#7

SAI UPDATE

DIGITAAL TIJDSCHRIFT VOOR SAI-LEDEN | SEPTEMBER 2021 | SAI

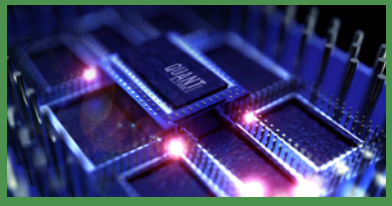
DE OPMARS VAN LOW CODE

DE DERDE WEG IN SOFTWAREONTWIKKELING

pag. 15

En verder:

DECOMMISSIONING IN IT | ZERO TRUST SECURITY: HYPE OF DE WEG VOORWAARTS?
BLOEDFRAUDE: DE GEVALLEN KONINGIN VAN SILICON VALLEY

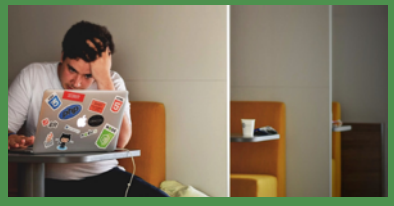


VIJF CRUCIALE VRAGEN OVER **QUANTUM COMPUTING**

pag. 22

WAT DOE JE METEEN NA **EEN CYBERAANVAL?**

pag. 7



WELKE **IT-SKILLS** WORDEN OVERBODIG?

pag. 11

EDITO

Beste SAI-lid en lezer,

Microsoft werd recent uitgeroepen tot *Enterprise Application Innovator of the Year* op de Data News Awards 2021. Microsoft won de award omdat het ondanks een bekend productgamma blijft innoveren. Het liet vooral Teams snel evolueren tot een succesverhaal dankzij extra goed werkende functionaliteiten en een naadloze integratie met Office 365 en andere Microsoft-diensten. De link met het hoofdthema in deze SAI Update is snel gemaakt: low code-ontwikkeling.

Low code doet mij persoonlijk terugdenken aan mijn eerste professionele IT-ervaringen begin jaren negentig waarbij ik toepassingen ontwikkelde met PACBASE, een (Franse) 4GL-tool die code omzette in COBOL-programma's die bruikbaar waren op IBM- en BULL-mainframes (en zelfs UNIX-machines). PACBASE was vooral een groot succes in Frankrijk en België bij de grotere organisaties. Uiteraard bestonden er tal van 4GL-tools zoals PowerBuilder, CA-Telon, Forté, Natural en Uniface. Het grote voordeel van dergelijke 4GL-tools was dat je niet echt programmeerde, maar werkte via een rapportgenerator waarin je jouw technische analyses direct kon inladen en omzetten in een toepassing.

De huidige low code-technologie doet eigenlijk hetzelfde: je tekent een toepassing visueel uit zonder één regel code. Via low code-platformen zou iedereen apps kunnen ontwikkelen die direct bruikbaar zijn op alle platformen (Android, iOS of web), ook door mensen die geen of nauwelijks IT-programmeerervaring hebben. Sommigen beweren dat iedereen in één maand de basis kan leren. Kortom, low code kan helpen om de grote vraag naar IT-ontwikkelaars snel te beantwoorden, als deze technologie wordt aangeleerd via talrijke onderwijsinstellingen en opleidingscentra.

Sommige IT-ontwikkelingsbedrijven beweren dat ze IT-projecten drie tot vier keer sneller kunnen opleveren dankzij low code-platformen. De winst zit niet alleen in de ontwikkelingssnelheid, maar ook in de visualisatie van de toepassing, waardoor toepassingen sneller kunnen gedeeld worden met opdrachtgevers voor feedback.

Toch ben ik van mening dat ook de huidige low code-platformen, net zoals de 4GL-tools uit de jaren negentig, enige basiskennis van programmaontwikkeling vereisen en raad ik bedrijven sterk aan om ook in low code-teams ervaren toepassingsontwikkelaars en technische analisten te plaatsen met concrete kennis van hoe je toepassingen opbouwt die ook op termijn onderhoudbaar zijn. Daarnaast moet elke organisatie zich zoals altijd vragen stellen over de langetermijntoekomst van leveranciers van low code-platformen (bestaan, onafhankelijkheid en licentievoorwaarden). PACBASE werd door IBM ondersteund tot 2015. Ik heb heel mooie herinneringen aan de verschillende projecten met PACBASE, vooral omdat ik na een zeer grondige PACBASE-opleiding van tien weken mocht samenwerken met een mix van zeer ervaren en intelligente teamleden. Ik wens het iedereen toe die toepassingen wil ontwikkelen.

Geniet intussen van dit zevende nummer van SAI Update. Ik hoop u te mogen ontmoeten op één van de vele SAI-activiteiten dit het najaar.

Marc Vael
Voorzitter raad van bestuur SAI

INHOUD

"

OOK SKILLS ROND AS 400 OF RPG BLIJVEN ERG IN TREK BIJ SOMMIGE BEDRIJVEN.

JOACHIM DESMET
IT-RECRUITER BIJ AMANDIS OP PAGINA 13.

ÉÉN PC OP DE TWINTIG DRAAIT NOG OP WINDOWS 7

Terwijl Windows 11 op 5 oktober uitkomt, is Windows 10 in België goed voor bijna 90 procent van het Windows-marktaandeel. Windows 7 blijkt een blijvertje, net als Windows XP.

Dat blijkt allemaal uit cijfers van **Statcounter** voor België. Het marktaandeel van Windows 7 bedraagt 5,5 procent, binnen de Windows-familie. Opvallend is dat dat percentage dit jaar amper is gedaald.

Windows 7 blijft dus hardnekkig aanwezig op sommige Belgische pc's, zowel in organisaties als bij particulieren. Weet dat Microsoft ruim anderhalf jaar niet meer in veiligheidsupdates of ondersteuning voorziet voor dit besturingssysteem.

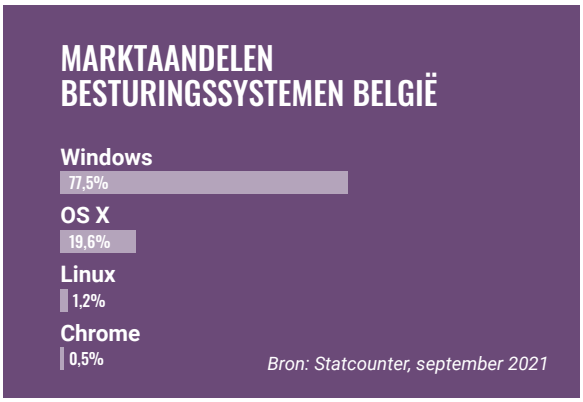
XP EN 11

Opvallend is dat her en der nog oudere Windows-versies opduiken. Zo heeft Windows XP in ons land een marktaandeel van 0,19 procent en Windows Vista haalt 0,27 procent. Terwijl XP zowat twintig jaar geleden werd gelanceerd en Vista vijftien jaar geleden.

Op de desktop-pc beschikt Windows 10 van alle Windows-versies intussen over een ruim marktaandeel van bijna 90 procent. Dat zal vermoedelijk niet meer toenemen. Microsoft brengt het nieuwe Windows 11 uit op 5 oktober, overigens gelijktijdig met zijn softwarepakket Office 2021.

EN DE REST?

Deze marktaandelen gelden alleen voor Windows-pc's. Volgens **Statcounter** heeft Windows van alle desktop-systemen in België een marktaandeel van 77,5 procent, waarmee het op een jaar tijd licht stijgt. OS X heeft een desktop-marktaandeel van 19,6 procent. Een jaar geleden was dat ruim 23 procent.



ÉÉN VIJFDE VAN IT-BUDGET GAAT NAAR SECURITY

Een doorsnee Belgische organisatie besteedt vandaag ruim een vijfde (21 procent) van zijn IT-budget aan cyberbeveiliging.

Dat is (in verhouding) een flinke toename. Vorig jaar ging in ons land dertien procent van het IT-budget naar cybersecurity. Dat alles blijkt uit het **Hiscox Cyber Readiness Report 2021**, een referentie als het gaat om onderzoek naar securitymiddelen en -inspanningen.

Met 21 procent zit ons land – procentueel alvast – op het gemiddelde van alle acht landen die voor het Hiscox-rapport werden onderzocht: de Verenigde Staten, Nederland, Frankrijk, Duitsland, Ierland, Spanje en het Verenigd Koninkrijk. In totaal werden zesduizend organisaties ondervraagd, waarvan ruim vijfhonderd uit ons land.

» *Op 26 oktober organiseert SAI een avondconferentie met boekvoorstelling van De Cyber Arena. Meer info en gratis registratie vind je **hier**.*

CLOUDBESTEDINGEN GROEIEN NAAR 1,3 BILJOEN DOLLAR

Onderzoeksbureau IDC meldt dat de totale uitgaven voor clouddiensten en -infrastructuur wereldwijd in 2025 meer dan 1,3 biljoen dollar zullen bedragen, met een jaarlijkse groei (CAGR) van 16,9 procent.

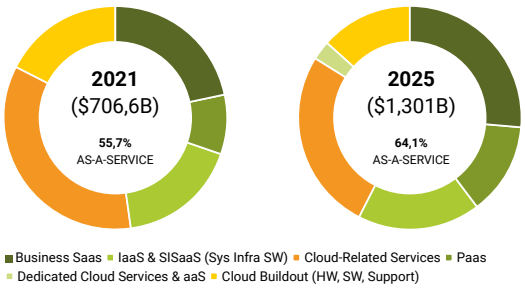
In deze prognose wordt gekeken naar zowel publieke als private clouddiensten. De publieke cloud blijft de grootste en snelst groeiende categorie in de hele cloudmarkt. De gecombineerde uitgaven voor gedeelde clouddiensten – Infrastructure as a Service (IaaS), System Infrastructure Software as a Service (SISaaS), Platform as a Service (PaaS) en Software as a Service (SaaS) – bedragen in 2021 in totaal 385 miljard dollar. Zij zullen tot 2025 een samengestelde jaarlijkse groei (CAGR) van meer dan 21 procent laten zien, tot een bedrag van 809 miljard dollar.

AS A SERVICE

De categorie van de Dedicated (Private) Cloud Services, die bestaat uit gehoste private clouddiensten en het snel opkomende Dedicated Cloud Infrastructure as a Service (DCIaaS)-segment, zal met 31 procent forser groeien, maar vanuit een veel kleinere inkomstenbasis van 5 miljard dollar in 2021.

De as a Service-segmenten van clouduitgaven, waarin door IDC de onderdelen Shared Cloud as a Service en Dedicated Cloud as a Service worden gecombineerd, zullen volgens de prognose goed zijn voor het merendeel van alle clouduitgaven, met een groei van 55,7 procent in 2021 tot 64,1 procent in 2025.

