidsorganisatie: zowel de "aanschaf" van digitale technologie als de verwerking van de bedrijfsinformatie onttrekt zich aan zeggenschap en controle van het bestuur. Het overzicht waar welke gegevens en kopieën van bestanden zich bevinden ontbreekt, evenals het toezicht op de naleving van wettelijke en andere voorschriften, zoals contractuele afspraken en *business rules* per organisatie.'

Wat betekenen die ontwikkelingen voor digitale wet- en regelgeving en digitaal beleid?

'We zien een explosieve toename van digitale wet- en regelgeving. Voor digitale technologie is de laatste dertig jaar een even omvangrijk als uiteenlopende hoeveelheid bijzondere wet- en regelgeving tot stand gekomen, zowel uit Europa als uit Nederland in haar rol als autonome wetgever. Alles wat ICT betreft, is grosso modo extra, dat wil zeggen: aanvullend dan wel afwijkend, juridisch gecodificeerd, terwijl op de resterende onderwerpen in beginsel het algemene recht van toepassing blijft. De trend van de vergroting van de reikwijdte, het aanscherpen van eisen en de intensivering van regulering in het digitale domein zet zich onverkort voort.'

'Naast de overvloed aan bestaande en aankomende digitale wetgeving heeft Nederland, mede dankzij de ambities van het huidige kabinet Rutte III, geen gebrek aan digitaal beleid en dito voornemens. Na de Nationale Cybersecurity Agenda van 21 april 2018 met zeven stevige ambities en het Actieplan van Digitale Connectiviteit van 3 juni 2018 ligt er nu de Strategie Nederland Digitaal, die op 16 juni 2018 is gepubliceerd. Het gedachtegoed laat zich grof samenvatten als: ICT geldt nog altijd als onvolprezen as van innovatie, ongeacht sector. Cybersecurity vormt hiervan een belangrijk onderdeel. Uit het Regeerakkoord (2017-2021, Vertrouwen in de toekomst) blijkt dat het kabinet bedrijven wil stimuleren om veiliger software te maken via een nieuwe vorm van juridische aansprakelijkheid – een opmerkelijke maatregel die zich overigens beperkt tot veiligheidsaspecten.'

> *Controle blijft in alle gevallen essentieel*

En de private sector?

'In een rapport van 2012 legt branchevereniging Nederland ICT de oorzaak van het gebruik van "onveilige software" (mede) bij de klant. Er kan best veilig worden ontwikkeld, zo stelt de branchevereniging, maar als afnemers hier niet voor kiezen gebeurt er niets. In november 2017 publiceerde ECP.nl, Platform voor de Informatiemaatschappij, een "twintig-bouwstenen-actieplan" waarin wordt vastgesteld dat de veiligheid in de keten van leveranciers wordt gerealiseerd door een "roadmap" voor secure software. Kwetsbaarheden in software worden opgelost door zelfregulering en samenwerking tussen gebruikers en leveranciers. Kortom, de meningen zijn sterk verdeeld.'

Welke kansen biedt dit alles de IT-auditor?

'Elk van deze trends en ontwikkelingen biedt afzonderlijk al aanknopingspunten voor het werk van de IT-auditor. Enerzijds is de omvang van het IT-auditing domein explosief gegroeid, zowel door de zee van digitale regulering en de schaalgrootte van het gebruik van digitale technologie. Anderzijds noteren we tegelijkertijd een verbreding door middel van diversiteit van de regulering en nieuwe ICT-toepassingen, bijvoorbeeld bij de inzet van het samenhangende algoritme-gedreven trio IoT, big data en kunstmatige intelligentie. Van belang is nog de constatering dat de wijze waarop er wordt gereguleerd, in beginsel voor de IT-auditor niet of nauwelijks relevant is. Het maakt immers niet uit of er in Europa een verplichte (veiligheids)certificering voor IoT-apparaten komt, zoals Nederland voorstaat.'

