#2

SAI UPDATE

DIGITAAL TIJDSCHRIFT VOOR SAI-LEDEN | MEI 2020 | SAI

DE IMPACT VAN COVID-19 OP IT

En verder:
DOE MEE AAN DE QUIZ | NEGEN TOEKOMSTIGE FUNCTIES IN INFORMATIEBEVEILIGING | DE BELOFTE VAN QUANTUMCOMPUTING

VIJF CRUCIALE VRAGEN
OVER 5G
pag. 14

TWEE JAAR GDPR:
VAN WAAR KOMT DE WIND?
pag. 25

HOE ETHISCH IS
ARTIFICIAL INTELLIGENCE?
pag. 8

EDITO

Beste SAI-lid en lezer,

Welkom bij deze tweede editie van jullie SAI-magazine. Niemand zal betwisten dat dit bijzondere tijden zijn, met een enorme impact op ons allemaal, zowel privé als professioneel. Zo ook op SAI. Onze laatste traditionele SAI-avondconferentie vond plaats op 5 maart in Antwerpen. Sindsdien konden onze avondconferenties en workshops niet meer plaatsvinden op de traditionele manier en dat was logisch en volledig verantwoord. Zonder problemen vonden we onze sprekers bereid om hun geplande sessie volledig digitaal te geven op een andere datum tijdens de werkuren en ingekort tot één uur. Deze aanpassingen werden door jullie gesmaakt. Onze workshops kunnen wellicht pas na de zomervakantie weer opstarten met de nodige voorzorgsmaatregelen. Hierover later meer nieuws via onze website ***www.sai.be***.

Deze coronacrisis heeft ICT duidelijk en op een positieve manier op de voorgrond geplaatst. Digitalisering zal alleen maar versnellen. Hoe erg deze crisis ook is, wie vooruitkijkt en digitaal handelt, heeft het bij het rechte eind. De digitale revolutie heeft sinds 1998 het economische landschap compleet hertekend. Zowel het gedrag van consumenten, de samenstelling van beurzen als de werking van organisaties zijn enorm beïnvloed en worden nog altijd verder getransformeerd.

E-commerce barst meer dan ooit internationaal en lokaal uit zijn voegen, net als platformen voor videoconferencing zoals Microsoft Teams, Zoom en Jitsi. Studenten en leerlingen migreren massaal naar online onderwijsplatformen zoals Smartschool, Bingel en Diddit. Netflix, Fortnite, Twitter en YouTube zijn nog nooit zo populair geweest.

Wie de digitale revolutie tot op heden al spannend vond, zet zich best schrap want er komen nog veel meer digitale innovaties en allerlei hybride transformatiemodellen op ons af. Hopelijk zitten daar ook heel wat Belgische succesverhalen bij.

Organisaties en sectoren die echter nog niet stevig op de digitalisering hadden ingezet, kregen sinds maart 2020 een zware rekening gepresenteerd. Zij zitten in zeer moeilijke papieren en het is niet zeker dat ze het einde van 2020 halen. Wendbare organisaties die snel inspeelden op deze coronacrisis door hun product of businessmodel aan te passen en door nieuwe klanten te zoeken, verwerven momenteel een groter marktaandeel en draaien op volle toeren. Hen zul je niet horen klagen.

Ten slotte wordt het traditionele kantoormodel volledig in vraag gesteld. Werkgevers die denken dat werknemers na deze coronacrisis weer maximaal één dag telewerk per week zullen aanvaarden, zullen geconfronteerd worden met hoogoplopende interne discussies en zelfs vertrek van hun talenten naar organisaties met een flexibelere telewerkregeling. Daarmee staat het belangrijkste feit van deze crisis als een paal boven water. Directies en werknemers wereldwijd zullen het nieuwe mantra moeten erkennen: het is digitaliseren of verdwijnen. SAI is paraat om hieraan actief mee te werken op de wijze zoals SAI dit al meer dan vijftig jaar doet: door praktisch bruikbare ICT-kennis voor alle leden uit te wisselen.

Intussen wens ik u en uw familie een uitstekende fysieke en mentale gezondheid toe en veel digitaal werkplezier.

Marc Vael
Voorzitter raad van bestuur SAI

INHOUD

“

AI IS EEN KRACHTIG WAPEN, MAAR JE MOET DE GEBRUIKS-AANWIJZING GRONDIG LEZEN.

JOACHIM GANSEMAN
ONDERZOEKER BIJ SMALS RESEARCH

PROGRAMMEERTAAL VOOR KINDEREN HAALT TOP TWINTIG

C is de populairste taal in de top twintig van programmeertalen. Maar het meest opvallende is de opmars van Scratch, bedoeld om kinderen te leren programmeren.

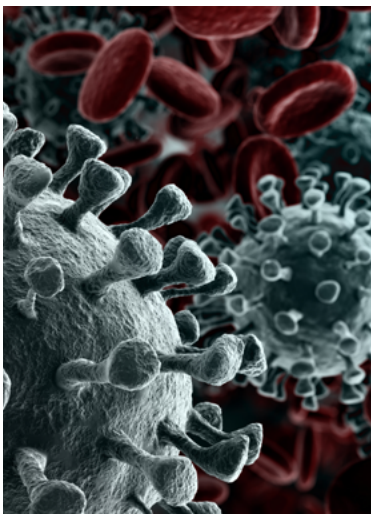
In de TIOBE-programmeerindex blijken C, Java en Python de meeste vooraanstaande programmeertalen. De meeste aandacht gaat naar Scratch, de graphical block-based programmeertaal voor kinderen. Scratch staat namelijk op plaats 19, vorig jaar was dat nog 27. Het is daarmee een van de grootste stijgers in de lijst, samen met R, Swift, Go en PL/SQL. Volgens Paul Jansen, CEO van TIOBE Software, zijn er in totaal meer dan vijftig miljoen projecten 'geschreven' in Scratch. Elke maand worden er een miljoen nieuwe Scratch-projecten toegevoegd.

Mei 2020	Programmeertaal	*Mei 2019*
1	C	*2*
2	Java	*1*
3	Python	*4*
4	C++	*3*
5	C#	*6*
6	Visual Basic	*5*
7	JavaScript	*7*
8	PHP	*9*
9	SQL	*8*
10	R	*21*
11	Swift	*18*
12	Go	*19*
13	MATLAB	*14*
14	Assembly language	*10*
15	Ruby	*15*
16	PL/SQL	*20*
17	Classic Visual Basic	*16*
18	Perl	*13*
19	Scratch	*28*
20	Objective-C	*11*

Opvallend is ook dat C in deze editie Java inhaalt als nummer één. "Een van de redenen zou het coronavirus kunnen zijn", oppert Paul Jansen. "Sommige programmeertalen hebben er echt baat bij. Voorbeelden zijn Python en R op het gebied van de datawetenschappen, omdat iedereen op zoek is naar een tegengif voor het virus. Maar ook embedded-softwaretalen zoals C en C++ winnen aan populariteit omdat die gebruikt worden in software voor medische apparatuur."

De TIOBE-programmeerindex is een bekende indicator voor de populariteit van de programmeertalen. De beoordelingen zijn gebaseerd op het aantal geschoolde ontwikkelaars wereldwijd, cursussen en externe leveranciers. Naast TIOBE zijn er overigens nog indexen die een andere aanpak hanteren en daardoor vaak andere talen, zoals Python en Javascript, hoger doen eindigen.

“BINNEN ZES MAANDEN KOMT GROOTSTE CYBERATTACK OOIT”



Het coronavirus legt de basis voor een massale cyberaanval. “We zullen de komende zes maanden de grootste aanval in de geschiedenis zien”, is de voorspelling van Stephen McBride, chief analyst bij onderzoeksbureau RiskHedge.

Het coronavirus heeft, zo oppert McBride in zakenblad Forbes, de virtuele verdediging van elk bedrijf opengebroken. “Hoe meer apparaten op een netwerk zijn aangesloten, hoe groter het aanvalsoppervlak wordt. Daardoor kunnen hackers gemakkelijker in het netwerk infiltreren.”

Voordat de pandemie toesloeg, kregen werknemers die op afstand werkten meestal speciale werklaptops met aangescherpte beveiliging. Maar nu hadden bedrijven slechts enkele dagen de tijd om hun plannen op afstand in elkaar te flansen. “Je kunt er zeker van zijn dat de meeste geen beveiligde systemen hebben opgezet. Honderden miljoenen medewerkers gebruiken persoonlijke laptops op onbeveiligde internetverbindingen thuis. Zo krijgen ze toegang tot – vaak vertrouwelijke – werkbestanden. Dit is een droom voor cybercriminelen. Ze kunnen via één toegangspunt de controle over een heel netwerk in handen krijgen.”

WAT ZIJN JOUW UITDAGINGEN IN CYBERBELEID?

Budget en skills (en het gebrek eraan), samen met complexiteit en culturele weerstand. Dat zijn volgens SAI-leden de grootste uitdagingen voor een organisatiebrede cybersecurity-aanpak.

Dat bleek tijdens een onlinepoll op het SAI-webinar over het *Cyber Target Operating Model of the Future*. Andrea Radu, Maarten Mostmans, respectievelijk director Cyber en partner Cyber bij Deloitte, gaven er hun visie over het wat, hoe en waarom van hun model.

Zo'n *Cyber Target Operating Model* (TOM) maakt niet alleen een cyberstrategie mogelijk, het vergroot ook het vermogen van een organisatie om binnen een aanvaardbare risicobereidheid te opereren, terwijl het de blootstelling aan cyberaanvallen helpt te verminderen. Dit door de opbouw en governance van cybercapaciteiten binnen de organisatie terwijl je de juiste mensen erbij betrekt.

Naast de SAI-deelnemers haalde Deloitte zelf nog enkele andere uitdagingen aan waarmee bedrijven te maken hebben bij de uitrol en het beheer van zo'n *Cyber TOM* en dus eigenlijk bij een cyberaanpak in het algemeen. Die gaan over drie domeinen:

UITDAGINGEN OP HET VLAK VAN DE SERVICECATALOGUS

- De reikwijdte van de securityservices omvat niet het bedreigingslandschap
- *One size fits all*-benadering van services
- Cyberservices en -functies zijn niet duidelijk gedefinieerd
- Geen duidelijk inzicht in de effectiviteit van de cyberservices
- Cyberservices zijn niet ingebed in de business

UITDAGINGEN OP HET VLAK VAN ORGANISATIE

- Overlappende verantwoordelijkheden over cyberservices
- Cyberdiensten worden geleverd vanuit verschillende delen van de organisatie
- Onduidelijke rollen en verantwoordelijkheden
- Gebrek aan samenhang en eenheid in het bereiken van de cyberstrategie
- Onduidelijke afbakening tussen de eerste en tweede verdedigingslinie
- Gebrek aan middelen en vaardigheden om de cyberdiensten te leveren
- *Single points of failure*
- Geen duidelijke verantwoording voor cybersecurity in de organisatie
- Gebrek aan leiderschap om de cyberstrategie uit te voeren

UITDAGINGEN OP HET VLAK VAN GOVERNANCE

- Cyberprestaties worden bij geen enkel bestuursorgaan van de organisatie besproken
- Gebrek aan een gemeenschappelijke governancestructuur voor de uitvoering van cyberinitiatieven en -programma's
- Gebrek aan focus en prioritering voor cyberinitiatieven
- De besluitvorming over strategische initiatieven gebeurt vaak op operationeel niveau
- Werken in silo's
- De business maakt geen deel uit van de cybergovernance