PROGNOSE WERELDWIJDE CLOUDUITGAVEN



Bron: IDC Whole Cloud Forecast 2021-2025: The Path Ahead for Cloud in a Digital-first World.

IT-CARTOON LECTRR

ADVIES VAN IEEE: LEER PYTHON

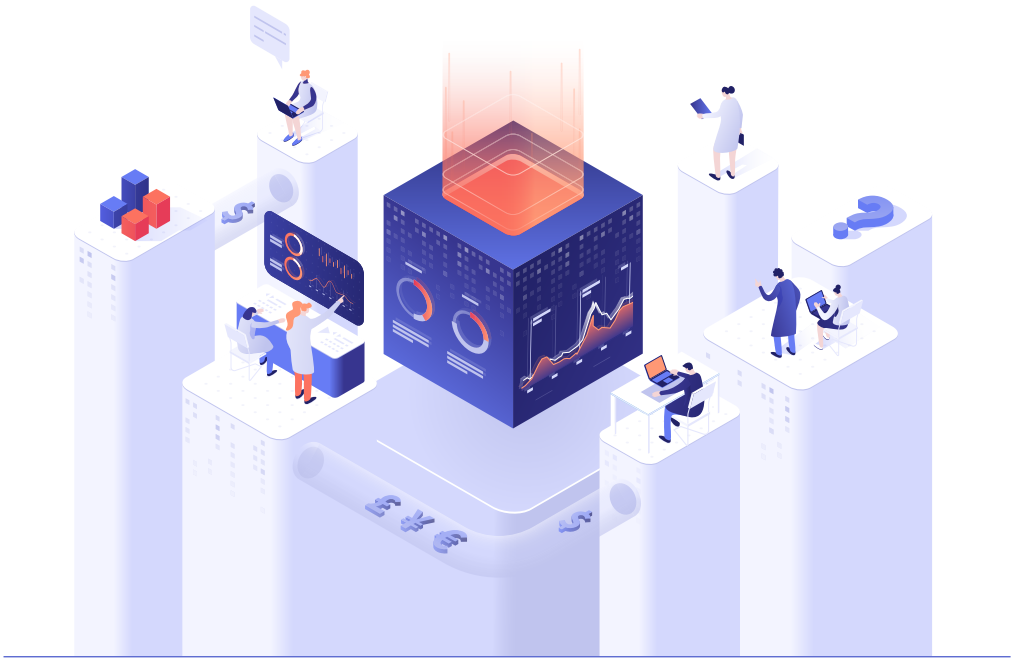
Leer Python: dat is de belangrijkste conclusie uit de jaarlijkse rangschikking van beste programmeertalen, opgesteld door IEEE Spectrum.

Python voert daar dominant de lijst aan, gevolgd door Java, C en C++. “Je hoeft geen door de wol geverfde Pythonista te worden, maar de taal goed genoeg leren om een van de vele ervoor gemaakte library’s te gebruiken, is waarschijnlijk je tijd waard”, luidt het advies van Stephen Cass, special projects editor bij IEEE Spectrum Spectrum. “Eenmaal je de basis van Python onder de knie hebt, komt het erop aan de *ins & outs* van specifieke library’s voor zaken als *embedded* projecten en grootschalige AI-systemen te leren”, stelt hij. “En eerlijk gezegd, afhankelijk van het domein, de complexiteit en/of de kwaliteit van de documentatie, kan het begrijpen van zo’n library aanzienlijk moeilijker zijn dan het leren van Python zelf.”

#	TAAL	SCORE
1	Phyton	100
2	Java	95,4
3	C	94,7
4	C++	92,4
5	JavaScript	88,1
6	C#	82,4
7	R	81,7
8	Go	77,7
9	HTML	75,4
10	Swift	70,4

Maar Python heeft zijn grenzen, voegt Stephen Cass er snel aan toe. “Dat blijkt uit de voortdurende populariteit van talen die beter geschikt zijn om specifieke problemen op te lossen, zoals R, SQL en Matlab. En ook C, C++, Java en JavaScript. Ook zij blijven dominant in de top van de rangschikking, zowel door hun eigen verdiensten als door de enorme bestaande basis van code die in deze talen is geschreven”, stelt hij.

Hoewel er al heel wat high-leveltalen zijn gekomen en gegaan, zal er volgens Cass altijd plaats zijn voor wie bereid is om zo dicht mogelijk bij het *metal* te werken in een of andere assemblagecode. Assembly staat in de lijst overigens op achttien. Ook Arduino duikt erin op: op plaats elf.



WELKOM IN HET TIJDPERK VAN DE GRAPH DATABASE

Deze zomer kondigde databasespecialist Neo4j een investeringsronde van 325 miljoen dollar aan, een van de grootste in een privaat databasebedrijf. Het wijst op de opmars van en interesse in de *graph database*.

Graph databases zijn ontworpen om relaties (edges) tussen gegevenspunten (nodes) weer te geven. Ze maken gebruik van grafiekstructuren voor semantische query's om data weer te geven en op te slaan.

De interesse in deze technologie reflecteert zich dus bij investeerders. De financiële transactie verhoogt de waardering van Neo4j tot meer dan 2 miljard dollar. Emil Eifrem, CEO en medeoprichter van Neo4j, omschreef de financiële injectie als een *inflection point* in de bredere databasemarkt. “Databases vormen de grootste markt op het gebied van bedrijfssoftware. De groei concentreert zich in nieuwe generaties databases die de uitdagingen van vandaag op het gebied van data op ongekende manieren aanpakken”, aldus Eifrem, die met Neo4j naar eigen zeggen driekwart van de Fortune 100-bedrijven bedient.

DIVERSE AANBIEDERS

Nieuw is het concept van de graph database alvast niet. Instagram, Twitter, Facebook, Amazon – en praktisch alle toepassingen die snel informatie moeten bevragen die verspreid is over een dynamisch exponentieel groeiend netwerk van gegevens – maken al gebruik van graph databases. De use cases zijn overigens breed: van fraudedetectie tot aanbevelingen.

Andere graph databases naast Neo4j zijn onder meer ArangoDB, Dgraph, Datastax, GraphDB, Cassandra en Titan. Bij Microsoft is het Azure Cosmos DB. Ook Amazon, dat een politiek hanteert van zogenaamde *purpose driven* databases, biedt met Neptune een eigen graph database.

Ook analisten zien heil in deze databasetechnologie. Volgens Gartner zullen graph-technologieën tegen 2025 worden gebruikt in 80 procent van de data- en analyse-innovaties, tegenover 10 procent dit jaar.

» *Op 16 november organiseert SAI een avondconferentie over Knowledge Graphs.*
Meer info en gratis registratie vind je **hier**.

WAT DOE JE METEEN NA EEN CYBERAANVAL?

Natuurlijk is voorkomen beter dan genezen. Maar heel veel organisaties (groot of klein) krijgen te maken met een cyberaanval (groot of klein). Welke actie onderneem je dan? De recente cyberaanval bij OZ Onafhankelijk Ziekenfonds is een geschikte case die andere organisaties kan inspireren.

OZ getroffen door cyberaanval – belangrijke informatie over Mijn OZ accounts, zo klinkt het onderwerp in de mail die OZ stuurde naar zijn klanten. “OZ Onafhankelijk Ziekenfonds werd getroffen door een cyberaanval. Hackers hadden hierdoor toegang tot klantgegevens. Onmiddellijk na deze vaststelling werd het datalek gedicht. De gelekte gegevens werden niet openbaar gemaakt”, zo luidden de eerste zinnen.

Met deze boodschap informeerde het ziekenfonds de ongeveer 190.000 klanten met een online-account op ‘Mijn OZ’ over de hacking waarvan ze het slachtoffer werd. Maar voor het tot deze communicatie kwam, had de organisatie al een hectische week achter de rug. Wat OZ heeft ondernomen, leest als een plan van aanpak voor elk getroffen bedrijf.

Al zijn er natuurlijk altijd punten van kritiek en is elk geval anders.

Dit zijn de acties die OZ ondernam.

1

HET DATALEK DICHTEN

OZ werd op een dinsdag zelf gecontacteerd door de hacker die het datalek kenbaar maakte. Daardoor kon de organisatie niet meteen inschatten hoe lang de virtuele deur had opengestaan.

In elk geval schoot de IT-dienst van OZ, naar eigen zeggen, meteen in actie toen de hackers meldden dat ze aan data konden in de systemen van het ziekenfonds. “Het datalek werd onmiddellijk gedicht”, communiceerde OZ aan zijn klanten.

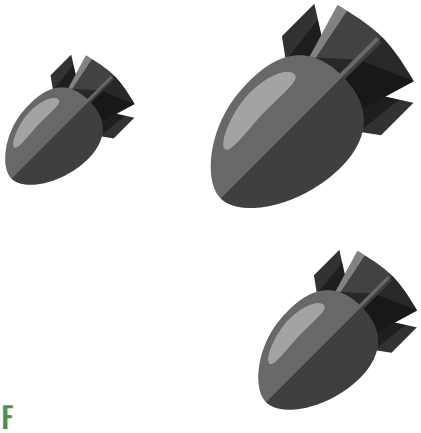
‘Onmiddellijk’, is natuurlijk een relatief begrip in IT-land. In de praktijk was dit ongeveer een dag later het geval. “Daarna hebben we de afgelopen dagen onze systemen meermaals getest. Ook de interne en externe controles en procedures werden extra verscherpt”, klinkt het bij OZ. “Ook onze data protection officer volgt het dossier nauwgezet op.”

2

BEVOEGDE AUTORITEITEN INLICHTEN

Wie te maken krijgt met een datalek van persoonsgegevens kan een melding maken bij de Gegevensbeschermingsautoriteit (GBA) via een elektronisch formulier. Dat deed OZ vrijwel meteen. OZ legde ook klacht neer bij het CERT, het Cyber Emergency Team van de federale overheid.

Vóór het GDPR-tijdperk was de melding van een gegevenslek buiten de telecomsector niet wettelijk verplicht, maar wel raadzaam. Intussen verplicht de GDPR om een gegevenslek te melden aan de bevoegde toezichthoudende autoriteit. Voor België is dit dus de GBA. Alleen als het niet waarschijnlijk is dat het gegevenslek een risico inhoudt voor de rechten en vrijheden van natuurlijke personen, moet het lek niet worden gemeld. In principe meldt de verwerkingsverantwoordelijke het gegevenslek aan de GBA binnen de 72 uur nadat die er kennis van nam.