'Hetzelfde geldt ten aanzien van de stimulans voor de productie van veilige software: zelfregulering, zoals de sector graag wil, tegenover een nieuw bijzonder aansprakelijkheidsregime voor gebrekkige computerprogramma's, volgens de kabinetsplannen. Controle blijft in alle gevallen essentieel. Op verschillende wijze kunnen er voor de beroepsgroep van IT-auditors nieuwe kansen worden geïdentificeerd. Het voldoen aan wet- en regelgeving (*regulatory compliance*) per individuele regulering of voor clusters van regulering biedt op zich voldoende aanknopingspunten. Een andere optie betreft het ontwikkelen van frameworks per generiek bedrijfsproces of bedrijfstak. En vergeet het overheidsbeleid niet: Het kabinet wil op verantwoorde wijze de maatschappelijke en economische kansen van digitalisering optimaal benutten met Nederland als pionier en proeftuin op dit gebied (zie strategie Nederland Digitaal). Ook dit beleid kan als startpunt worden genomen voor de onvermijdelijke IT-auditing. Kort samengevat: ik zie de IT-auditor als cruciale kwaliteitsbewaker.'

De belangrijkste wet- en regelgeving die eraan komt

Een, niet volledig, overzicht van wet- en regelgeving uit Europa en Nederland die in 2019 in werking treedt of nog op de tekentafel ligt, verzameld door Victor de Pous en opgenomen in zijn jaarlijkse Outlook digitaal recht, die in januari verschijnt.

Wet- en regelgeving: vanuit de Europese Unie

- Europese Richtlijn betaaldiensten 2
- Wetsvoorstel Implementatiewet herziene richtlijn betaaldiensten
- Europese Richtlijn netwerk- en informatiebeveiliging
- Wetsvoorstel beveiliging netwerk- en informatiesystemen
- Europese Richtlijn PNR-gegevens
- Wetsvoorstel gebruik passagiersgegevens
- Europese Richtlijn gegevensbescherming opsporing en vervolging
- Wetsvoorstel gegevensbescherming opsporing en vervolging
- Voorstel Europese Richtlijn auteursrechten in de digitaal eengemaakte markt
- Voorstel Europese e-Privacy Verordening
- Voorstel Europese Verordening vrij verkeer niet-persoonsgebonden gegevens
- Voorstel Europese Verordening ICT cybersecurity certificering
- Voorstel Europese Verordening biometrie op identiteitskaarten
- Voorstel Beleidsregel Netwerkaansluitpunt
- Wetsvoorstel implementatie artikel 1 richtlijn elektronische handel

Wet- en regelgeving: Nederland als autonome wetgever

- Aanpassing Grondwet: telecommunicatiegeheim
- Wet computercriminaliteit III
- Wet vastleggen en bewaren kentekengegevens door politie
- Wet experimenteerwet zelfrijdende auto's
- Wetsvoorstel register onderwijsdeelnemers
- Wetsvoorstel kansspelen op afstand
- Wetsvoorstel digitale overheid
- Wetsvoorstel modernisering elektronisch bestuurlijk verkeer
- Wetsvoorstel aanpassing bewaarplicht telecommunicatiegegevens
- Wetsvoorstel ongewenste zeggenschap telecommunicatie
- Wetsvoorstel open overheid
- Wetsvoorstel overstap telecommunicatie-eindgebruikers
- Voorstel regulering cryptovaluta
- Voorstel Besluit smartphone-verbod in het verkeer
- Aanscherping rechtspositie consument in digitale economie
- Wetsvoorstel aansprakelijkheid onveilige software
- Wetsvoorstel modernisering Archiefwet
- Wetsvoorstel gebruik ANPR-gegevens Belastingdienst

Drs. W. (Wilfried) J.A. Olthof | Directeur bij *NOREA*

Wilfried Olthof is directeur van NOREA en heeft daarvoor functies vervuld bij de Perscombinatie, het ministerie van VROM en de Vrije Universiteit Amsterdam. Hij heeft Politicologie en Bestuurswetenschappen gestudeerd.