» *Herbekijk dit SAI-webinar op:* ***https://sai.be/event/14714***

CLOUDMARKT GROEIT MET EEN DERDE, DANKZIJ (EN ONDANKS) COVID-19

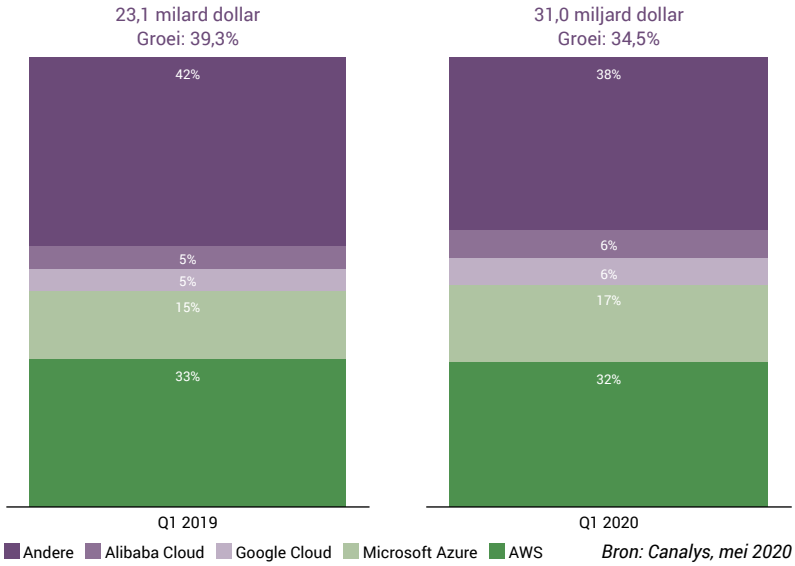
De uitgaven voor cloudinfrastructuurdiensten bereikten in het eerste kwartaal van 2020 opnieuw een record, met een groei van 34 procent tot 31,0 miljard dollar.

De groei in clouddiensten werd gedreven door organisaties over de hele wereld die overstapten naar afstandswerken als gevolg van de COVID-19-pandemie. Door de bijhorende lockdowns zochten bedrijven naar snelle toegang tot compute resources. Meer vraag naar online samenwerkingstools, e-commerce en clouddiensten voor consumenten leidde tot een sterke toename van het verbruik van cloudinfrastructuur, waarvan alle grote cloudaanbieders profiteerden. “Cloud is een essentieel instrument geworden om de bedrijfscontinuïteit in deze moeilijke tijden te ondersteunen”, aldus Alastair Edwards, chief analyst bij Canalys.

GROEI ONDANKS CORONA

Tegelijk werd deze groei afgezwakt door een vertraging in grote, complexe bedrijfsmigraties en transformation-projecten, omdat bedrijven zo goed als alle IT-taken een halt toeriepen toen de lockdowns begonnen. Cloudproviders voelden ook de negatieve impact van een vertraging in grote consulting-geleide projecten, waaronder SAP-migraties en hybride cloudimplementaties en andere projecten die een grote impuls hebben gegeven aan de groei van de cloud in de afgelopen kwartalen. De cloudinvesteringen in de zwaarst getroffen verticale segmenten, zoals horeca, luchtvaart, toerisme en industrie, werden afgebouwd of vertraagd. Dit alles deed een deel van de kortetermijngroei in de loop van het kwartaal teniet.

WERELDWIJDE UITGAVEN CLOUDINFRASTRUCTUURDIENSTEN



Bron: Canalys, mei 2020

SAI-EVENT: BESTE CYBERSECURITYFILM ALLER TIJDEN

Op 27 mei om 11.00 uur houdt SAI, samen met het vakblad Computable, een virtueel event. We gaan op zoek naar de allerbeste Hollywood-film over cybersecurity.

Marc Vael, voorzitter van de raad van bestuur van SAI, zal tijdens dat virtuele evenement de shortlist van tien films bekendmaken en bespreken. Marc schreef hierover onlangs het boek Informatieveiligheid en cybersecurity duiden via film. De tien besproken films behandelen één specifiek thema rond informatiebeveiliging en cybersecurity, met telkens heel wat praktische tips en kernboodschappen voor IT- en zakenmensen.

» *Inschrijven kan hier:* ***https://sai.be/event/15037***

» *Stemmen voor je favoriete securityfilm kan* ***hier***

WAT DOET COVID-19 MET HET DATA-UNIVERSUM?

Meer dan 59 zettabytes aan digitale data zullen dit jaar wereldwijd gecreëerd, gecaptured, gekopieerd en geconsumeerd worden. De COVID-19-pandemie draagt bij tot dit cijfer door toenemend thuiswerk en videogebruik.

Dat blijkt allemaal uit de jongste Global DataSphere van onderzoeksbureau IDC. Die meet hoeveel data elk jaar in de wereld gecreëerd en verbruikt worden in de wereld. Voor de komende vijf jaar mikt IDC op een jaarlijkse datagroei (CAGR) van 26 procent. Daar zijn verschillende verklaringen voor.

1/ MEER GEREPLICEERDE DATA

Terwijl COVID-19 de creatie van nieuwe unieke data belemmerde, heeft het toegenomen verbruik van gerepliceerde data de voortdurende groei van de Global DataSphere aangewakkerd.

De verhouding tussen unieke data (gemaakt en gecaptured) en gerepliceerde data (gekopieerd en geconsumeerd) is ongeveer één op negen, maar de trend is een langzame migratie naar minder unieke en meer gerepliceerde data. Tegen 2024 verwacht IDC dat deze verhouding één op tien zal bedragen.

2/ IMPACT VIDEO

Productiviteitsdata vormen de snelst groeiende datacategorie. Tegen 2024 zullen de productiviteitsdata 29 procent van de Global DataSphere bedragen en de entertainmentdata 40 procent. “We leven in een wereld die steeds meer gebruik maakt van video en we consumeren elk jaar meer en meer entertainmentvideo’s”, klinkt het bij IDC. Tegelijk maken we voor onze productiviteit gestaag gebruik van de videodata die we vastleggen, wat bijdraagt tot de groei van de productiviteitsdata in de DataSphere.

3/ MEER DATA IN DRIE JAAR DAN IN DERTIG JAAR

De hoeveelheid gegevens die in de komende drie jaar worden gecreëerd, zal groter zijn dan de gegevens die in de afgelopen dertig jaar zijn gecreëerd. “De Global DataSphere wordt meer en meer bepaald door de exponentiële groei van data die we telkens opnieuw verwerken en kopiëren”, besluit David Reinsel, senior vice president van IDC’s Global DataSphere.

DE DATASPHERE BEDRAAGT

59.000.000.000.000.000.000 bytes (of $59x10^{21}$)

IN 2020

Ter vergelijking: in 2016 schatte IDC het totale aantal gegenereerde data op 16.1 zettabytes.

JOACHIM GANSEMAN, ONDERZOEKER BIJ SMALS RESEARCH

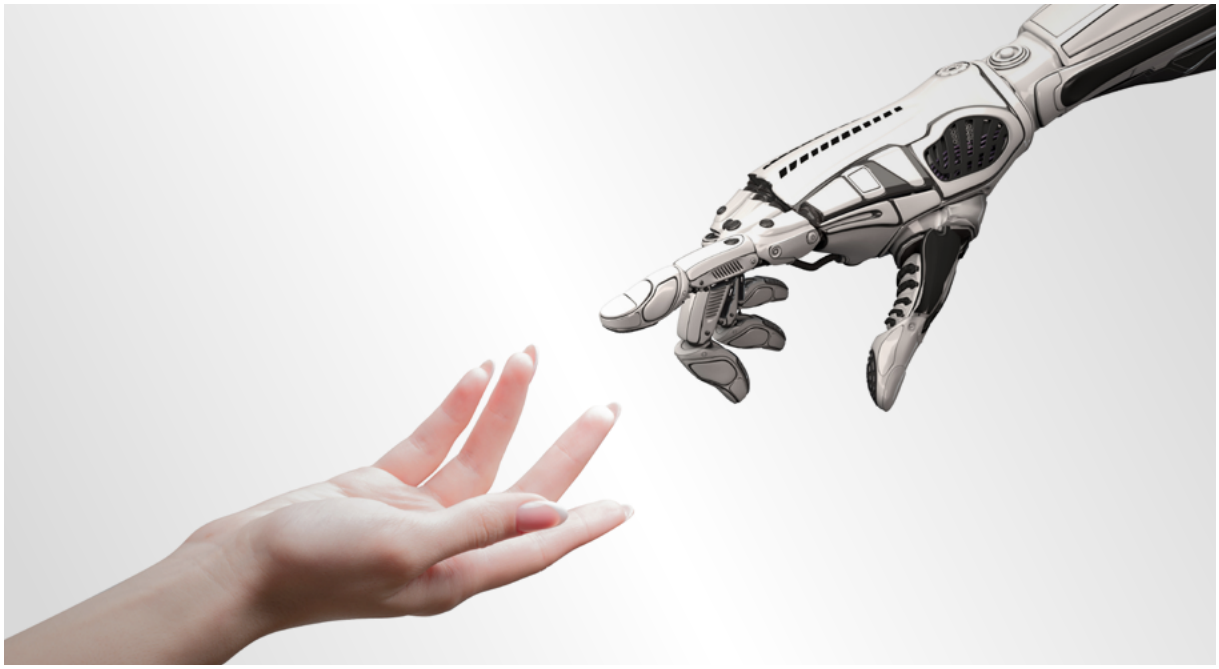
"AI IS EEN KRACHTIG WAPEN, MAAR JE MOET DE GEBRUIKSAANWIJZING GRONDIG LEZEN"

Artificial Intelligence blijft een technologie met bijzonder veel potentieel, waar velen – ook in deze tijden van diepe crisis – bijzonder veel van verwachten. Maar er bestaat ook veel argwaan, met name over het ethische aspect van deze technologie. Terecht of niet? Leidt het gebruik van AI tot inbreuken op de privacy, discriminatie en andere vormen van misbruik? En zo ja, wat kunnen we eraan doen? We legden het voor aan Joachim Ganseman, onderzoeker bij Smals Research.

Is AI echt onethisch?
Joachim Ganseman: "Een technologie op zich kan natuurlijk niet onethisch zijn, maar ze kan wel tot ethisch bedenkelijke toestanden leiden. Dit kan het gevolg zijn van bewust misbruik van AI, denk maar aan spammers die AI gebruiken om spamfilters te omzeilen of de vele vormen van fake news en deepfake video's. Ook de vele complottheorieën die vandaag rond het coronavirus circuleren, gebruiken vaak AI. Maar evengoed kan het veroorzaakt worden door een ondoordacht gebruik van data en algoritmes."

Kun je enkele voorbeelden geven van een fout gebruik van data en algoritmes met ethisch bedenkelijke gevolgen?
"Je kunt allerlei voorbeelden bedenken, van ronduit slechte databases die tot totaal onbetrouwbare resultaten leiden, tot

Joachim Ganseman:
"Een technologie op zich kan natuurlijk niet onethisch zijn."



onvoldoende gespreide trainingdata. Er zijn voorbeelden gekend van gezichtsherkenningsoftware die totaal de mist inging omdat alleen was getraind op gezichten in en rond Silicon Valley, waardoor de software niet bruikbaar was om Afro-Amerikaanse gezichten te herkennen. Het kan ook het gevolg zijn van onbewuste vooroordelen. Het bekendste voorbeeld is Amazon: de AI die werd gebruikt in hun selectieproces bleek vrouwen te benadelen en werd dus afgevoerd als mislukte software. Maar eigenlijk weerspiegelde die exact de selectiecriteria die Amazon ook zonder AI hanteerde en kwam deze wantoestand dankzij AI eindelijk aan het licht. Een onverwacht heilzaam effect van AI dus."