3

VERWITTIG COLLEGA’S OF SECTORGENOTEN

Hackers gingen tijdens de cyberaanval bewust op zoek naar kwetsbaarheden in het beveiligingssysteem van OZ. In combinatie met een menselijke fout konden er gegevens worden ingekeken, gelinkt aan het online platform ‘Mijn OZ’. Dat is het onlinekantoor waarmee bepaalde transacties met het ziekenfonds kunnen worden afgehandeld.

De hackers gingen aan de haal met persoons- en contactgegevens, bankrekeningnummers, voorkeuren, verzekeringen en betaalinformatie, familiegegevens en volmachten, medische akkoorden en informatie over terugbetalingen, uitkeringen en ziekteperiodes. Wat niet gelekt is, zijn – volgens OZ – klantendossiers en medische verslagen. Ook logins en wachtwoorden zouden niet zijn buitgemaakt.

Het kan best zijn dat hackers ook bedrijven uit dezelfde branche aandoen. Zeker als het om een specifieke of openbare sector gaat. In het geval van de cyberaanval bij OZ informeerde de organisatie ook andere Belgische ziekenfondsen. “Op basis van onze informatie hebben zij ook hun systemen getest”, zei algemeen directeur Rik Selleslaghs hierover later in de media.

4

LOSGELD OF NIET?

Bij veel gevallen, en zeker als het gaat om ransomware, komt de vraag rond het betalen van losgeld aan de orde. De meeste experts raden dit af, behalve als de schade bij niet-betalen erg groot kan uitdraaien.

In het geval van OZ was de keuze gemakkelijker, omdat er data werden ingekeken, maar ze zouden niet zijn versleuteld. De hacker lichtte OZ namelijk zelf in met de Engelstalige boodschap dat het mogelijk was om gegevens te onderscheppen en te verwijderen. Hij of zij eiste losgeld om het incident stil te houden. Het ziekenfonds betaalde niets aan de hackers. Daarop besloot OZ zelf over de cyberaanval te communiceren.

5

KLANTEN INFORMEREN (EN TE WOORD STAAN)

Voor de cyberaanval in de media kwam, informeerde OZ zijn klanten dus via mail. “We nemen de bescherming van uw persoonlijke gegevens bijzonder ernstig”, schreef de organisatie aan zijn klanten. “We excuseren ons dan ook oprecht en blijven er alles aan doen om een nieuwe inbreuk te vermijden.”

Hier rezen wel enkele vragen over de timing. OZ mailde zijn klanten vrijdagavond om 20.00 uur, wat inzake media en (klanten)communicatie een eerder rustige periode was. Volgens sommigen wachtte de organisatie tot dat moment. Wat vervelend was: in de mail van OZ werd voor vragen een telefoon-

Omdat persoonsgegevens gelekt zijn in combinatie met een telefoonnummer, kreeg de organisatie ook de vraag of er een risico is op een zogenaamde sim-swap.

nummer vermeld, maar daar was vrijdagavond niemand bereikbaar. Klanten die belden, kwamen uit op een bandje.

Al ging OZ in het weekend wel over tot verdere actie. Op zaterdagochtend rond 10.00 uur plaatste de organisatie een speciale webpagina online met een Q&A over de cyberaanval. Daarin werd concreet aangegeven wat er was gebeurd, en ook welke data werden gelekt. Ook werden tijdens dat weekend telefoonnummers en mailboxen bemand voor verdere vragen.

Moet een organisatie overigens wettelijk zijn klanten verwittigen? Dit moet in bepaalde gevallen. Wanneer het gegevenslek een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, is de melding namelijk verplicht aan de betrokkenen van wie er gegevens geraakt werden door het lek.

6
DE PERS TE WOORD STAAN

Zodra klanten geïnformeerd zijn, kun je ervan uitgaan dat ook (vak) journalisten contact opnemen met je organisatie, van mails tot telefoons. Op vrijdag konden e-mails niet altijd beantwoord worden. Maar tijdens het weekend stond de OZ-directeur zelf de pers te woord. Op maandag werden, via de woordvoerder, de laatste mails van journalisten met vragen over de cyberaanval beantwoord. De kwestie is dus om altijd iemand aan te duiden die de communicatie, en coördinatie ervan, voor zijn of haar rekening neemt.

7
INSPELEN OP (EN WAARSCHUWEN VOOR) NEVENEFFECTEN

Onvermijdelijk zijn er bij een cyberaanval een aantal *side effects*. Dat was ook bij OZ het geval. Want hoewel de hacker aangaf dat de gegevens waren verwijderd, bleef de organisatie voorzichtig. Het waarschuwde zijn klanten voor phishing als de (persoons)gegevens alsnog misbruikt worden.

Het gaf hierbij ook enkele concrete situaties mee. “Kijk goed naar de afzender, het e-mailadres en spelfouten”, klonk het. En het lichtte ook de manier van werken toe: “OZ vraagt nooit per mail, telefonisch of sms om wachtwoorden te wijzigen of te delen. OZ vraagt nooit om op een link te klikken of om geld terug te storten.”

Omdat persoonsgegevens gelekt werden samen met een telefoonnummer, kreeg OZ ook de vraag of er een risico is op een zogenaamde sim-swap. Daarbij bellen malafide personen naar de provider met de vraag om het telefoonnummer in kwestie over te zetten naar een sim-kaart die in hun bezit is. De controlevragen die de provider dan stelt, zouden te beantwoorden zijn met de gelekte persoonsgegevens. “Maar sinds mei 2020 is een dergelijke sim-swap voor privépersonen onmogelijk zonder visuele controle van de identiteitskaart”, zo stelde OZ de klanten gerust.

OZ nam naar eigen zeggen contact op met de telecomoperatoren. “Zij hebben hun medewerkers opgeroepen om naar aanleiding van de cyberaanval op OZ extra aandachtig te zijn voor dergelijke vormen van fraude.” Of hoe er bij de afhandeling van zo’n cyberaanval wel wat komt kijken. Hadden we al gezegd dat voorkomen beter is dan genezen?

DE GEVALLEN KONINGIN VAN SILICON VALLEY

Met het proces rond Theranos-oprichter Elizabeth Holmes begon een van de grootste fraudezaken in de Verenigde Staten ooit. Wat op het spel staat: de *fake it till you make it*-aanpak die in Silicon Valley nooit ver weg is.

Op haar negentiende richtte Elizabeth Holmes de start-up Theranos op. Het idee achter haar technologiebedrijf was revolutionair: een nieuwe en snelle manier van bloedtesten – snel, accuraat en pijnloos – die de hele medische wereld op zijn kop zou zetten.

ÉÉN DRUPPEL

Theranos – een combinatie van de woorden 'therapie' en 'diagnose' – ontwikkelde een apparaat met de naam Edison, een zwart kastje ter grootte van een koffiezet-apparaat. De technologie kon bloed testen op tientallen aandoeningen, waaronder diabetes en kanker. Een druppel bloed was al voldoende. Zelfs drogisterijketen Walgreens plaatste bloedafname-automaten van Theranos in hun filialen.

Maar uiteindelijk bleken de bloedanalyses erg onbetrouwbaar. In bepaalde gevallen werden de resultaten zelfs vervalst. Theranos pimpte de testresultaten van zijn product op door bloedmonsters in reguliere laboratoria te laten testen. Ook zou Holmes tegen investeerders hebben gelogen over niet-bestaande contracten die het bedrijf zou hebben gesloten.

TEAMSPELER

Bloedfraude beschrijft op een prangende manier de opmars en ondergang van het bedrijf. Het boek van John Carreyrou, die twintig jaar journalist was bij *The Wall Street Journal*, leest als een thriller. En eigenlijk was het dat ook. De auteur sprak met 150 betrokkenen, onder wie 60 (ex-)werknemers van Theranos. Eigenlijk dateert het al uit 2018, maar met het proces van Holmes is *Bloedfraude* opnieuw razend actueel.

Het boek opent met het ontslag van Henry Mosley, de voormalige CFO van Theranos, die zich kritische vragen stelde over proeven en contracten. "Henry, jij bent geen teamspeler. Ik denk dat je beter kunt gaan", zo luidde het vernietigende oordeel van Holmes toen de man zijn ontslag kreeg.

SCHRIKBEWIND

Elizabeth Holmes, als fan van Steve Jobs vaak gekleed met de obligate rolkraagtrui, voerde volgens het boek van Carreyrou jarenlang een schrikbewind. De rechtszaak over de vermeende fraude is mede door COVID-19 (en de zwangerschap van Holmes) uitgesteld, maar raakte uiteindelijk wel gestart. Het is een van de grootste fraudezaken ooit in de Verenigde Staten en een pijnlijke ontknoping voor de vrouw die ooit de jongste selfmade miljardair van de wereld werd genoemd.

Veel start-ups hanteren een fake it till you make it-strategie.

Naast het lot van Holmes zelf komt ook de aanpak in Silicon Valley in het vizier. Veel start-ups hanteren er een *fake it till you make it*-strategie. Wat is er allemaal waar van hun productinnovaties op de PowerPoint-slides, die durfkapitalisten te zien krijgen? Hoever kun je gaan om jezelf te verkopen?

Bloedfraude - Hoe één vrouw uit Silicon Valley de wereld belazerde, John Carreyrou, Xander, 2018, ISBN: 9789401609852

» *Over het proces van Elizabeth Holmes loopt ook een erg interessante podcast-reeks:* ***The Dropout***

VAN COBOL TOT CONFIGURATIE

DEZE ACHT IT-VAARDIGHEDEN NADEREN HUN VERVALDATUM

Als IT'er moet je keuzes maken, ook in de vaardigheden. En op die vaardigheden zet je beter niet meer volop in. De toekomst in IT is namelijk divers: van cloud tot multifunctioneel én van business tot sociaal.

In een recent onderzoek van Deloitte gaf een meerderheid van de CIO's aan dat een derde van de huidige vaardigheden van hun IT-medewerkers in de komende drie jaar niet meer relevant zal zijn. Volgens 68 procent van de door Deloitte ondervraagde executives is de vaardigheidskloof in hun organisatie 'matig tot extreem', terwijl 27 procent die als 'groot' of 'extreem' beoordeelt.

Werk aan de winkel dus. Want als het op vaardigheden aankomt, is diversificatie het geheim van een toekomstbestendige IT-carrière. Het IT-landschap evolueert snel en werkgevers zijn op zoek naar vaardigheden die aansluiten bij hun toekomstige behoeften en wensen. Wij checkten bij enkele IT-specialisten en -recruiters welke IT-domeinen stilaan het einde van hun levenscyclus bereiken.

1/ LEGACY EN ON-PREMISES VAARDIGHEDEN

Door de opkomst van cloud-gebaseerde diensten en de trend naar hybride en remote werkomgevingen is er minder behoefte aan on-premise IT-personeel. Met vaardigheden die puur gericht zijn op fysieke hardware en legacy-systemen wordt je carrière steeds meer beperkt, zeker als je op lange termijn bekijkt.

IT'ers die generalisten zijn met brede vaardigheden, maar geen hedendaagse gebieden beheersen – van cybersecurity tot cloud – zullen waarschijnlijk moeite hebben om relevant te blijven in huidige of toekomstige functies.

Wat natuurlijk ook meespeelt, is dat datacenters hun resources meer en meer naar hyperscalers verhuizen. En bepaalde vaardigheden in het onderhouden ervan zijn door optimalisatie minder nodig. Functies als systeembeheerders en netwerkingenieurs verschuiven stilaan naar nicherollen binnen cyber en cloud.

"In infrastructuur en operations zien we de vraag naar klassieke systeem- en netwerkengineers verlagen ten koste van cloudexperts", bevestigt Jan Goesaert, IT-recruiter en managing director bij AT Recruitment.

Let wel: de behoefte aan basisvaardigheden rond het begrijpen van de integratie van infrastructuur, besturingssystemen en software zal niet verdwijnen. Maar tech-professionals zullen er steeds minder het verschil mee kunnen maken op de arbeidsmarkt.

2/ VEROUDERDE PROGRAMEERTALEN

Het leek wel of de voorbije jaren en maanden een comeback betekende van oudere programmeertalen, zoals Cobol. Het is zo dat er de laatste tijd bij een legacy-vernieuwing wel wat Cobol is gebruikt of opgefrist, maar het gaat hier niet om nieuwe projecten.

"In softwaredevelopment is de vraag naar oudere talen, zoals C, Cobol en RPG, helemaal weggevallen. .NET en Java zijn weliswaar blijvers, maar toch gaat dit eerder ten koste van bijvoorbeeld mobile developers", aldus Jan Goesaert van AT Recruitment. Waar draait het dan om bij mobiele omgevingen? "Onze klanten zijn vooral klassiekere organisaties. Denk bijvoorbeeld aan Katoen Natie, DP World, Lantis of Primagaz. De meeste situeren zich in een Android/Xamarin-omgeving."

3/ SLECHTS ÉÉN PROGRAMMEERTAAL BEHEERSEN

Wie uitblinkt in individuele programmeertalen die momenteel in gebruik zijn, voelt zich misschien veilig, maar de behoefte om meerdere talen te begrijpen, zal de komende jaren snel groeien. Focussen op één taal maakt je carrière dus kwetsbaar. "Vermijd overmatige specialisatie in specifieke producten of nichetechnologieën", zo adviseerde David Wintrich, chief academic officer van bootcamp Tech Elevator, onlangs op CIO.com. "Generalisten zullen zich beter kunnen aanpassen aan veranderende technologielandschappen en beter toegerust zijn om mee te evolueren met de behoeften van organisaties."

"Hard skills zonder soft skills kun je voor 100 procent als 'dead skill in IT' bestempelen."

JOACHIM DESMET,
IT-recruiter bij Amandis

Wat zeker ook meespeelt, is dat de evolutie in de IT-wereld steeds sneller verloopt. In het verleden kon een tech-prof nog een decennium lang één technologie gebruiken. Maar dat is niet langer het geval, oppert David Wintrich. Zo voegen toonaangevende techbedrijven de kennis van tweede en derde programmeertalen toe aan de gewenste vaardigheidssecties van hun functiebeschrijvingen.

4/ SLECHTS ÉÉN DOMEIN BEHEERSEN

Data en security worden vaak als domeinen van de toekomst aanzien. "Wij zien als recruiter inderdaad een *boom* in BI- en dataexperts, devops- en securityprofielen", zegt Jan Goesaert.

De studie van Deloitte bevestigt overigens – ook binnen veelgevraagde gebieden zoals data science – het belang van diversificatie van vaardigheden, vaak omdat teams erg heterogeen worden. Data-analisten bouwen bijvoorbeeld vaak modellen die veel werk vereisen om toe te passen op een productieomgeving, wat leidt tot een relatief nieuw gebied genaamd MLOps. "MLOps-praktijken moedigen communicatie aan tussen uitgebreide ontwikkel- en productieteams, een aanpak die – net als bij DevOps – een breder en groter team van professionals in staat stelt om efficiënter samen te werken om meer gedaan

te krijgen op een gestandaardiseerde manier", klinkt het bij Deloitte.

5/ HANDMATIGE QA

Ook scripted testing is, volgens Deloitte, een IT-vaardigheid die aan het vervagen is. Zo wordt handmatig testen geleidelijk vervangen door cross-functionele teamleden met geautomatiseerde testvaardigheden. Steeds meer organisaties schakelen over op automatisering. "De verschuiving naar agile ontwikkeling en DevOps heeft de behoefte aan omvangrijke *quality assurance* (QA)-teams verminderd."

6/ ALLEEN HARD SKILLS

Bij tech-teams is het meer dan ooit een kwestie van samenwerking. Diegenen die effectief kunnen communiceren, zullen hun waarde zien stijgen. Dat beaamt ook Joachim Desmet, director bij IT recruiter Amandis.

Naast soft skills gaat het uiteraard ook om business skills. Een puur technische ingesteldheid, zonder vermogen om (strategische) gesprekken met bedrijfsleiders te voeren, is niet langer een geschikte aanpak. "Hard skills zonder soft skills kun je voor 100 procent als 'dead skill in IT' bestempelen", stelt Joachim Desmet van Amandis. "Daar blijven wij ook bij onze klanten flink op hameren."

7/ CONFIGURATIE EN BEHEER VAN FYSIEKE MACHINES

Van de totale tijd die IT'ers aan hun werk besteden, zal er minder tijd gaan naar handmatige configuratietaken en handmatige, fysieke verplaatsing van machines. Veel van de fysieke elementen die in sommige tech-functies aanwezig zijn, behoren binnenkort tot het verleden omdat data en software gewoon niet meer op locatie staan.
Kortom, weten hoe je dingen fysiek moet repareren, zal binnenkort geen deel meer uitmaken van de dagelijkse rol van de gemiddelde IT-professional. Tech zal veel minder 'hands-on' worden. Begrijpen hoe dingen werken en hoe ze kunnen worden verbeterd, wordt veel belangrijker.

8/ PRILLE TECHNOLOGIE (ZONDER COMMUNITY)

Deze laatste categorie in ons overzicht is een vreemde eend in de bijt. Het gaat namelijk om skills die eigenlijk nooit echt een volwaardige skill zijn kunnen worden. "Wat ons namelijk ook opvalt in de markt, en wat wij ook zien als een mogelijke dead skill, is innoveren om te innoveren binnen de ICT-sector. Er wordt soms gekozen om te werken in een bepaalde nieuwe technologie die zeker performant is, maar eigenlijk te weinig relevante community kent", verduidelijkt Joachim Desmet van Amandis. "We kennen bijvoorbeeld bedrijven die een tijdje geleden gestart zijn met GO als ontwikkelingstaal, nog andere met Haskell. Maar zij vinden geen mensen die de juiste ervaring hebben met deze ontwikkelingstaal. Dat mist dan zijn doel, in onze opinie. Andere technologieën kunnen dezelfde resultaten bereiken en zijn minstens even performant, alleen zijn ze wat minder hip."

TOCH EVEN OPLETTEN: SOMMIGE SKILLS GAAN LANG MEE

Het is al vaak gezegd: in IT komen er alleen maar zaken (en technologieën) bij en verdwijnt niets echt. En dat geldt eigenlijk ook voor skills. "De aangehaalde dead skills lijken ons terecht uitgepikt en stemmen zeker overeen met hoe wij de markt ervaren. Maar er is een grote 'maar'. Want deze dead skills zijn eigenlijk pas dood – of beter: démodé – binnen grote en moderne omgevingen waarbij IT een cruciale rol speelt. Dit gaat dus voornamelijk op bij de unicorns van de ICT-markt, bij beloftevolle scale-ups, kapitaalkrachtige start-ups of bedrijven die gewoonweg ICT centraal stellen en hierin erg veel willen en kunnen investeren", stelt Joachim Desmet van Amandis.

"AS 400 of RPG blijven erg in trek bij sommige bedrijven."

Maar niet elk bedrijf is volgens hem even *state of the art*. "De grotere kmo's in onze portefeuille, zelfs grote spelers in de bancaire- en digital entertainment-industrie, hebben net deze dead skills nodig om te kunnen blijven draaien. Neem nu *AS 400* of *RPG*, die zijn inderdaad niet langer sexy te noemen, maar blijven erg in trek bij sommige bedrijven", zegt Desmet. "Wij krijgen trouwens nog altijd veel aanvragen binnen, net voor deze dead skills."

“INFRASTRUCTUURTAKEN WORDEN SOFTWARETAKEN”

Filip Michiels is een bruggenbouwer in IT. Hij werkt(e) voor zowel business als IT, zowel bij leveranciers als eindgebruikers en zowel boven als onder de taalgrens. Maar bovenal is hij een *technology believer*. Op 5 oktober geeft hij een avondconferentie voor SAI. “Op de universiteit waren ze blij dat ik weg was, maar uiteindelijk heb ik mijn doel gevonden: IT menselijker maken.”

Filip Michiels is vandaag chief operations officer van Computerland, een afdeling van de Waalse NRB Groep. Michiels was ervoor aan de slag bij reisorganisatie TUI, waar hij zeven jaar CIO was. In 2019 werd hij verkozen tot CIO van het jaar. “Toen ik startte bij TUI had ik minder besef van hoe cruciaal IT wel was binnen het bedrijf”, vertelde hij daar later over.

Zijn studietraject verklapte al zijn wendbaarheid tussen business en IT. De intussen vijftiger studeerde (met lichte tegenzin) computerwetenschappen aan de UGent, daarna bedrijfseconomie aan de universiteit van Antwerpen en later ook IT-management aan de Vlerick Business School. Hij begon zijn loopbaan bij cosmeticabedrijf Estée Lauder, waar hij doorgroeide tot executive manager international information systems. Nadien ging hij werken bij HDP & Arista, Across, Lanxess en Gateway.

Filip Michiels: “Ik ken bedrijven waar kritieke patches maanden blijven liggen.”

DATACENTERS LEEGMAKEN

In Michiels’ ervaring gaat de massa nu pas merken hoe belangrijk technologie is, zo gaf hij eerder aan. Corona hielp hierbij ook wel. Investeringen die vroeger niet zo gemakkelijk te verklaren waren, werden dat ineens wel. “Hoe moeilijk het voor een bedrijf ook is, het is nu gemakkelijker om technologisch vooruit te gaan.”