Hoe voorkom je dat er fouten sluipen in je AI?

"Er zijn enkele vuistregels. Eén: maak je AI-team zo divers mogelijk, in geslacht, leeftijd, afkomst enzovoort. Zo voorkom je zo veel mogelijk onbewuste vooroordelen bij het samenstellen van je dataset en algoritmes. Als je een idee wilt hebben van wat voor onbewuste vooroordelen er allemaal bestaan, moet je gewoon eens kijken op ***https://en.wikipedia.org/wiki/List_of_cognitive_biases***. Ze zijn niet allemaal van toepassing voor AI, maar het geeft je wel een idee hoe ons onderbewustzijn met ons aan de haal kan gaan.

Twee: voorzie voldoende controlemomenten, zeker aan het begin van de cyclus. Hoe eerder je een fout resultaat ontdekt, hoe eerder je kunt ingrijpen en hoe goedkoper het oplossen van de fout. Drie: maak je programma's en data zo transparant mogelijk, voor iedereen. Hoe meer mensen inzage krijgen in de data en het proces achter een bepaalde beslissing van AI-software, hoe groter de kans dat bepaalde, al dan niet bewuste, wantoestanden worden blootgelegd."

Maar wat doe je tegen bewust misbruik van AI?

"Dat is nog moeilijker te controleren natuurlijk. De voorbeelden van deepfake video's waarbij iedereen, van Obama tot VRT-nieuwsankers, digitaal kan worden 'misbruikt' voor valse boodschappen, zijn voldoende gekend. De video's worden ook alsmaar overtuigender, zodat je niet meer weet wat je mag geloven. Binnen de openbare omroep VRT hebben ze zelfs een factcheckteam ingezet om hiernaar op zoek te gaan. Misschien zijn overheden op dat vlak nog niet proactief genoeg, omdat het erg arbeidsintensief is en de allerbeste onderzoekers vergt. Wel op Europees niveau: daar hebben ze de erg nuttige pagina ***https://euvsdisinfo.eu*** opgericht, vooral gericht op wat Rusland allemaal uitspookt, sinds hun bemoeienissen in Oekraïne enkele jaren geleden."

Als we dit allemaal horen, lijkt het alsof we AI beter zouden bannen.

"Integendeel! AI is een krachtig wapen, zowel voor slechte als voor goede toepassingen. Maar je moet wel de gebruiksaanwijzing grondig lezen en toepassen. Als je weet wat er allemaal fout kan gaan, dan heb je al een eerste stap in de goede richting gezet. Voorts raad ik iedereen aan om betrouwbare en gezaggevende bronnen te raadplegen, zoals het ***Kenniscentrum voor Data en Maatschappij***, met praktische tools voor onder meer risicoanalyses, en de richtlijnen van de ***Europese Commissie voor ethiek in AI***. Veel succes en ... hou het ethisch!"

AI 4 GOOD

DE SPELREGELS VOOR ETHISCH VERANTWOORD INNOVEREN

Ook de Vlaamse Dienst voor Arbeidsbemiddeling en Beroepsopleiding (VDAB) gebruikt al al verscheidene jaren AI. Eén van de resultaten kun je nu al bewonderen op www.vdab.be: de jobsuggesties die je voorgeschoteld krijgt op basis van wat anderen met een gelijkaardig profiel interessant vinden. Nog voor Gartner enkele jaren geleden 'ethische AI' als één van de belangrijkste nieuwe trends identificeerde, was VDAB al actief aan het nadenken over de spelregels om geautomatiseerde intelligentie te ontwikkelen, verduidelijkt Guido Van Humbeeck, Directeur Architectuur & Innovatie bij VDAB. "Het is dus niet toevallig dat onze DPO (Data Privacy Officer) zetelt in de werkgroep die de ***'European Guidelines for Trustworthy AI'*** opstelt.

DRIE COMPONENTEN

Volgens de Europese Commissie zijn dit de drie basiscomponenten voor betrouwbare AI:

1. Het moet wettelijk zijn, dus beantwoorden aan de heersende wetten en regels overal waar de AI wordt ingezet.

2. Het moet ethisch zijn, dus voldoen aan de heersende ethische principes en waarden.

3. Het moet technisch en sociaal gesproken robuust zijn, want zelfs goed bedoelde AI kan nog veel ongewilde schade toebrengen.

Guido Van Humbeeck, Directeur Architectuur & Innovatie bij VDAB: "Het is niet altijd duidelijk wat ethisch de beste oplossing is."

Deze componenten worden praktisch vertaald in vereisten, zoals auditeerbaarheid, transparantie en aansprakelijkheid. Toch is dit alles nog geen garantie op 'ethisch verantwoorde' AI. "Het is ook niet altijd duidelijk wat ethisch de beste oplossing is", verklaart Guido Van Humbeeck. "Behandel je iedereen gelijk of geef je iedereen evenveel kansen op succes? We weten dat dat niet altijd hetzelfde is."

IN DE PRAKTIJK

Om de ethische waarde van zijn AI zo goed mogelijk te garanderen en om vooroordelen maximaal te vermijden, gaat VDAB in drie fasen te werk:

- **De experimentele fase:** bias awareness bij de data scientists: de data scientist is vrij in het gebruik van data in haar/zijn zoektocht naar een mogelijke oplossing voor een geïdentificeerde uitdaging. Enkele basistesten op data moeten bias voorkomen.

- **De verkennende fase**, formele bias-checks: in functie van het te bouwen model worden de data gecheckt op mogelijke bias. De resultaten die uit het model komen, worden ook aan bias-checks onderworpen.

- **De uitvoeringsfase**, Model Monitoring waarin wordt gewaakt over mogelijke wantoestanden wanneer de AI-toepassing op grotere schaal wordt ingezet, zowel op data, model als modelgebruik.

Elk van deze fasen wordt uitgewerkt in deeltaken. Doorheen het hele traject wordt altijd gedacht aan nauwgezette monitoring van de ingezette modellen, zodat een mogelijke wantoestand door foute beslissingen of vooroordelen zo snel mogelijk wordt geïdentificeerd. "Dit gebeurt allemaal onder een zorgvuldig samengestelde 'ethische raad' met zowel innovatie-experts als externe ethische experts en onze Data Privacy Officer aan het hoofd, als liaison met de CEO en zijn raad van bestuur.
Zo krijgen we een duurzame werking gebaseerd op ethisch verantwoorde innovatie", besluit Guido Van Humbeeck.

VAN IAAS TOT SERVERLESS: WAT DOE JE ZELF?

VIJF TINTEN CLOUD

Vroeger was het eenvoudig. Je infrastructuur stond gewoon on premise bij jou en jij stond als IT-verantwoordelijke voor alles in. Maar in de cloud zijn er meer gradaties. We overlopen de belangrijkste vormen én de verantwoordelijkheid van de klant.

"In IT en cloud geldt meer en meer het principe *you build it, you run it*. Het team dat de toepassingen ontwikkelt, is ook het team dat verantwoordelijk is voor de uitvoering en ondersteuning", opent Michael Willemse, managing partner en cloud solution architect bij Cloudway, als we met hem het luik van de klantenverantwoordelijkheid en het klantenbeheer in de cloud overlopen. Voor alle duidelijkheid: het gaat bij dit overzicht over het rekenkundige aspect van cloudoplossingen.

Ook SaaS of Software as a Service is een bepaalde cloud-tint en vaak de eerste waarvoor bedrijven opteren, al ligt de klemtoon in dit artikel op vier andere soorten. "De focus ligt hierbij ook op custom development", vertelt Willemse. Of hoe applicaties en infrastructuur steeds dichter naar elkaar zijn toegegroeid. We overlopen de verschillende soorten, op basis van de aanpak bij grote cloudproviders.

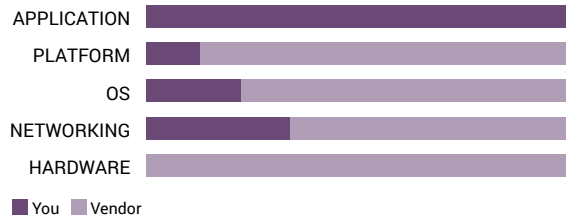
1/INFRASTRUCTURE AS A SERVICE (IAAS)

"Bij deze vorm nemen we als klant abstractie van de hardware. De focus ligt voor de klant op de compute en networking stack met virtualisatie en software defined networking. De splitsing van de verantwoordelijkheid gebeurt bij IaaS op netwerk- en OS-niveau", stelt Michael Willemse. "Het schalen gebeurt door virtuele machines toe te voegen of te verwijderen", stelt hij.

Prijsmodel: *pay per hour or second, met optionele verbintenis*
Voorbeelden: *Amazon Elastic Cloud*

2/PLATFORM AS A SERVICE (PAAS)

Platform as a Service is een categorie van cloud-computingdiensten waarbij klanten via een platform hun applicaties kunnen ontwikkelen, uitvoeren en beheren. "En dit zonder zich te bekommeren om de complexiteit van het bouwen en onderhouden van de infrastructuur die daar gewoonlijk mee gepaard gaat", licht Michael Willemse toe. Hij ziet in de markt toch een lichte daling in het PaaS-gebruik ten voordele van containers. In dit model beheer je zelf de applicatie en is er een gedeelde verantwoordelijkheid op het vlak van netwerk en besturingssysteem.

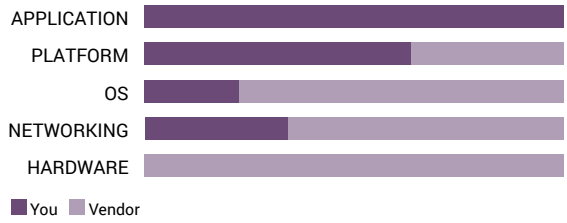


Prijsmodel: *pay per hour or second*
Voorbeelden: *AWS Elastic Beanstalk, Heroku, Google App Engine*

3/CONTAINERS (CAAS)

Een container is een standaard software-unit die code (en alles wat daarbij komt kijken) verpakt zodat een applicatie vlot en betrouwbaar werkt van de ene computeromgeving tot de andere. "Veel bedrijven evolueren naar containers, maar doen dit niet alleen in een cloudomgeving. Ze werken ook met containers in een on premise-omgeving, eigenlijk als shift van virtuele machines naar containers", aldus Willemse.

Als gebruiker beheer je bij containers in de cloud zelf (mee) elementen zoals Docker-beelden, OS, platform en dergelijke. "Bij container orchestration zijn er verschillende niveaus van beheer. Maar als je containers on premise hebt, is container orchestration sowieso je eigen verantwoordelijkheid."



Prijsmodel: *pay per hour or second*
Voorbeelden: *Docker, Kubernetes (container orchestration)*

4/SERVERLESS (FAAS)

Bij serverless – ook wel Functional Platform as a Service of F(P)aaS genoemd – leveren gebruikers alleen code en een stuk configuratie aan voor de beoogde software. De configuratie bepaalt daarbij op welke manier het stuk code kan worden opgeroepen. De cloudprovider neemt de volledige verantwoordelijkheid in handen voor het beheer van de onderliggende resources. Hij zorgt ook voor de scaling, die over het algemeen volledig transparant is. Ongebruikte capaciteit wordt niet gefactureerd aan de klant. "Serverless maakt maximaal gebruik van de gedeelde verantwoordelijkheid", stelt Willemse.