Michiels is ook een *believer* in cloudtechnologie. Zo koos hij bij TUI voor een *cloud first*-strategie. “We hebben onze datacenters leeggemaakt”, klonk het. Volgens hem is het eenvoudig. “Wat maakt jou anders dan je concurrenten? Als dat niet je IT-park is, is het tijd om naar de cloud te verhuizen”, vindt hij. Die cloud heeft ondertussen een hoge vlucht genomen. “Machines in bedrijf stellen, onderhouden en patchen, is niet de corebusiness van de meeste bedrijven. Ik ken bedrijven waar kritieke patches maanden blijven liggen”, klonk het onlangs tijdens een presentatie op de Infosecurity-beurs.

INFRASTRUCTUUR

Toch heeft amper één Belgisch bedrijf op de vijf momenteel een deugdelijke cloudstrategie, erkent Michiels. “Afhankelijk van welk model je kiest (SaaS, PaaS, IaaS ...) heeft dit een diepgaand effect op hoe je organisatie werkt. Daar komt dus ook een ‘verandermanagement’ bij kijken. Infrastructuurtaken worden softwaretaken. Mensen moeten anders gaan werken en dat is niet altijd gemakkelijk.”

Filip Michiels vertelt graag over zijn soms markante ervaringen doorheen een bijna dertigjarige carrière in IT, die hij doorbracht in verschillende sectoren, landen en posities. Een niet te missen avondconferentie vol storytelling en voorbeelden die aangeven waarom IT zo belangrijk blijft.

» *Bekijk **hier** meer info of registreer je voor dit event.*

DE DERDE WEG IN SOFTWAREONTWIKKELING

Lange tijd moesten bedrijven voor hun nieuwe toepassingen ofwel ontwikkelaars inhuren, ofwel kant-en-klare software gebruiken. Nu is er echter een derde weg: low code/ no code-toepassingen. Maar loopt het echt zo'n vaart? "Binnen een breed IT-landschap zal low code absoluut zijn plaats opeisen."

De trend rond low code en no code valt niet weg te denken. Bedrijven schakelen low code-toepassingen in, of overwegen ze. In de markt van platformen zien we nieuwe namen en veel dynamiek. We vragen een aantal experts – zowel low/no code-adepten als kritische stemmen – waar we vandaag (niet) staan als het gaat om development met low code/no code.

1/ TUSSEN LOW CODE EN NO CODE ZIT ENTERPRISESOFTWARE

Low code en no code gaan vaak samen over de tongen, maar zijn niet hetzelfde. “Vaak worden ze inderdaad samen genoemd, maar er is wel degelijk een verschil”, erkent Jan Vermeulen, director custom software development bij Capgemini. “Het theoretische verschil is dat je met no code geen codering meer hoeft te doen, of kunt doen. Alles is visueel, en gelimiteerd tot wat het platform kan”, vertelt hij. Bij low code wordt er zeer veel visueel geprogrammeerd, maar is er ook nog een uitwijkmogelijkheid naar traditionele code voor zaken die het platform niet out-of-the-box ondersteunt.

Dit verschil is minder triviaal dan je zou denken. “Het gevolg van deze benadering is het échte verschil tussen low en no code: met no code kun je snel kleine, niet-business-kritische toepassingen bouwen. Met échte low code, en dan denk ik aan namen als Mendix en OutSystems, kun je echt enterprisesoftware bouwen.”

2/ CITIZEN DEVELOPERS VERSUS PROFESSIONELE ONTWIKKELAARS

Aswin van Braam, Mendix-specialist bij Ordina, ziet het grootste verschil in de doelgroep en de achterliggende technologie. “Een no code-platform richt zich op de *citizen developer*: iemand zonder noemenswaardige IT-achtergrond.” Via drag & drop kun je een applicatie maken op basis van kant-en-klare stukjes code. “Dit zal in de basis eenvoudige applicaties opleveren. Een no code-platform maakt gebruik van webtechnologieën zoals HTML en JavaScript.

Low code kan de klassieke buy versus build-beslissing meer doen kantelen richting build.

Een low code-platform richt zich daarentegen op de professionele ontwikkelaar. “Hoewel ook hier gebruik kan worden gemaakt van een visuele bouwstijl, is het ook mogelijk om zelf code te wijzigen of te schrijven, waardoor je complexe(re) applicaties kunt ontwikkelen. Low code-platformen gebruiken Java en/of .Net.”

Volgens Aswin van Braam is net de combinatie van no code en low code ijzersterk. “Hiermee leg je de verbinding tussen business en IT. De business kan de logica achter een oplossing beter begrijpen omdat die visueel is. En IT kan de behoeften van de business beter begrijpen. Een platform als Mendix, dat we veel gebruiken bij Ordina, zorgt voor een naadloze verbinding tussen low code en no code.”

3/ HET LEGOBLOKJE: DE DERDE WEG IN SOFTWARE

Is low code/no code effectief de derde weg tussen maatsoftware enerzijds en de zogenaamde COTS (*commercially available off-the-shelf*) anderzijds, zoals Harvard Business Review recent liet uitschijnen? Daarover verschillen de meningen.

Abhishek Roy, geo practice head UK & Europe voor low/no code bij TCS, vindt van wel en hanteert hierbij de metafoor van legoblokjes. “Klassieke ontwikkeling kun je vergelijken met beginnen met plastic grondstof om elk legoblokje zelf

Aswin van Braam (Ordina): “Een low code-platform richt zich op professionele ontwikkelaars.”

te bouwen. Terwijl *off the shelf* de speelgoedvrachtwagen zal zijn die je koopt met weinig of geen ruimte voor aanpassing of uitbreiding", stelt hij. Low/no code is, volgens hem, het best te vergelijken met de legoblokjes zelf. "Je bouwt kleine, op het doel afgestemde componenten die onafhankelijk kunnen worden gebruikt en naar behoefte kunnen worden uitgebreid of opgeschaald."

Marc Schijvaerts, managing director bij PeopleWare, is iets kritischer. "No/low code maakt alles wat laagdrempeliger en kan zeker zijn plaats vinden in eenvoudige rechttoe rechtaan softwareapplicaties", oppert hij. "Het zal zijn plaats verwerven aan de onderkant van de klassieke ontwikkelingsprojecten, maar is in de huidige vorm niet geschikt om complexe softwaretoepassingen mee te bouwen. Voor *off the shelf* producten zie ik ook niet direct veel concurrentie."

4/ EERDER DE DERDE VERSNELLING

Derde weg of niet. Impact kan low code creëren, ook omdat de benadering anders is. "Low code versnelt softwareontwikkeling. Op die manier kunnen zowel de *time to market* als de kosten van klassieke ontwikkeling drastisch verlagen, en zo de *buy vs build*-beslissingen meer doen kantelen richting *build*", meent Jan Vermeulen van Capgemini.

Daarbij moet je, zo voegt hij eraan toe, ook rekening houden met de licentiekosten voor het gebruik van het low code-platform. Wat low code inderdaad doet positioneren tussen klassieke ontwikkeling – op maat, geen licentiekosten maar wel grotere *build cost* en lagere *time to market* – enerzijds en *off the shelve* anderzijds: niet op maat, met licentiekosten en (in theorie) beperkte aanpassingskosten. "Low code brengt oplossingen op maat, heeft licentiekosten, een snelle time to market en beperktere ontwikkelingskosten", vat Vermeulen samen.

Jan Vermeulen (Capgemini): "De toekomst van ontwikkeling wordt hybride".

5/ NEED FOR SPEED EN WAR FOR TALENT ALS DRIJFVEREN?

Toegankelijkheid naar andere IT-profielen en snelheid zijn belangrijke factoren voor low code. "De belangrijkste drijfveer is ontegenzeggelijk de behoefte aan snellere levering, aangezien bedrijven er voortdurend naar streven om meer bedrijfswaarde te creëren in minder tijd", weet Abhishek Roy van TCS. Hij wijst ook op een hypervraag rond digitalisering die werd versneld door de pandemie.

"Vandaag kijken IT'ers vaak nog argwanend naar low code-platformen."

Ben van der Linden van iO (het vroegere Intracto), die in Nederland een softwareteam aanstuurt dat al zeven jaar oplossingen bouwt met Outsystems, licht het aspect snelheid verder toe. "Het gaat om de mogelijkheid om snel functionaliteit op te leveren en snel aanpassingen of uitbreidingen door te voeren", weet Ben van der Linden. Maar het gaat verder dan dat. "Denk aan eenvoudige integraties met externe systemen met behulp van API's of een SQL-databasekoppeling", vult hij aan. "Wat ook speelt, is dat het low code-platform veel technische taken uit handen neemt, zoals responsieve UI, database transactions, user management, error logging enzovoort. Een project wordt hiermee minder complex en de focus kan liggen op de businesslogica."

Marc Schijvaerts, managing director bij PeopleWare, ziet ook de markt bewegen. "Ik zie ook klassieke softwareontwikkelingsbedrijven op de kar springen van no/low code. De drijfveer voor hen is duidelijk: een snelle oplevering tegen een competitieve prijs", vindt hij. "No/low code-platformen verlagen zeker

en vast de drempel om software op maat te maken, zonder over een brede en diepgaande IT-kennis te beschikken. Het is zowat de eenvoudige Filemaker, Dbase of Access van decennia geleden."

6/ VAN RAD NAAR LOW CODE: OUDE WIJN IN NIEUWE ZAKKEN?

Doet low/no code niet denken aan *Rapid Application Development* (RAD) van weleer? Dat moest ook het ontwikkelingsproces versnellen. Abhishek Roy van TCS ziet evenwel verschillen. "RAD was meer gericht op het bouwen van zogenaamde point solutions, wat resulteerde in applicatiesilo's. Terwijl low code-platforms – naast RAD-mogelijkheden – organisaties de mogelijkheid bieden om *end-to-end customer journeys* te bouwen. En dat in één platform met de vereiste workflow, omnichannel-gebruikersinterface, integraties, cloud enablement en uitbreidbare fit-for-purpose-oplossingen."

7/ OP NAAR HYBRIDE ONTWIKKELING VAN SOFTWARE

Wordt de toekomst van softwareontwikkeling sowieso hybride? En dus traditionele ontwikkeling én low/no code? "Het eenvoudige antwoord op deze vraag is ja", stelt Jan Vermeulen van Capgemini. "Net zoals de pakketindustrie een hybride vorm heeft samen met klassieke ontwikkeling. Bekijk maar eens hoeveel *custom add ons* in ABAB, Java of SAPUI er op een typische SAP-implementatie worden gebouwd", klinkt het. "Zo zal ook low code hier z'n plaats krijgen en kunnen er bijvoorbeeld mobiele apps en customer portals gebouwd worden met low code, en de API's die zij zullen aanspreken met klassieke ontwikkeling of beschikbaar door een pakket", voorspelt Vermeulen. "De low code *pure players* zoals OutSystems en Mendix zijn wel op weg om de noodzaak voor klassieke ontwikkeling steeds meer te verkleinen."