In dit model staat de leverancier in voor de hardware, het netwerk, het OS en het platform. "Hier merk je duidelijk een verhoogd niveau van ondersteuning en verantwoordelijkheid door één enkele cloudprovider. Alleen de applicatie valt voor rekening van de gebruiker. En dan is de service-API van de leverancier onderdeel van de applicatie."

Prijsmodel: *pay per use*
Voorbeelden: *AWS Lambda, Azure Functions, Google Cloud Run & Functions*

DAAR IS PIZZA AS A SERVICE WEER

Al jaren gebruiken IT'ers of IT-managers de pizza-metafoor om de verschillen in cloudcategorieën aan te duiden. Met containers en serverless (FaaS) zijn de mogelijkheden wel uitgegroeid tot het 2.0-model.

PIZZA AS A SERVICE 2.0

TRADITION ON-PREMISES (LEGACY)	INFRASTRUCTURE AS A SERVICE (IaaS)	CONTAINERS AS A SERVICE (CaaS)	PLATFORM AS A SERVICE (PaaS)	FUNCTION AS A SERVICE (FaaS)	SOFTWARE AS A SERVICE (SaaS)	
CONVERSATION	CONVERSATION	CONVERSATION	CONVERSATION	CONVERSATION	CONVERSATION	Configuration
FRIENDS	FRIENDS	FRIENDS	FRIENDS	FRIENDS	FRIENDS	Functions
BEER	BEER	BEER	BEER	BEER	BEER	Scaling
PIZZA	PIZZA	PIZZA	PIZZA	PIZZA	PIZZA	Runtime
FIRE	FIRE	FIRE	FIRE	FIRE	FIRE	Os
OVEN	OVEN	OVEN	OVEN	OVEN	OVEN	Virtualisation
ELECTRIC/GAS	ELECTRIC/GAS	ELECTRIC/GAS	ELECTRIC/GAS	ELECTRIC/GAS	ELECTRIC/GAS	Hardware
HOMEMADE	COMMUNAL KITCHEN	BRING YOUR OWN	TAKEAWAY	RESTAURANT	PARTY	

You manage Vendor manages

VIJF CRUCIALE VRAGEN OVER 5G

Hoe je het draait of keert, zowel bedrijfsmatig als privé wordt 5G het ICT-event voor de komende jaren. De reikwijdte is breed: van razendsnel mobiel internet tot zelfrijdende auto's en … brandende gsm-masten. SAI Update biedt de management summary in vijf 5G-vragen en antwoorden.

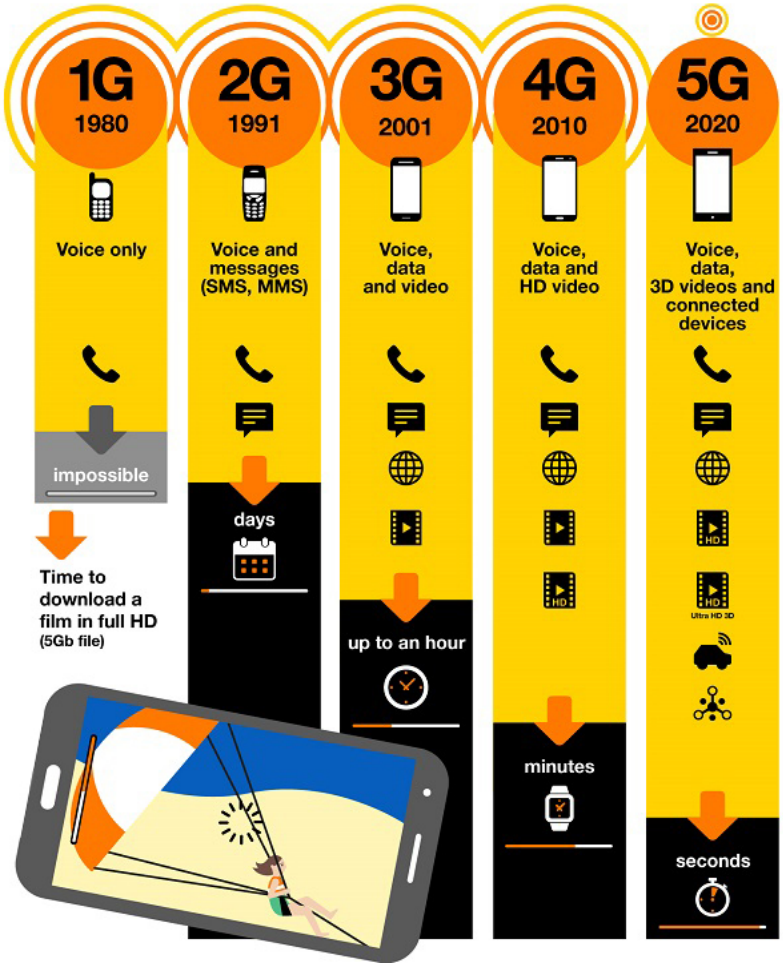
1

WAT ZIJN DE TECHNISCHE VOORDELEN VAN 5G?

In vergelijking met 4G is 5G veel meer dan een extra G erbij. Het meest in het oog springende verschil is de hogere frequentie waarop 5G werkt. Bovendien zal er bij 5G meer en meer gebruik worden gemaakt van slimme antennes die gerichte bundels straling uitzenden naar actieve gebruikers. Terwijl 4G-antennes hun radiogolven in de hele buurt uitstralen, stuurt een 5G-antenne zijn data veel gerichter (zie figuur).

4G-antenne

5G-antenne



Bron: Orange

Deze technische eigenschappen maken 5G op allerlei domeinen veel krachtiger 4G. Voor het grote publiek springt vooral die **hogere snelheid** in het oog, volgens Samsung tot tweehonderd keer meer dan bij 4G. “5G biedt véél hogere download- en uploadsnelheden. Downloads zijn bijna onmiddellijk klaar en op elk toestel is de snelheid buitengewoon”, zo klinkt het bij Proximus, dat in ons land de eerste stappen naar een 5G-netwerk zette. Een beetje verder worden op hun 5G-website ook andere voordelen aangehaald, al zitten die wat verder weg.

In bedrijfscontext zijn ook andere zaken van tel. **Latency** of reactiesnelheid is daar een belangrijke van. Die reactiesnelheid bedraagt bij een 4G-netwerk tientallen milliseconden, bij 5G zou dat in theorie slechts één milliseconde uitmaken. Ook al zal dat in de praktijk wat meer zijn, de vertraging tussen het versturen en ontvangen van data ligt dus erg laag is. Een andere vooraanstaande troef van 5G is de verbeterde **consistentie** van de verbinding. Want momenteel zijn 4G-netwerken niet altijd even consistent qua snelheid.

Ook een belangrijk voordeel is het zogenaamde **network slicing**, dat de concepten van software-defined networking (SDN) en network functions virtualisation (NFV) toepast op mobiele telecomnetwerken. Hierbij wordt abstractie gemaakt van de fysieke hardwarecomponenten en wordt functionaliteit via software centraal geregeld. Het resultaat is een dynamische netwerkinfrastructuur die flexibel kan worden beheerd. Technisch gezien kunnen mobiele operatoren door middel van slicing meerdere virtuele netwerken beheren en bedienen. Ten slotte worden er ook andere voordelen van 5G genoemd: van efficiënter omgaan met energie tot de mogelijkheid tot verfijnde locatiebepaling.

2

VOOR WELKE DOELGROEPEN?

In onze contreien zijn er nog maar amper 5G-smartphones beschikbaar. Bij Proximus maken ze op dit moment melding van de *Oppo Find X2 Pro 5G* die hun 5G-netwerk aankan, al breiden ze hun aanbod zo snel mogelijk uit.

Dat is niet zozeer de reden waarom 5G vooral een businesskwestie is. Ook een in de consumentenmarkt behoorlijk actieve speler zoals Samsung stelde in zijn paper over *The Societal Impact van 5G* vooral businessdomeinen waar 5G het verschil zal maken: gezondheidszorg, transport, entertainment en industrie. En het lijkt vooral in de industrie te zijn waar voor 5G in eerste instantie de cases opduiken, ook in ons land zoals in de havens van Antwerpen en Zeebrugge (zie cases op de volgende pagina's).

3

MET WELKE AANBIEDERS?

In België is het wettelijke kader voor 5G nog (lang) niet finaal. De veiling van de 5G-vergunningen laat daardoor op zich wachten. "Het BIPT heeft een oplossing gezocht door een systeem van tijdelijke 5G-vergunningen in te voeren. De kandidaten voor die tijdelijke vergunningen zijn bekend, maar de tijdelijke vergunningen zijn vandaag nog niet toegekend", stelt Gerrit Vandendriessche, partner bij ALTIUS.

Naast de drie grote Belgische telecomoperatoren Orange, Proximus en Telenet, hebben ook IT-dienstverlener Cegeka en Entropia, dat telecomnetwerken levert voor kritieke bedrijfscommunicatie, zich kandidaat gesteld voor een tijdelijke 5G-vergunning. Het Vlaamse Citymesh en het Waalse Gridmax (dat recent werd overgenomen door Cegeka) zijn al in de 5G-band actief op basis van een oude vergunning. Het geeft aan dat 5G niet langer alleen een zaak is van de klassieke telecomoperatoren.

Niet elk land heeft overigens een spectrum voor private 5G-netwerken, maar in België is dat wel mogelijk. Om dat te kunnen bewerkstelligen, moet er nog een koninklijk besluit worden afgewerkt om (een deel van) de frequentieband ook ter beschikking te stellen van bedrijven.

4

WAT MET SECURITY?

Tot nu toe ging security van mobiele netwerken voornamelijk over de bescherming van de centrale core. Maar bij 5G gaat het om een virtuele omgeving, waar core-componenten en functionaliteiten eender waar in het netwerk kunnen worden verspreid. In zo'n dynamische omgeving moet ook je security mee veranderen en evolueren naar een omgeving waar securityfuncties meer en meer via virtual machines worden geleverd. Hier zal *security by design* soelaas kunnen brengen, wat wil zeggen dat men vanaf de implementatie kan bekijken en vastleggen hoe 5G-beveiliging gerealiseerd wordt voor elk domein. De (eerste) gevirtualiseerde 5G-netwerken maken het mogelijk om 5G-beveiliging eigen te maken en te beheersen, vooraleer het op grote schaal daadwerkelijk gebruikt wordt.

5

EN WAT MET ONZE GEZONDHEID?

Dat is misschien wel het heetste hangijzer rond 5G op dit moment.

In heel Europa waren er tegen eind april al 88 gsm-masten in brand gestoken. Vooral via sociale media wordt er veel foutieve informatie verspreid over gsm-masten en 5G-technologie. Onder complotdenkers leeft bijvoorbeeld de stelling dat de masten het coronavirus zouden verspreiden of schadelijk zijn voor de gezondheid. "Er is veel nepnieuws", oppert Marc Lambotte, CEO van Agoria, dat in een persbericht ijverde voor strenge straffen voor de daders.

Toch is er ook veel ongerustheid. "Mensen blijven bezorgd dat de continue blootstelling tot kanker kan leiden. Maar daar zijn geen aanwijzingen voor", zo liet Eric van Rongen, die al ruim 25 jaar onderzoek voert naar niet-ioniserende straling, zich in *Data News* ontvallen. Ook over 5G klonk hij eerder geruststellend: "De hoogste frequentie bij 5G komt niet dieper dan de huid."