Aswin van Braam van Ordina ziet een hybride situatie ontstaan met meerdere technologieën, zowel high als no/low code, in een organisatie. De toekomst is volgens hem de combinatie van beide ontwikkelingsmethodes. "Er zullen in de toekomst meerdere no/low code-platformen binnen een organisatie aanwezig zijn, net zoals dit nu ook al het geval is met high code", meent hij. "Afhankelijk van de beschikbaarheid van ontwikkelingscapaciteit en behoefte aan innovatie, komt er wel een shift naar een groter percentage softwareontwikkelingstrajecten die met low code zal worden ingevuld."

"Low/no code is de eenvoudige Filemaker, Dbase of Access van decennia geleden."

Bij Gartner Digital Markets, waarmee we ook contact opnamen voor dit SAI-dossier, laat marketingspecialist Gijs Eras één Gartner-onderzoek en percentage vallen: 65 procent. "De verwachting is namelijk dat vanaf 2023 maar liefst 65 procent van de softwareontwikkelingstrajecten met een no/low code-platform wordt ingevuld."

8/ DE TOEKOMST IS LOW (OR NO)

Ook volgens meer klassieke softwarebedrijven is low/no code *here to stay*. "De toekomst van softwareontwikkeling wordt inderdaad hybride, daar ben ik vrijwel zeker van", aldus Marc Schijvaerts van PeopleWare. Vandaag kijken IT'ers vaak nog argwanend naar no/low code-platformen. Voor eenvoudige zaken zoals het CRUD-beheer (*create, read, update, delete, n.v.d.r.*) van data in lijstjes, is no/low code ideaal. Complexe processen vragen nog altijd het schrijven van aangepaste code door een ervaren IT-professional. Maar binnen een breed en gemengd IT-landschap zal no/low code absoluut zijn plaats opeisen", voorspelt hij. "Het zou me niet verbazen mochten we binnen afzienbare tijd enkele overnames zien van no/low code-platformen door grote spelers zoals Microsoft of Amazon."

KAN LOW CODE DE HOGE VERWACHTING INLOSSEN?

VIER REALITYCHECKS

Hoe zit het met de projecten, platformen, technologie, samenwerking en uitdagingen rond low code?

Realitycheck 1

WELKE PROJECTEN KOMEN IN AANMERKING?

Wordt low code nog altijd geassocieerd met kleinere, afgelijnde projecten? “Er zijn hiervoor geen specifieke richtlijnen. We zien de low code-adoptie bij bedrijven ook verschuiven van *point solutions* naar mainstream digitale transformatie”, antwoordt Abhishek Roy, geo practice head UK & Europe voor low/no code bij TCS. “Low code-adoptie kent een sneeuwbaleffect. Het is zich in veel organisaties aan het uitbreiden over bedrijfsfuncties en divisies. De meeste programma's zijn gericht op betere operationele efficiëntie, vereenvoudigde klantervaring, legacytransformatie en meer automatisering.”

Eigenlijk kunnen we vandaag met low code alle soorten applicaties ontwikkelen, oppert Aswin van Braam, Mendix-specialist bij Ordina. “Zo worden complete portalen met miljoenen gebruikers en complexe, hoog transactionele processen hiermee ontwikkeld. Ook de Zorg-app die wij voor Nederlandse verzekeraar VGZ realiseerden op basis van het Mendix-platform is een goed voorbeeld: die is voor miljoenen verzekerden.”

Ook Ben van der Linden van iO wijst op de reikwijdte. “De projecten die wij ontwikkelen in Outsystems, en dus met low code, zijn heel divers. Dat gaat van integratie- en servicelagen, backoffice-webapplicaties en mobile businessapps.” Van der Linden wijst op een project bij een klant waar een servicelaag werd ontwikkeld op de centrale ledendatabase. “Hierin worden tientallen verzoeken per seconde verwerkt. Low code wordt dus niet alleen voor kleinere projecten ingezet.”

WELKE PROJECTEN NIET?

Wat, volgens Ben van der Linden, minder goed werkt, zijn webapplicaties (of mobile apps) waarbij het design en de gebruikerservaring 100 procent bepalend zijn, zoals een websitedesign op maat. “Je hebt hiermee geen voordeel van de bouwdoos met UI-elementen en het platform kan tegen je werken omdat je om bepaalde standaardoplossingen heen moet werken”, stelt hij. “Wat vaak ook geen goed idee blijkt, is een maatwerkapplicatie die na oplevering niet meer doorontwikkeld wordt. Dit omwille van de licentiekosten van bijvoorbeeld Outsystems die je doorlopend moet betalen.”

Volgens Aswin van Braam van Ordina moet er vooral worden gekeken naar de architectuur en de onderlinge samenhang van data in de systemen. “En natuurlijk waar je het eventueel nog meer voor gaat gebruiken. Een *one-off* website bouwen in Mendix is geen goed idee. Als dit echter een van de vijf à twintig applicaties is waarvoor je low code kunt gebruiken, dan kan het ineens wel een goed idee zijn.”

Volgens Marc Schijvaerts, managing director bij PeopleWare, laat low code vandaag niet toe om complexe software te bouwen. “Laat staan dynamisch schaalbare *high throughput* dataverwerking”, oppert hij. “Low code is zeker geschikt voor toepassingen die voor een heel groot stuk CRUD zijn – zuiver data-entry, met validaties, maar zonder veel andere complexe of complexere logica”, meent hij. “Ook voor PoC's (*proof of concepts*, n.v.d.r.) en MVP’s (*minimum viable products*, n.v.d.r.) kan dit een goede aanpak zijn, om te kijken of er effectief een markt is alvorens de echt grote ontwikkeling aan te vatten. Een groot gevaar is echter de lock-in van het gebruikte low code-platform of ecosysteem en de mogelijkheid tot migratie nadien.”

Realitycheck 2

ZIJN DE LOW CODE-PLATFORMEN MATUUR GENOEG?

De markt voor low/no code-platformen is breed en groeit, stelt Jan Vermeulen, director custom software development bij Capgemini. “Voor 90 procent van deze markt wordt beter alleen

gekozen voor kleinere, minder schaalbare toepassingen. Voor de twee leiders in de low code-markt – OutSystems en Mendix – is het mogelijk om ook echt *enterprise software* te bouwen. Er zijn geen grenzen aan de platformen en ook op het vlak van schaalbaarheid zijn ze *enterprise grade*."

Volgens Vermeulen kun je de markt van low/no code vandaag indelen in drie grote segmenten. Ten eerste de *low code pure players* zoals Mendix en OutSystems die toelaten om full stack custom businessapps te bouwen. "Beide zijn ruim tien jaar oud en hebben ondertussen een brede waaier aan referenties bij internationale bedrijven."

Ten tweede zijn er de ecosystemen met low code. "Daar gaat het om grote softwarebedrijven zoals Salesforce, Pega, Appian. Zij maken gebruik van het low code-paradigma – zeg maar visueel programmeren – om hun bestaande software te laten aanpassen of uitbreiden."

Ten derde zijn er, volgens Vermeulen, de no code-leveranciers. "Een waaier van kleinere spelers die een platform aanbieden dat beperktere toepasbaarheid heeft. Hier duiken namen op als *Appsheet* van Google en *Honeycode* van Amazon." Een speciale plek is er voor Microsoft Power Platform. "Dat is gepositioneerd tussen de eerste twee segmenten: er is vrij veel mee mogelijk, maar de hoofdfocus is uitbreiding van O365- of Dynamics-platformen."

Ook Abhishek Roy van TCS ziet grofweg drie categorieën: *pure play low code*-platforms met als doel om sneller applicaties te ontwikkelen via tools en connectors. "Ten tweede low code-platformen om complexe mogelijkheden voor businessprocessmanagement aan te pakken voor het digitaliseren van bedrijfsprocessen en casemanagement. En ten derde bedrijfssoftwareoplossingen die hun componenten uitbreiden om de flexibiliteit van lowcode te bieden", aldus Roy. "Elk platform heeft zijn eigen sterktes en zwaktes die geëvalueerd moeten worden ten opzichte van de prioriteiten van de organisatie."

Realitycheck 3

HOE VERHOUDT LOW CODE ZICH TEN OPZICHTE VAN DEVOPS?

Zowel low code als Devops draait rond applicaties van hoge kwaliteit ontwikkelen in een snel tijdsbestek. "Maar ze pakken het op verschillende manieren aan", oppert Abhishek Roy. "Devops door de traditionele IT-ontwikkeling te optimaliseren met specifieke tools en technologieën. Low code door de business een *single visual fabric* te bieden om snel wensen toe te passen en een gevoel van controle te geven", oppert hij. "Realistisch gezien is het in een hybride softwareontwikkelingsscenario nodig om de low code-technologieën te integreren met het Devops-framework voor hoge kwaliteit en verbeterde governance en controle."

DE MARKT VAN LOW/NO CODE IS EEN DRIELUIK

1
Pure players
(Mendix, OutSystems, ...)

2
Ecosystemen
(Salesforce, Pega, Appian, ...)

3
No code-leveranciers
(Google Appsheet, Amazon Honeycode, ...)

Ook Jan Vermeulen ziet brood in die integratie. "Devops gaat in principe over het nauwer laten samenwerken van verschillende stakeholders in een softwareontwikkelingsproject met developers, infrastructuurmensen (ops), maar ook zelfs business in het kader van *BIZdevops*. Low code speelt hier ook erg op in: visueel programmeren versterkt de samenwerking tussen developers en business."

Realitycheck 4

WAT ZIJN DE UITDAGINGEN ROND NO/LOW CODE VOOR DE IT-AFDELING?

Heel wat, zo blijkt. "De eerste uitdaging waarmee de IT-afdeling wordt geconfronteerd, is het hoge tempo waarin ze het low code-platform moeten inpassen in hun ecosysteem, rekening houdend met hun bedrijfsstrategie en -standaarden", stelt Abhishek Roy van TCS. Dit kan een continu proces zijn, omdat grote bedrijven de neiging zullen hebben om te zoeken naar meerdere *fit-for-purpose* low code-applicaties en -oplossingen."

Een andere uitdaging is, volgens hem, om zo snel mogelijk een Centre of Excellence (CoE) op te richten. "Dat is een cruciaal onderdeel van het low code-traject en helpt valkuilen te vermijden door het vereiste kader en overzicht te bieden. Low code-adoptie mag niet eindigen in het creëren van applicatiesilo's op businessportfolioniveau."