Ook Proximus zet alle zeilen bij om mensen gerust te stellen over 5G. "De normen in Vlaanderen, Wallonië en Brussel liggen ruimschoots onder de Europese stralingsnorm van 41 volt per meter die mee wordt bepaald door de Wereldgezondheidsorganisatie", aldus Proximus-voorzitter Stefaan De Clerck tijdens een (virtuele) persbriefing. Hij toonde een grafiek waaruit bleek dat de 5G-straling in Nederland, Frankrijk en Duitsland vijf keer hoger ligt.

CASE 1
5G IN DE ANTWERPSE HAVEN

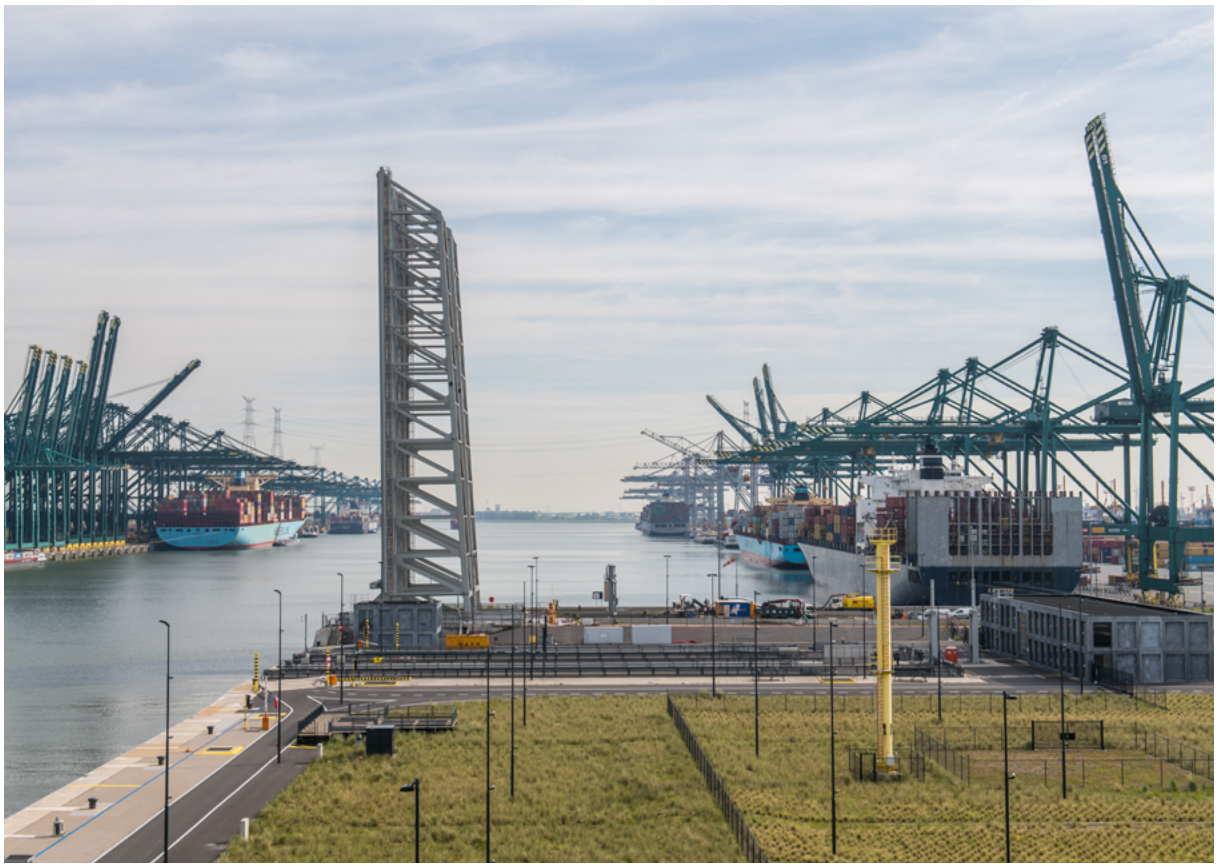
In de Antwerpse haven creëren zowel Proximus als Orange een 5G-netwerk voor industriële toepassingen. Het Proximus-project omvat de uitbouw van een mobiel netwerk specifiek voor Port of Antwerp. De mogelijke toepassingen zijn divers, zoals sleepboten die met elkaar en met de haven worden geconnecteerd om een efficiëntere coördinatie van de scheepvaart mogelijk te maken. Andere toepassingen zijn draadloze camerabewaking of het inzetten van drones voor beveiligingsdoeleinden en inspecties. Proximus en Port of Antwerp gebruiken een non-standalone architectuur die beantwoordt aan de 3GPP-standaardisatie in de kern van het netwerk.

Ook Orange Belgium test in de Antwerpse haven met enkele industriepartners zoals Borealis, Covestro en Port of Antwerp zelf. Het testnetwerk dat Orange er eind 2019 uitrolde, is volgens de operator het eerste op zichzelf staande 5G-netwerk dat in België door industriepartners wordt gebruikt en aangepast is voor draadloze productie en automatisering in real time. Orange Belgium voegt de 5G-capaciteiten niet toe aan de bestaande 4G/3G-technologie, maar rolt een apart standalone netwerk uit om de mogelijkheden rond network slicing, een lage latency en massive IoT naar eigen zeggen optimaal te benutten.

STANDALONE OF NON-STANDALONE

Er is bij 5G dus een fundamenteel onderscheid tussen standalone versus non-standalone netwerken. Bij de non-standalone versie wordt de nieuwe 5G-technologie als uitbreiding op de 4G-infrastructuur gebouwd. Dit is de eenvoudigste optie om uit te rollen voor initiële toepassingen, wanneer de dekking van 5G nog beperkt is. De prestaties kunnen evenwel beperkter uitvallen.

Bij de standalone netwerken gebruikt men slechts één radioaccesstechnologie op een nieuw netwerk in plaats van het (bestaande) 4G-netwerk. Dit nieuwe 5G-netwerk kan over het algemeen een grote diversiteit aan verkeer verwerken en toepassingen met verschillende netwerkvereisten ondersteunen, zoals hogere bandbreedte of lage latency.



CASE 2
5G BIJ BRUSSELS AIRPORT EN DE HAVEN VAN ZEEBRUGGE

Brussels Airport Company bouwde met het Finse Nokia en de Belgische operator Citymesh een van de eerste 5G-ready netwerken uit op de luchthaven. Het netwerk is intussen in gebruik. Via de hogere capaciteit van 5G wil de luchthaven nog meer inzetten op IoT (Internet of Things), geautomatiseerde voertuigen, mobiele veiligheidssystemen of track & trace-technologie.

Nokia en Citymesh zijn overigens ook partner voor het 5G-project van de haven van Zeebrugge dat midden 2020 operationeel zal zijn. Dat netwerk bevat meer dan honderd eindpunten. De verbonden apparaten kunnen dankzij het 5G-netwerk in de achterhaven in real time gevolgd, geanalyseerd en beheerd worden. Concreet gaat het over realtimeverbindingen met sleepboten, luchtvervuilingsdetectoren, veiligheidscamera's en kadesensoren.

CASE 3
DE SPREEUWEN IN DEN HAAG

In de herfst van 2018 vielen in een park in Den Haag meer dan driehonderd spreeuwen uit de bomen. Niemand had een verklaring. Behalve enkelingen die via sociale media opperden dat er geheime 5G-testen hadden plaatsgevonden. Men had op het dak van een lokale gsm-winkel een zendmast gezet. "Die 5G-stralen waren zo krachtig dat ze vogels gewoon deden doodvallen", berichtte de website JDreport.com. Later bleek dat de spreeuwen gestorven waren door giftige taxusbladeren. De stad Den Haag bevestigde ook dat er in die periode geen 5G-testen hadden plaatsgevonden. Maar intussen blijft het spreeuwenverhaal op internet circuleren.

VAN CYBER CALAMITY FORECASTER TOT AI-AUDITOR

NEGEN TOEKOMSTIGE FUNCTIES IN INFORMATIEBEVEILIGING

We willen ons veilig voelen in de nieuwe (en enge) wereld van machines, robots en kunstmatige intelligentie. Technologische en politieke trends zullen ons vak zeker beïnvloeden. Deze nieuwe wereld vraagt om nieuwe banen met nieuwe vaardigheden die een antwoord bieden op de toekomstige uitdagingen.

Niet alleen de rol van CEO en CFO zal veranderen door de technologische dominantie in het bedrijfsleven, maar ook de rol van de veiligheidsverantwoordelijken. In hun werk Cybersecurity readiness through workforce development stelt Zukin samen met de medeauteurs dat “een bredere vaardighedenset, met inbegrip van communicatie, veranderingsmanagement en leiderschap, nodig is om snel en gezamenlijk te kunnen reageren op veranderende cyberdreigingen”.

BELANGRIJKE TRENDS EN ROLLEN

We identificeren de volgende belangrijke trends die de benodigde capaciteiten van het personeel beïnvloeden:

- Verfijning en dynamiek van cyberaanvallen
- Machinaal leren en kunstmatige intelligentie
- Virtuele identiteiten
- Data
- Cloud
- Gedistribueerde hybride omgevingen
- Nieuwe manieren van werken (DevOps, Agile, Scrum)
- Voortdurende ontwikkeling van software
- Oorlog om talent
- Regelgeving en assurance

Deze trends vragen om andere mogelijkheden en rollen in het cyberdomein, zoals *Cyber Calamity Forecaster, Machine Risk Officer* en *Virtual Identity Defender*. Maar ook de *Data Trash Engineer, Cloud Orchestration Architect, Security Vaccinator, Cyberattack Agent, Cyber Talent Magnet* en *AI-auditor* komen erbij.

Om een idee te geven van wat die rollen betekenen, geven we per rol een korte uitleg. Uiteindelijk vertalen we dit naar onze visie op de rol van de CISO. Onze doelstelling is om enkele van de belangrijkste trends te duiden op basis van onze ervaring en externe onderzoeksrapporten en artikels voor HR-bedrijven.

CYBER CALAMITY FORECASTER

Door de snel veranderende bedreigingen wordt het moeilijk om deze kennis bij te houden en te vertalen naar acties. De **Cyber Calamity Forecaster** legt over het hoofd geziene mogelijkheden en niet-onderzochte aannames over de cyberwereld bloot. De ideale kandidaat levert analytische, adviserende en technische expertise en analyse over wereldwijde cyberactiviteiten. Hij of zij doet dit door de huidige en voorspelde cyberomgevingen en geopolitieke ontwikkelingen in kaart te brengen, om zo cyberproducten, waarschuwingen en voorspellingen te creëren.

Deze Calamity Forecaster moet drie belangrijke nieuwe capaciteiten combineren in één rol. In de huidige netwerkbeveiliging wordt waakzaamheid voor nieuwe dreigingen en aanvalsvectoren steeds belangrijker. Snelle detectie, risicobeoordeling en preventieve of mitigerende maatregelen krijgen steeds meer aandacht.

SCHAALBAARHEIDSPROBLEEM IN DE DATASTROOM

Om dit probleem het hoofd te bieden, vertrouwen SOC’s op een groot aantal meldingen van nieuw gedetecteerde (of vermoede) bedreigingen in openbare bronnen: newsfeeds, mailinglijsten, Twitter-berichten, fora enzovoort. Daarnaast zijn er niet-publieke bronnen: for-pay vendor threat bulletins of aankondigingen in gesloten kanalen. Dit vormt een groeiende uitdaging en is een specifiek voorbeeld van het firehose-dataprobleem. Er zijn enorm veel data beschikbaar. De betrouwbaarheid ervan staat op voorhand nooit vast. Bovendien is het niet gegarandeerd dat de data zo gestructureerd zijn dat ze

eenvoudig (semi-)geautomatiseerd verwerkt kunnen worden.

Veel databronnen werpen (mogelijk vanuit verschillende perspectieven) een licht op zaken die een onderliggende samenhang delen. Het is belangrijk om de relatie tussen meldingen uit verschillende bronnen te ontdekken. Ook het feit dat databronnen in verschillende brontalen geschreven zijn, speelt een rol. Veel (maar niet alle) bronnen zijn in het Engels (van wisselende kwaliteit) geschreven. Men mag nooit uitsluiten dat een zeer relevant en urgent rapport eerst in het Russisch, Koreaans, Chinees, Duits of Frans verschijnt. Gezien de omvang (firehose) van de datastroom ontstaat een probleem van schaalbaarheid. Een hoge mate van automatisering is nodig. Met dit probleem in het achterhoofd, definiëren we drie gerelateerde vaardigheden:

1. Beoordeling van de kwaliteit van de gegevensbron
2. Intelligente correlatie-, relevantie- en risicobepaling
3. Automatisering van de Data Source Handling Process Flow en het sturen van die flow naar doelgroepen in een presentabel en bruikbaar formaat

Op basis van de verzamelde bedreigingsgegevens kan de Calamity Forecaster een trendanalyse uitvoeren op sectoren (zoals finance, retail en productie), landen, platformen (Microsoft, Oracle enzovoort) of omgevingen (industriële installaties). Deze rol wordt steeds belangrijker omdat de meeste mensen door de bomen het bos niet meer zien.

ACHT ANDERE NIEUWE ROLLEN IN CYBERSECURITY

1

De rol van **Machine Risk Officer** wordt essentieel om nieuwe vertrouwensmechanismen te ontwikkelen en nieuwe risico-baten-benaderingen te bedenken voor het werken met intelligente machines. De werknemer in deze functie zal de rollen en verantwoordelijkheden tussen mens en machine definiëren en de regels bepalen voor de manier waarop menselijke tegenhangers moeten omgaan met de door machines veroorzaakte misstanden.

2

De **Cyber Diplomat** is essentieel voor het beheer van belanghebbenden en regelgevers. Hij of zij zoekt samenwerkingen met andere publieke en private bedrijven en de overheid. Oorlogen worden gewonnen door genoeg (én de juiste) bondgenoten te hebben. Naar de oorlog trekken zonder hen leidt tot mislukking, zoals de geschiedenis van onder meer Napoleon en Hitler leert. De medewerker in deze functie vormt sterke allianties en beïnvloedt de buitenwereld over de mening van de entiteit zelf.

3

In de rol van de **Security Pusher** wordt verwacht dat je elke situatie analyseert waar klanten contact hebben met het merk of de organisatie. Je kwalificeert de betrokken emoties en stelt daarna een abonnementsstrategie voor om deze te vervullen. De taak bestaat uit het onderzoeken, volgen, vormgeven en voorstellen van de beslissingen om ervoor te zorgen dat de cyberrisico's worden behandeld in lijn met de risicobereidheid en het gedrag van de klant. Dit vereist frequente interactie met klanten, belanghebbenden en partijen die betrokken zijn bij de levering van diensten in de waardeketen om effectief te kunnen opereren. Deze rol komt naar voren bij managed security service providers (MSSP) en integratoren die bepaalde verplichtingen hebben tegenover hun klanten als beveiligingsadviezen niet worden opgevolgd door organisaties.

4

Als **Cyber Attack Agent/SEAL** maak je deel uit van een nieuwe Special Operations-divisie binnen het SOC. De opdracht: het ontwikkelen, ondernemen en leiden van het cyber-afschrikkingsprogramma. Als een belangrijk lid van dit team help je bij de ontwikkeling en levering van strategische cyberaanvallen tegen de infrastructuur van tegenstanders en tegen systemen in de publieke en private sector. Om in aanmerking te komen voor deze cruciale rol moet je een uitstekende staat van dienst hebben qua cyberhacking, grey-hat-gerichte softwareontwikkeling of gedistribueerde denial of service-aanvalervaring. Cyber aanvalsagenten/afdichtingen zullen moeten opereren als een effectief en zeer wendbaar team, dat nauw samenwerkt met elkaar en met de cybersecurityteams van het NCSC.

5

In de rol van **Data Trash Engineer** pas je analytische nauwkeurigheid en statistische methoden toe op datatrash om de besluitvorming, productontwikkeling en strategische initiatieven te begeleiden. Dit gebeurt door een data trash nutrition labeling-systeem te creëren dat de kwaliteit van de afvaldatasets beoordeelt en de data-groei-data-trash-ratio beheert. Deze rol is nodig om het verzamelen van zware data door organisaties te voorkomen en om te voldoen aan de GDPR-regelgeving, zoals voor het bewaren van gegevens.

6

De **Cyber Philosopher** zal de discussie over de balans tussen mensheid en machines levendig houden, om te voorkomen dat er een Judgement Day plaatsvindt.

7

De **AI-auditor** zal een onafhankelijk oordeel vormen over de integriteit van de AI. Deze auditor maakt deel uit van een overheidsinstelling die zonder vragen en zonder financiële prikkels audits uitvoert. Zoals we in de toekomst zullen leren, kan de AI-auditor geen deel meer uitmaken van een commerciële organisatie.

8

De **Security User Experience** (SUX) **Designer** is een expert in beveiliging binnen producten en diensten en zorgt voor een gebruiksvriendelijke ervaring. De manier waarop de beveiliging is ontworpen en integraal deel uitmaakt van het product of de dienst, resulteert in een perfecte balans tussen gebruiksgemak en een veiligere ervaring. In een wereld waar het onbekend wordt wie er te vertrouwen is, wordt vertrouwen essentieel voor de bedrijfsstrategie.

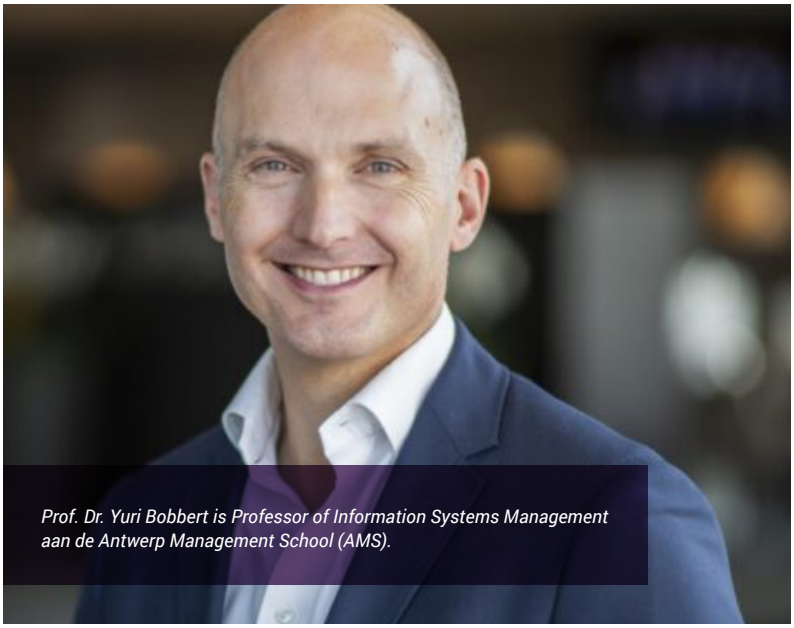
GESCHOOLD TALENT NODIG

Voor deze toekomstige rollen is opgeleid talent nodig. Veel van de al ontwikkelde leer- en certificeringsprogramma's zijn voor HR-professionals of recruiters een compleet oerwoud. Voor de HR-professional wordt het steeds complexer om het talent te onderscheiden van de amateurs. Je kunt niet alleen oordelen over een certificering, je moet ook dieper zoeken naar intrinsieke motivaties en persoonlijke capaciteiten. Dit lijkt een open deur, maar in informatiebeveiliging is het voor een HR-professional moeilijk om te zien hoe goed iemand eigenlijk is in een bepaald domein.

Marcelle Lee stelt in het artikel Seeking the Purple Squirrel in ISACA Journal voor om te kiezen voor een open functieomschrijving Desired Experience: "Security is een snel evoluerende ruimte, bestaande uit tal van verschillende technologieën. Van geen enkele persoon wordt verwacht dat hij of zij alle kenmerken van deze lijst bezit. Een nieuwsgierige geest, het vermogen om na te denken over de regels en hoe deze te breken en de bereidheid om te leren, zijn de belangrijkste kenmerken die we zoeken. Als je een aantal van de volgende eigenschappen hebt en bereid bent om er meer van te leren, dan willen we dat graag van je horen."

Ondanks de enorme vooruitgang in de industrie, de race om talent en het uitkijken naar de Purple Squirrel, blijft de onnauwkeurigheid van gegevens en informatie een enorme uitdaging voor veel organisaties. Dit blijkt uit de ontoereikende detectiepercentages en de trage reactietijden bij aanvallen. De belangrijkste hoofdoorzaken voor deze onvoldoende geconfigureerde beveiligingstools en talloze puntoplossingen is het gebrek aan vakmanschap.

Maar er staat veel op het spel. Een ontoereikende en schijnbaar zwakke reactie op inbreuken kan een negatieve impact hebben op de gepercipieerde waarde van het bedrijf en mogelijk op de koers van het aandeel. Deze informatie druppelt zelden over naar de operationele teams. Ik ben ervan overtuigd dat dit – zoals in het recente rapport van Wakefield Research en Deloitte over The future of cyber survey 2019 – de belangrijkste reden is waarom de helft van de CISO's hun SOC willen uitbesteden en meer waar voor hun geld willen krijgen.



Prof. Dr. Yuri Bobbert is Professor of Information Systems Management aan de Antwerp Management School (AMS).

DRIE ROLLEN VOOR DE MODERNE CISO

Ik zie de rol van de CISO uitbreiden naar econoom, 'talentenmagneet' en orkestrator met een duidelijke visie op de aanpak van valkuilen op de drie organisatieniveaus.

1. **Econoom**, omdat de CISO moet vertrouwen op gedetailleerde, betrouwbare brongegevens om het cyberrisicogehalte in de context van alle andere risico's te bepalen. Op basis van feiten en cijfers moet de CISO uitleggen dat de investeringen hun geld waard zijn en aan het bestuur verkopen.
2. **Talentenmagneet**, vanwege de voortdurende strijd om veiligheidstalent. Dit betekent dat de CISO het aanwervingsproces van toppersoneel moet leiden en beïnvloeden. Hij of zij zoekt talent dat in staat is om KRI's en KPI-mechanismen in de technologie en processen te ontwikkelen. Vandaar de noodzaak om ook toekomstige rollen te voorspellen, die snel kunnen ontstaan.
3. **Orkestrator**, omdat risico's van derden het grootste risico vormen voor platformgebaseerde bedrijfsmodellen die werken in een groot API-gebaseerd ecosysteem en die duidelijke, vooraf gedefinieerde indicatoren nodig hebben om de cyberprestaties over meerdere omgevingen te monitoren. Dit betekent dat de CISO de beveiliging van de hele keten moet ontwerpen en orkestreren, zodat hij of zij volledig zicht krijgt op de effectiviteit van de beveiligingscontroles.