Vaak liggen de uitdagingen in *governance* en het vermijden van *shadow IT*, beaamt Aswin van Braam, Mendix-specialist bij Ordina. "Ook merken we in de praktijk dat het overtuigen van interne stakeholders van de kwaliteit en veiligheid tijd vergt. De business wil snel en IT wil mee. Maar hoe geef je iedereen het vertrouwen dat de nieuwe, snellere oplossing ook voldoet aan de benodigde standaarden?", oppert hij. "Een andere uitdaging is dat er door low code een *shift* ontstaat in de benodigde vaardigheden. Niet iedere IT-organisatie is daar klaar voor."

AFVALBEHEER VIA LOW CODE

Indaver, de Belgische verwerker van gevaarlijk industrieel afval, koos ervoor om zijn digitale bedrijfsprocessen te verbeteren en creëerde een suite van low code-applicaties om het beheer, het transport, de recycling en de afvoer van meerdere afvalstromen over internationale grenzen in te richten.

De apps, ontwikkeld door Indaver, omvatten een native mobile app voor afvalinzameling en een digitale oplossing die QR-codescanning gebruikt voor track & trace van de supplychain van afvalbeheer.

DRIE MAANDEN

Indaver ging in zee met Mendix en ontwikkelde apps die grafische planning van afvalverwerking en documentstromen mogelijk maken. Dit moet ervoor zorgen dat gevaarlijk afval wordt afgehandeld volgens de geldende regels in Europese landen, waaronder België.

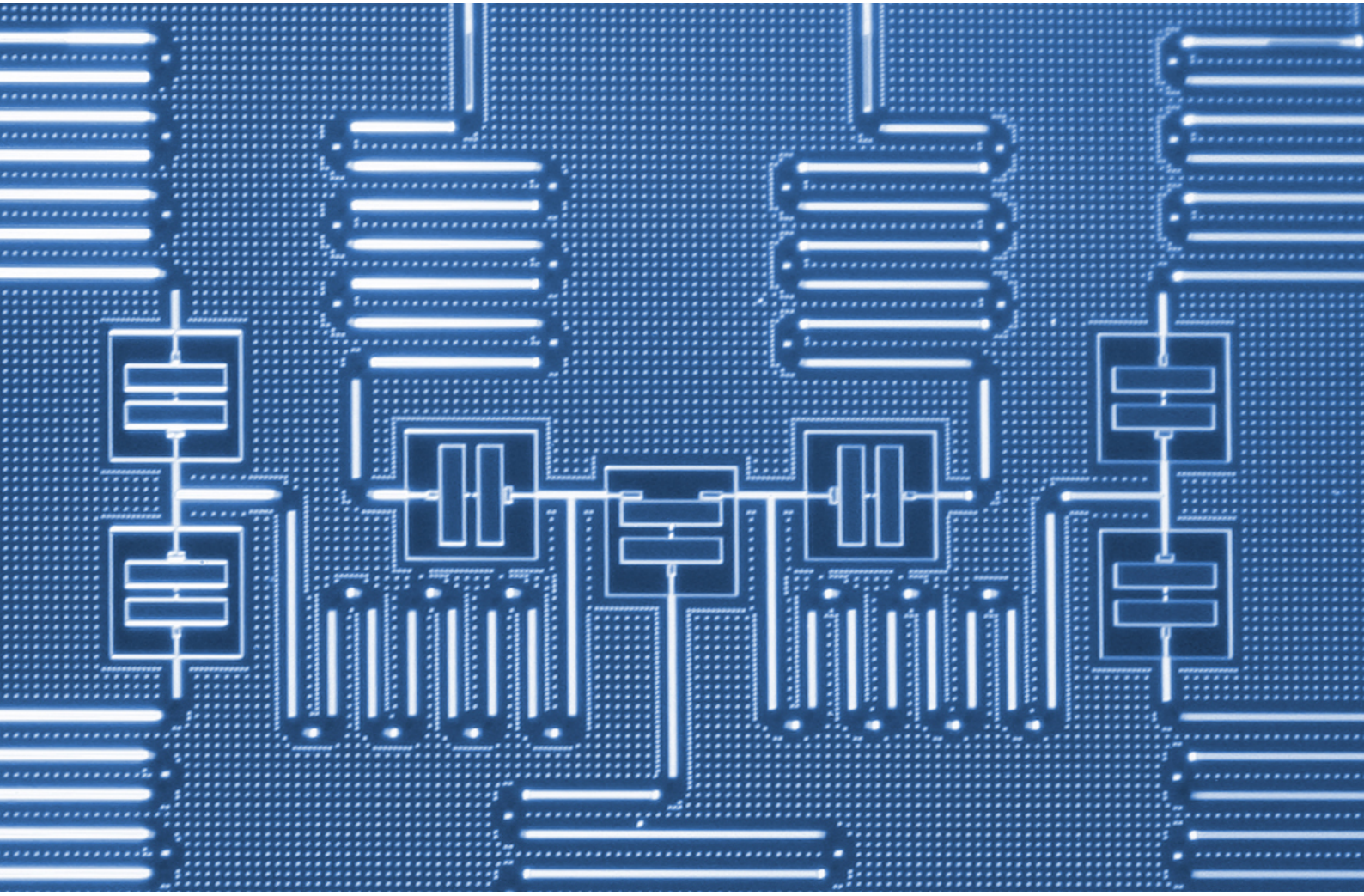
Om met het platform aan de slag te gaan, creëerde Mendix-partner Mendify een competentiecentrum bij Indaver, mede om het personeel te trainen om het low code-platform te kunnen gebruiken. “De bouw ervan nam maar drie maanden in beslag”, zegt Annick Van Driessen, international director supply chain operations.

BACKENDINTEGRATIE

Naast de track & trace-app bouwden Indaver en Mendify onder meer ook het *Waste Property Passport*. Afval bestaat doorgaans uit veel complexe onderdelen. Deze data worden opgeslagen in meerdere systemen, waaronder SAP. De Mendix-backend integreert alle data. Dit is met name van belang bij de verwerking van gevaarlijk afval.

Bovendien kunnen klanten van Indaver nu zelf de eindcontrole doen in de app. Tot voor kort werden afvalkenmerken gecontroleerd door de klant en Indaver via e-mail, telefoon en bezoeken op locatie. Door het Waste Property Passport te gebruiken, is volgens Indaver de foutmarge door verkeerde interpretatie verkleind. In het verleden kon informatie uit e-mail namelijk afwijken van de data in het ERP-systeem. “De app biedt nu één versie van de waarheid, en dat vermindert ook de risico’s.”

Indaver koos voor low code voor hun apps rond grafische planning van afvalverwerking en documentstromen.



VIJF CRUCIALE VRAGEN OVER QUANTUM COMPUTING

Quantum computing is een compleet andere manier van rekenen dan wat we al zes decennia lang doen met onze actuele computers, ook wel 'classical computing' genoemd. Quantum computing richt zich op problemen die vandaag te veel rekentijd vragen of onoplosbaar zijn met onze traditionele computersystemen. En dit in een aanvaardbare doorlooptijd, via uitvoering van één of meerdere quantum algoritmen. Maar wat betekent dat concreet?

Dit artikel ambieert een aantal vraagtekens uit te wissen: waar staan we met quantum computing? Is het de moeite waard om erin te investeren en zo ja, hoe en wanneer? En stel dat je er dan ook in gelooft, hoe begin je met je quantum journey?

1

Waarom krijgt quantum computing zo veel aandacht?

Wat maakt dat bondskanselier Angela Merkel in hoogsteigen persoon de inauguratie van de eerste quantum computer in Duitsland met een speech mee introduceert? Hoe komt het dat de recente Qiskit Summer School 2021 meer dan duizend studenten ertoe beweegt om in de vakantiemaand juli tien opeenvolgende dagen een cursus te volgen over quantum machine learning (QML) en grensverleggende oefeningen te maken met Python? Waarom volgt het Vlaams Supercomputer Centrum de laatste evoluties op het vlak van quantum computing op? Waarom organiseren alle Belgische en Luxemburgse universiteiten extra sessies rond quantum computing voor hun studenten, doctorandi en onderzoekers?

Wel, in heel wat actuele maatschappelijke, wetenschappelijke, economische en bedrijfskundige vraagstukken van vandaag kun je eenvoudigweg geen vooruitgang boeken zonder computersimulaties. Denk aan het ontwerpen van nieuwe materiaalcomposities, het samenstellen van nieuwe chemische stoffen met minimale milieu-impact, het oplossen van optimalisatievraagstukken voor onze mobiliteit, het ontdekken van nieuwe medicijnen en vaccins: supercomputersimulaties zijn een *conditio sine qua non*.

Jammer genoeg bereiken we met deze berekeningen de limieten van klassieke computers. Voor vele problemen vinden we geen oplossing binnen een aanvaardbare tijdslimiet, en andere problemen kunnen we gewoon niet simuleren wegens te hoge complexiteit. Voor nog andere moeten we ons tevredenstellen met ruwe benaderingen, terwijl we accurate resultaten willen. Dit is de niche waarin quantum computing zijn rol kan spelen, samen met (maar niet ter vervanging van) classical computing.

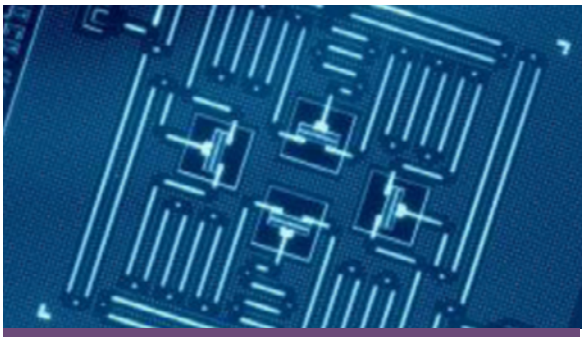
2

Wat is het fundamentele verschil tussen quantum computing en classical computing?

Tot welke fenomenale digitale revolutie onze traditionele computers ook geleid hebben, de basis rekeneenheid blijft nog altijd de bit, die op een gegeven ogenblik in de tijd ofwel de waarde 0 ofwel de waarde 1 aanneemt. En met deze 0 en 1 exploiteren we het binaire talstelsel, op basis van een aantal booleaanse operatoren zoals NOT, AND, OR, NAND en XOR. Dit fundament is nog altijd het basisprincipe, gaande van onze smartwatch tot de krachtigste high performance computer.

Quantum computers rekenen met quantum bits of qubits. Qubits kunnen op een gegeven ogenblik in de tijd niet alleen de waarde |0> of |1> aannemen, de zogenaamde 'ground state' en 'excited state', maar ook een lineaire combinatie van |0> en |1>, zeg maar $\alpha|0> + \beta|1>$, waarbij de coëfficiënten complexe getallen zijn. Dit fenomeen, superpositie genoemd, is niet alleen een wiskundige beschrijving, het is een natuurlijke realiteit die je aantreft op het niveau van moleculen, atomen en subatomaire deeltjes, beschreven in de quantum mechanica.