Tekst: Prof. Dr. Yuri Bobbert

WORDT DE DPO AU SÉRIEUX GENOMEN?

Enkele weken geleden legde de Gegevensbeschermingsautoriteit (GBA) Proximus een recordboete op. Een belangenconflict rond de Data Protection Officer (DPO of functionaris voor gegevensbescherming) lag hier ten grondslag.

Het gaat om een boete van 50.000 euro die de Gegevensbeschermingsautoriteit (GBA) uitschrijft. Dat is de hoogste boete ooit in ons land voor een overtreding van de General Data Protection Regulation (Regulation (EU) 2016/679), beter bekend als GDPR.

BESLISSING MET GROTE IMPACT

Deze zaak draait om een rol- of belangenconflict. De GBA veroordeelt Proximus voor 'niet-naleving van de verplichting om een belangenconflict in hoofde van de functionaris voor gegevensbescherming (DPO) te vermijden (artikel 38.6 GDPR) en het niet afdoende betrekken van de functionaris voor gegevensbescherming (DPO) (artikel 38.1 GDPR). "De functionaris voor gegevensbescherming (DPO) kan binnen de organisatie geen functie bekleden waarbij hij doelstellingen en middelen voor de verwerking van persoonsgegevens mee moet bepalen", klinkt het in het besluit.

Deze uitspraak zal een serieuze impact hebben, oordeelt Jan Maarten Willems (BearingPoint), die zelf als externe DPO actief is bij een aantal organisaties. "De geest van

Jan Maarten Willems (BearingPoint): "Je kunt bij dataverwerking niet tegelijk rechter en partij zijn."

WIE MOET EEN DPO AANSTELLEN?

Een functionaris voor gegevensbescherming (DPO) moet aangeduid worden wanneer (artikel 37 GDPR):

1. de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve bij gerechten in de uitoefening van hun rechterlijke taken
2. een verwerkingsverantwoordelijke hoofdzakelijk is belast met verwerkingen die regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen
3. de verwerkingsverantwoordelijke hoofdzakelijk is belast met grootschalige verwerking van bijzondere categorieën van gegevens zoals strafrechtelijke veroordelingen en strafbare feiten.

de beslissing van de GBA is duidelijk: je kunt bij dataverwerking niet tegelijk rechter en partij zijn."

COVID-19-PERIODE

Volgens Willems is de vraag duidelijk: kunnen we na twee jaar GDPR-wetgeving spreken over een echte job als DPO? "Zal de DPO eindelijk naar waarde worden geschat?", vraagt hij zich af.

Zeker in coronatijden vallen de gevolgen van de uitspraak van de GBA niet te onderschatten. "Veel bedrijven zullen de komende weken en maanden willen besparen, zeker op functies die niet direct een aantoonbare opbrengst hebben."

WIE O WIE WIL DPO ZIJN?

Wie komt er in een bedrijf in aanmerking als DPO, in combinatie met een andere job? "Het moet iemand zijn die onafhankelijk van het topmanagement kan werken", stelt Jan Maarten Willems. Dat betekent alvast geen C-levelfunctie, maar ook lagere functies in een organisatorische structuur kunnen hier uit de boot vallen.

Wie misschien nog het meest in aanmerking komt, volgens Willems, is iemand uit het juridische departement, uit het datateam of iemand die uit de "business' komt met een duidelijk analytische achtergrond. "AI is het altijd de vraag binnen de organisatie of iemand van daaruit de rol van DPO op zich wil nemen."

TWEE JAAR GDPR: VAN WAAR KOMT DE WIND?

“Na twee jaar GDPR komt de Gegevensbeschermingsautoriteit of GBA stilaan op kruissnelheid”, bevestigt Gerrit Vandendriessche, partner bij advocatenkantoor ALTIUS. Met hem bespreken we kort enkele opvallende cases in binnen- en buitenland.

De eerste sanctie die de GBA uitvaardigde, was voor een burgemeester die verkiezingsreclame had gestuurd naar burgers die in zijn gemeente een bouwaanvraag hadden ingediend. De bijhorende boete bedroeg 2.000 euro. “Dat was eigenlijk nog beperkt in vergelijking met de record-boete van 50.000 euro over de onafhankelijkheid van een DPO die recent werd opgelegd”, zo verwijst Gerrit Vandendriessche naar de zaak rond Proximus (zie het artikel op de volgende pagina).

Volgens Gerrit Vandendriessche voert de GBA meer proactieve inspecties uit. “De GBA kijkt er steeds nauwkeuriger op toe hoe organisatie gegevens verwerken.” Los van de recente DPO-case bij Proximus vielen in onze contreien deze cases op, die de reikwijdte bevestigen en bedrijven tot nadenken aanzetten:

Gerrit Vandendriessche, partner bij ALTIUS: “De GBA kijkt er steeds nauwkeuriger op toe hoe organisaties gegevens verwerken.”

DE COOKIECASE

De GBA oordeelde dat de website Jubel.be de regels rond cookies overtrad. Volgens de GDPR moeten gebruikers namelijk toestemming verlenen wanneer er cookies worden gebruikt die niet strikt noodzakelijk zijn. Bovendien moet het cookiebeleid transparant zijn. Dat was telkens niet het geval. “Die case heeft nogal wat stof doen opwaaien. Veel bedrijven waren of zijn niet in orde met hun cookiepolicy”, weet Vandendriessche.

DE EID-CASE

Deze zaak ging over een drankenhandel die overschakelde van een papieren naar een elektronische klantenkaart. Hierbij werd de eID van een klant ingelezen via een intelligent kassasysteem. Een klant diende een klacht in bij de GBA omdat hij ook zonder zijn eID van klantenvoordelen wilde genieten, maar dat kon niet. Het Marktenhof floot de aanvankelijke veroordeling en boete door de GBA in beroep terug. De GBA had zich voor de veroordeling gebaseerd op een wet die nog niet in werking was en op een niet-bindende aanbeveling. Dat was volgens het Marktenhof onvoldoende om een schending van de GDPR te kunnen vaststellen.

WANNEER GAAT DE GBA TOT ACTIE OVER? EN VOORAL: WAT WORDT ER DAN ONDERZOCHT? ALLES, ZO BLIJKT

De GBA opereert meer proactief en naar aanleiding van klachten. Maar hoe maakt de instantie haar keuze? In de meeste gevallen gaat de Gegevensbeschermingsautoriteit tot actie over na een klacht van een klant enerzijds of anderzijds op vraag van het directiecomité van de Gegevensbeschermingsautoriteit zelf, bevestigt Gerrit Vandendriessche. Hij stelt vast dat de GBA alvast meer personeel heeft gevraagd aan het parlement, waardoor het ernaar uitziet dat de organisatie meer werk zal kunnen verrichten.

Cruciaal is echter om te weten dat bij een eventuele klacht van een klant, het niet bij het voorwerp van die ene klacht blijft. “Een klacht van een klant is inderdaad voldoende om tot actie over te gaan. Maar dan zal de GBA meestal meteen ook een volledige GDPR-analyse uitvoeren naar alle verplichtingen waaraan de organisatie moet voldoen.”

DE MAINFRAMECASE

Een opvallende uitspraak tegen de financiële groep ING. Een klant eiste dat zijn naam correct in de computersystemen zou worden bewaard. Het ging letterlijk om één letter: é in plaats van e. ING argumenteerde dat haar US-gebaseerd mainframe van 1995 alleen EBCDI (extended binary-coded decimal interchange code) ondersteunde, waarin de é niet voorkwam. Het mainframe onmiddellijk wijzigen, was volgens ING te duur en te ingrijpend want ING zou binnenkort toch overschakelen naar aan ander mainframe dat wel letters met accenten ondersteunde. “Maar de GBA was het hier niet mee eens en vond het fundamenteel recht op verbetering aangetast. De GBA beval ING om de naam van de klant correct te schrijven. Dit werd bevestigd door het Marktenhof, dat eraan toevoegde dat noch een ‘ouderwets’ computerprogramma, noch (te grote) kosten, redenen kunnen zijn om GDPR-rechten van klanten te schenden. ”

DE TENNISBONDCASE

Een Nederlandse case, maar opmerkelijk en interessant. De Nederlandse toezichthouder gaf de Nederlandse tennisbond namelijk een boete van (maar liefst) 525.000 euro wegens het doorverkopen van persoonsgegevens van leden aan sponsors. “De bond vond dat ze een gerechtvaardigd belang had bij de verkoop van die gegevens. Maar de toezichthouder was het daarmee niet eens en heeft geoordeeld dat bond geen grondslag had om die persoonsgegevens door te geven aan sponsors.”

Op 26 mei 2020 om 11.00 uur organiseert SAI een webinar met een panel over de huidige stand van zaken rond GDPR en privacy. Ook Gerrit Vandendriessche en Jan Maarten Willems geven hun visie. ***Klik hier om in te schrijven!***

DOE MEE EN WIN EEN MOOIE PRIJS MET DE SAI-QUIZ

VRAAG 1

Naar waar verwijst dit deel van een bekende poster?

VRAAG 2

Wie was de initiatiefnemer achter de oprichting van SAI?

SCHIFTINGSVRAAG

Hoeveel SAI-leden zullen het juiste antwoord gemaild hebben tegen dinsdag 1 september 2020?

» *Stuur het antwoord op deze vragen voor 1 september 2020 naar **communicatie@sai.be**.*
De winnaar wordt bekendgemaakt in het volgende magazine en wordt persoonlijk verwittigd.

***Quizwinnaar SAI Update Februari 2020:** Dirk Heyndrickx, Business Analyst bij DXC Technology Belgium. Proficiat!*
De juiste antwoorden waren Blue Thunder en Ron Tolido.

VIER CRUCIALE BEGRIPPEN ROND QUANTUMCOMPUTING

Wat maakt quantumcomputing zo speciaal? Welke mogelijkheden en theorie zitten erachter? Tijd om enkele belangrijke elementen bloot te leggen en cruciale vraagstukken te bekijken, zoals het einde van het internet.

Bij een quantumcomputer maakt de processor gebruik van de principes van de quantummechanica. Zo'n processor kan in één keer parallel verschillende en dezelfde berekeningen uitvoeren over een zeer grote hoeveelheid data, aldus Koen Pellegrims, die recent een SAI-avondconferentie verzorgde over het concept. "Fundamenteel anders dus dan bij klassieke computertechnologie, die gebaseerd is op informatie waar alles 0 en 1 is", vertelt hij. "Bij die klassieke computing zijn de resultaten deterministisch, dat is bij quantumcomputing niet zo. Daar zijn de resultaten probalistisch of benaderend." Deze concepten staan voorop bij quantumcomputing:

1/DRIE QUANTUMEFFECTEN: KRUIS EN MUNT TEGELIJK

De drie basics van een quantumcomputer zijn de quantumeffecten: superpositie, verstrengeling en interferentie, die quantumdeeltjes onder bepaalde omstandigheden kunnen vertonen. "Het zijn de elementen op basis waarvan berekeningen gebeuren, die onderhevig zijn aan de wetten van de quantumfysica", valt Pellegrims samen. Superpositie van een quantumdeeltje betekent dat bijvoorbeeld de spin hiervan (normaal maar één mogelijke waarde) alle mogelijke waarden tegelijkertijd kan aannemen. Koen Pellegrims maakt de vergelijking met een muntstuk. "In klassieke computing is dat kruis of munt, dus 0 of 1. Maar in quantum kan zo'n muntstuk in beweging

veel meer vormen aannemen."
Pas als men iets doet om de spin te meten, dan zal het deeltje weer terugvallen naar één waarde.

Verstrengeling, het tweede effect, van twee gepaarde deeltjes betekent dat er een verbinding bestaat tussen deze twee deeltjes, die onafhankelijk is van de onderlinge afstand. Als de toestand van een deeltje gemeten wordt, weet men ook onmiddellijk wat de toestand van het andere deeltje is. Interferentie ten slotte is het effect waarbij het golfkarakter van een deeltje versterkt of uitgedoofd worden door een ander quantumdeeltje.

2/QUBITS: IT TAKES TWO TO TANGO

Het geheugen van de quantumcomputer is opgebouwd uit qubits. Dit zijn deeltjes in superpositie die via een ingenieus patroon met elkaar verstrengeld zijn. "In superpositie heeft een qubit de binaire waarden 0 én 1, dus de twee tegelijkertijd in plaats van 0 óf 1. Eén qubit heeft dus eigenlijk de waarde van twee bits", aldus Pellegrims.

Het principe loopt als volgt: de quantumprocessor voert manipulaties uit op de qubits in het geheugen op basis van input uit ditzelfde geheugen. Maar die processor haalt en bewerkt de waarde 0 én 1. Bovendien stijgt de rekenkracht exponentieel met het aantal qubits. Bijvoorbeeld: stel dat het aantal n bijvoorbeeld acht is, dan zal de processor in één keer voor alle mogelijke inputs (twee tot de achtste = 256) dezelfde berekening uitvoeren. Conventionele computertechnologie zou hier juist 256 keer dezelfde handeling voor moeten verrichten.

3/DE REGEL VAN BORN: KWESTIE VAN WAARSCHIJNLIJKHEID

De waarschijnlijkheidsrelatie van Born (*the Born rule*) is een beginsel in de quantummechanica dat bij quantumcomputing opduikt. Deze belangrijke regel, genoemd naar de Duitse fysicus Max Born, dient om de interpretatie van de quantummechanische golffunctie uit te leggen. "Deze waarschijnlijkheidsinterpretatie beschrijft met welke waarschijnlijkheid een bepaalde meetwaarde optreedt bij het uitvoeren van een meting aan een quantumsysteem."

4/ HET ALGORITME VAN SHOR EN … HET EINDE VAN HET INTERNET

Doordat een quantumcomputer fundamenteel anders werkt dan een klassieke computer, zullen er ook speciale programmeertalen voor ontwikkeld moeten worden. En die moeten deterministisch zijn. Momenteel doen twee algoritmes de ronde. Het eerste is het algoritme van Grover om ongesorteerde data te doorzoeken.

Het meest in het oog springt evenwel het algoritme van Shor voor het ontbinden in priemfactoren. "Dat algoritme zou het mogelijk maken om encryptie te kraken", aldus Pellegrims. De knoop zit in het feit dat het algoritme van Shor op een dergelijke manier schaalt dat het verhogen van de sleutelgrootte niet volstaat om een systeem te beveiligen. Een gebruiker die een systeem beveiligt, zou daar dan bij wijze van spreken net zoveel tijd voor nodig hebben als een potentiële hacker die diezelfde beveiliging kraakt.

Al wil Pellegrims dit ook nuanceren. "Een vaak gehoorde stelling is dat met quantumcomputing en dit algoritme het internet meteen onbruikbaar wordt. Omdat de klassieke RSA-beveiligingstechnologie vlot te kraken valt. Zover zijn we niet. Maar weet dat data die bijvoorbeeld vandaag worden onderschept morgen – of overmorgen – eventueel wel ontsleuteld kunnen worden."

REALITYCHECK: KOMT ER EEN QUANTUMCOMPUTER OP JE BUREAU? SPOILER ALERT: WAARSCHIJNLIJK NIET

- De wereldwijde race naar de quantumcomputer is volop aan de gang. Google, Microsoft en IBM, maar ook Baidu, Alibaba en Tencent proberen de eerste stabiele quantumcomputer te maken. Vooral Google en IBM zijn in gevecht met elkaar over 'quantumsuprematie'.
- De technologie staat nog niet op punt. Qubits zijn momenteel nog vrij instabiel en niet foutloos. Om ze optimaal te laten werken is een behoorlijk complexe omgeving vereist, onder meer qua temperatuur.
- De zoektocht gaat naar uitdagingen of vraagstukken die quantumcomputers kunnen oplossen. Excel of Word op een quantumcomputer is dus een bizar idee. Denk bijvoorbeeld aan berekeningen over klimaatvoorspellingen, medisch- of ruimteonderzoek.
- Er zal mede hierdoor nooit (of toch zeker niet meteen) een quantumcomputer op jouw bureau staan. "Ook koeling van dat hele systeem zou al een behoorlijke uitdaging zijn", oppert Pellegrims.
- De vraag is ook of eventuele hybrideoplossingen mogelijk zijn. "Denk aan een computer met een klassieke processor en dan eventueel een quantum-coprocessor. Al is dat ook nog verre toekomstmuziek."

DE DEFINITIEVE DOORBRAAK VAN TELEWERK

In heel wat organisaties is telewerken 'het nieuwe normaal' geworden door de overheidsmaatregelen tegen de verspreiding van het coronavirus. Wie het kan, is zelfs verplicht om thuis te werken. Dit leidde tot een vervijfvoudiging van het aantal Belgen dat zijn of haar job 'vanuit zijn kot' doet.

Voor heel wat werkgevers en medewerkers is telewerken een flinke aanpassing. Voor sommige organisaties is telewerk anno 2020 zelfs een compleet nieuw gegeven. De invoering ervan werd in dergelijke organisaties steeds afgehouden om allerlei redenen:

- Het past niet in de organisatiecultuur.
- Uit solidariteit met de functies voor wie telewerk onmogelijk is (met als redenering "we implementeren telewerk voor iedereen of voor niemand").
- Gebrek aan vertrouwen bij de leidinggevenden.
- Het jaagt medewerkers op kosten door de inrichting van een deftig thuiskantoor.
- Het heeft een invloed op de carrière en het mentaal welzijn van medewerkers.
- Telewerken zorgt voor extra veiligheidsrisico's.
- Als telewerken dan toch 'moet', dan maximaal op één vast gekozen dag per week.

Het versneld invoeren van telewerk was voor deze organisaties een grote uitdaging. Een recente bevraging van meer dan duizend Belgen door het advieskantoor BDO en het HR-netwerk HR Square komt tot enkele verrassende vaststellingen rond telewerken in België.

VOOR DE CORONACRISIS

- Werkten bijna zes op de tien Belgen bijna nooit thuis.
- Werkte één op de drie regelmatig een dag van thuis uit.
- Werkte slechts 11% twee dagen of meer per week van thuis uit.

TIJDENS DE CORONACRISIS

- De helft van organisaties heeft nog geen beleid rond telewerken.
- Eén op de drie meldt dat hun onderneming geen formele policy rond telewerk inclusief fiscale en sociale aspecten heeft.
- Eén op de drie signaleert extra samenwerkingstools nodig te hebben en nog niet papierloos te kunnen werken van thuis uit.
- Zes op de tien vinden dat ze productiever werken vanuit het thuiskantoor.

Organisaties die voor de coronacrisis al vertrouwd waren met telewerken, merken dat ook voor hen alles anders is:

- Telewerken wordt niet meer afgewisseld met 'werken op kantoor'.
- Vergaderingen gebeuren hoofdzakelijk virtueel. Fysieke meetings worden gemakkelijk vervangen door videoconferenties en chat dankzij tools als Zoom, Webex, Slack, Microsoft Teams en Gotomeeting. Niemand hoeft zich te verplaatsen.
- Medewerkers moeten zich organiseren met andere huisgenoten. Ook al moeten veel ouders hun job plots combineren met kinderopvang en lesgeven, toch worden ze de voordelen van thuiswerk duidelijk gewaar. Tijdwinst is een factor. De grote meerderheid verliest in normale tijden één tot twee uur aan het woon-werkverkeer en spaart nu tot een werkdag per week aan transport uit.

Organisaties hebben tijdens de coronacrisis digitaler leren werken. Technologisch gaat het. Nu moeten aanpassingen doorgevoerd worden in de cultuur en het beleid. Organisaties mogen door telewerk productiviteitswinst boeken en kunnen tegelijkertijd kosten besparen.

Bovendien kan twee of drie dagen telewerk zorgen voor de nodige 'social distancing' op de werkvloer bij de corona-exit. Een steun in de rug voor 'het nieuwe normaal'. Nu velen geproefd hebben van thuiswerk willen veel medewerkers meer controle over de manier van telewerken, ook na de coronamaatregelen.

44%
wil gemiddeld twee dagen per week telewerken

18%
wil meer dan twee dagen per week telewerken

5%
ziet zelfs voltijds telewerk (vier à vijf dagen) zitten

< 5%
wil geen enkele dag thuiswerken na de coronacrisis

Uiteraard komen sommige jobs nooit in aanmerking voor telewerken, maar als telewerk de regel wordt in organisaties, zullen medewerkers meer stilstaan bij het effectieve en efficiënte gebruik van hun tijd. Telewerk en de fysieke afwezigheid van 'een baas' kan een interessant denkproces initiëren bij medewerkers: van 'ik ga naar het kantoor en presteer daar naar best vermogen mijn uren' naar 'hoe creëer ik optimaal toegevoegde waarde tijdens mijn werkweek?'. Bij medewerkers kan telewerk een betere balans tussen werk en privé opleveren.

De overgang naar verplicht telewerk door de coronacrisis maakt duidelijk dat telewerken van vitaal belang is voor het functioneren van de economie van de 21ste eeuw. Als medewerkers iets van de coronacrisis willen overhouden in de toekomst, dan is telewerken daar zeker bij. Telewerk gaat na de coronacrisis zeker niet verdwijnen of terugzakken naar één (vast gekozen) dag per week. De bereidheid bij medewerkers om één, twee of zelfs drie dagen van thuis uit te werken, is groter dan ooit. Flexibele telewerkregelingen zijn zinvol en voordelig voor alle organisaties en alle medewerkers die daarvoor in aanmerking komen.

Tekst: Marc Vael

VOLGENDE EVENTS VOOR SAI

WEBINAR: Panel: EU GDPR en privacy, huidige stand van zaken
Speciaal Event
26-05-2020
Meer info:
https://sai.be/event/15029

WEBINAR met COMPUTABLE CAFÉ: Cybersecurity via film
Speciaal Event
27-05-2020
Meer info:
https://sai.be/event/15037

WEBINAR: Decision & Process Modelling voor de komende jaren
Speciaal Event
04-06-2020
Meer info:
https://sai.be/event/15043

*Naar aanleiding van de huidige maatregelen rond COVID-19 voorzien we bij SAI voorlopig enkel een digitaal aanbod. Hou zeker **onze website** in de gaten voor meer info en voor eventuele aanpassingen of toevoegingen.*

» *Meer info op **SAI.be***

COLOFON
Werkten mee aan dit nummer: *William Visterin (hoofdredacteur), Teun van Dongen (art director), Robin Van den Bogaert (eindredactie), Yuri Bobbert, Stef Gyssels en Marc Vael.*