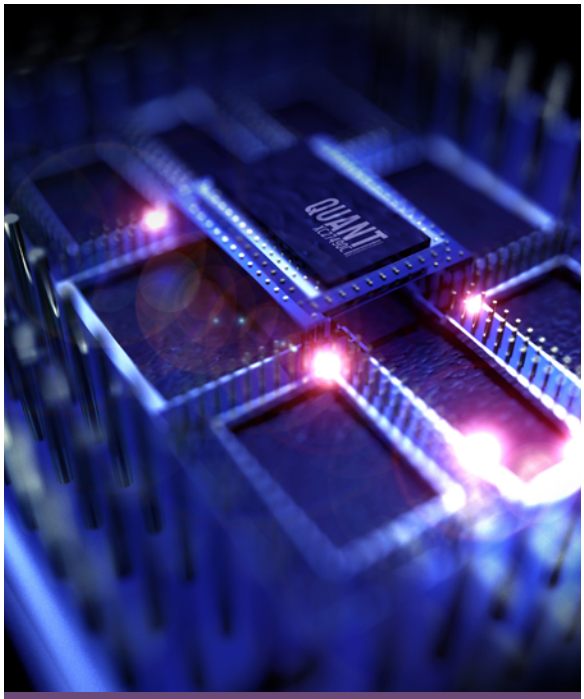
Superpositie is evenwel een zeer tijdelijk fenomeen: wanneer je de qubit onderwerpt aan een meting, zakt de superpositie in elkaar tot een klassieke meetwaarde 0 of 1. De grote progressie met quantum computers sinds 2016 is onder andere precies de verlenging van deze superpositietijd, in de grootteorde van microseconden. Deze tijdsintervallen zijn evenwel voldoende om te rekenen met een qubit. Rekenen met een quantum computer kan, mits de toepassing van een aantal operatoren, ook wel gates genoemd. Een quantum computer biedt dan ook een gate aan die een qubit in de 'superposition state' kan brengen, met name de Hadamard-gate (H).



HOE WORDEN QUBITS GEMAAKT?

Er zijn verschillende technologieën in gebruik en er wordt continu onderzoek gedaan naar de productie van qubits met een hoge mate van stabiliteit en kwaliteit. Momenteel zien we dat superconducting qubits (IBM, Google) en trapped ions (IonQ) de technologieën zijn met de beste resultaten. IBM heeft een traject uitgestippeld om in 2023 een toestel te bouwen met 1.121 qubits en vervolgens zelfs miljoenen qubits. Anno 2021 zijn dat er nog slechts 65.

Een tweede karakteristiek die we niet terugvinden in een klassieke computer en die een enorme versnelling en toename in parallelisme van de berekeningen mogelijk maakt, is verstrengeling of entanglement. Ook dit is een natuurlijk fenomeen, dat theoretisch bewezen werd door Einstein, Podolski en Roosen in 1935 en later ook wetenschappelijk werd geobserveerd. Het komt erop neer dat wanneer je de status van de ene qubit kent of aanpast, automatisch ook de status van een andere qubit bekend is of mee aangepast wordt. De conditionele NOT-gate (CNOT) laat toe om twee qubits in een entangled status te brengen.



HEBBEN WE BINNENKORT EEN QUANTUM COMPUTER IN HUIS?

Het antwoord op deze vraag is neen. De actuele quantum computers functioneren alleen in zeer specifieke omstandigheden en vragen heel wat kennis om een toestel operationeel te maken en te houden. Superconducting qubits, bijvoorbeeld, werken alleen op een betrouwbare en stabiele wijze in een temperatuur van 15 millikelvin, wat kouder is dan in de ruimte buiten de aardse atmosfeer. Quantum computing zal dus onder de vorm van cloud computing aangeboden worden, vanuit een aantal zeer gespecialiseerde datacenters. Via **deze link** vind je bijvoorbeeld quantum computers waarop je al gratis experimenten kunt uitvoeren.

3

Wat is een quantum circuit?

Naast de H- en CNOT-gates bevat een quantum computer nog talrijke andere operatoren, en de uitdaging is dan om een quantum circuit te ontwerpen. Een quantum circuit is geen hardwarebegrip, maar eigenlijk een quantum programma: een aantal qubits wordt geinitialiseerd, gemanipuleerd met de juist bedachte gates in de juiste combinaties en volgorde, en tot slot uitgelezen in klassieke bits, om te komen tot een combinatie van 0- en 1-waarden. Dit logische blok van operaties wordt herhaalde keren uitgevoerd (elke uitvoering noemt men een ‘shot’) om te komen tot een combinatie met een veel hogere frequentie dan alle andere bit-combinaties. De bit-combinatie met de hoogste frequentie of waarschijnlijkheid is het antwoord voor het gestelde probleem. Dé grote uitdaging is dus om te starten met zinvolle qubit-initialisaties, gevolgd door betekenisvolle gate-specificaties die de problematiek en de oplossing representeren. Dit laatste vraagt nog altijd veel research en is vaak gebaseerd op constructieve wiskundige redeneringen en bewijsvoeringen.

WAT ZIJN DE BELANGRIJKSTE QUANTUM GATES?

Naast de Hadamard- en CNOT-gate worden ook de Pauli-gates (aangeduid met X, Y, Z, I) en hun rotatie-varianten (RX, RY, RZ) zeer veel gebuikt. Andere gates zijn S, T, SDAG, TDAG, SWAP en Toffoli. Maar dit is lang niet alles. Je vindt **hier** een mooi overzicht.

Belangrijk is dat een gate een reversibele operatie moet zijn en voor de wiskundigen onder ons: een gate komt overeen met een unitaire matrix, een qubit met een kolomvector en een combinatie van meerdere qubits met het tensorproduct.

4

Wat zijn de typische toepassingsgebieden die op de radar staan?

Het eerste toepassingsgebied werd ooit door ene Richard Feynman bestempeld als de grote drijfveer voor quantum computers: quantum chemie en zijn brede toepassingsdomein. Denk aan moleculen modeleren, materialen ontwerpen en de energie gegeneerd door chemische reacties bepalen en exploiteren. Concreet denken we hier aan het ontwerpen van batterijen die een langere autonomie hebben, gekoppeld aan een lagere impact op het

milieu, het ontwerpen van nieuwe antibiotica en vaccins of het efficiënter benutten van fossiele brandstoffen.

Een tweede domein is quantum machine learning (QML), zeg maar het gebruik van quantum computing om algoritmen voor machine learning te verrijken met meer zogenaamde features of dimensies, of sneller tot accurate classificaties en patroondetectie te komen. QML maakt typisch gebruik van een hybride aanpak, waarin quantum en classical computing elkaar aanvullen.

Een derde beloftevol domein zijn allerlei optimalisatievraagstukken, zoals het bekende handelsreizigersprobleem (traveling salesman) en het probleem van de maximale snede (maxcut). De financiële wereld heeft zich ook al sterk toegelegd op research over quantum computing, met focus op risicoanalyse, kredietscoring, portfoliosamenstelling en vervangers van Monte Carlo-simulaties.

5

Welke quantum developers zijn er (binnenkort) nodig?

Quantum developers zijn nodig op drie fronten. Ten eerste hebben de producenten van quantum toestellen kernel developers in dienst, die ervoor moeten zorgen dat de quantum gates en de aanverwante quantum circuit operaties zo efficiënt mogelijk uitgevoerd worden. Ze werken ook mee aan de ontwikkeling van transpilers, die een circuit met abstracte gates omzetten in een logisch equivalent circuit met gates die fysiek toegepast zijn op een quantum computer.

HOE START JE MET JE PERSOONLIJKE QUANTUM JOURNEY?

Er bestaat ondertussen een enorme hoeveelheid aan materiaal om de wereld van quantum computing te ontdekken. Inspiratie vind je in *The Quantum Decade* van het IBM Institute for Business Value. Een relatief laagdrempelig boek is *Quantum Computing for Everyone* door Chris Bernhardt. Michael Nielsen en Isaac Chuang schreven het beroemde maar ook zeer gevorderde *Quantum Computation and Quantum Information*. Als je graag online studie afwisselt met praktijk, surf dan naar het Qiskit Textbook.

Vervolgens zijn er de algorithm developers, die een IT-probleem vertalen in één of meerdere quantum algoritmen. We vinden hen bij gespecialiseerde softwarebedrijven en opkomende opensourcecommunity's, de academische wereld en constructeurs.

Tot slot zijn er de model developers, zeg maar de traditionele programmeurs en ook data scientists, die in hun business-georiënteerde applicatie via API-calls één of meerdere quantum algoritmen aanroepen, door hun traditionele programmeertalen en -tools te gebruiken. Deze laatsten vinden we in alle mogelijke ondernemingen die nut zien in quantum computing en moeten alleen de fundamenten van quantum computing begrijpen en weten wat de functies zijn van een quantum algoritme.

Alle lagen in de quantum stack zijn nog in volle evolutie: hardwarecomponenten, geassembleerde toestellen, algoritmen, applicaties en use cases. Sommige ondernemingen oordelen dat het te vroeg is om nu al te investeren in dit nieuwe paradigma. Andere beseffen dat het niet zo eenvoudig is om op de rijdende 'quantumtrein' te springen, omdat de manier van redeneren totaal verschillend is. *"There are no fast followers in quantum"*, opperde Bob Sutor, IBM Quantum Strategy Leader van IBM Research. Wellicht is een realistische aanpak aangewezen: ten minste één medewerker van de innovatiecel aanduiden die quantum computing opvolgt en de rol van Quantum Ambassador of Champion op zich neemt. In de Developer of Data Science community zou er ten minste één Python-ontwikkelaar zich deels kunnen toeleggen op Qiskit, de opensourcedevelopmentkit voor quantum computing, geënt op Python.

Verschillende bedrijven die innovatie als een kerntaak zien, hebben enkele ambities gemeen: onderzoek rond het gebruik van quantum computers in hun bedrijfsprocessen, sneller competenties opbouwen, een aantal prototypes van applicaties ontwikkelen, behoren tot een ecosysteem van enthousiaste en leergierige partners, en zo de leiders blijven in hun industrie. Ongeveer 150 dergelijke bedrijven hebben zich verenigd in het IBM Quantum Network, waardoor ze toegang hebben tot de meest geavanceerde en recente toestellen en experten van IBM. Waar Daimler, ExxonMobil en JPMorgan Chase vandaag al staan met quantum computing is gewoonweg fenomenaal en een belangrijke troef voor hun marktleiderschap. Voor onze Vlaamse ondernemingen is het ogenblik zonder enige twijfel gekomen om de eerste stappen te zetten van de quantum journey.

WAT GEBEURDE ER IN FRAUNHOFER OP 15 JUNI 2021?

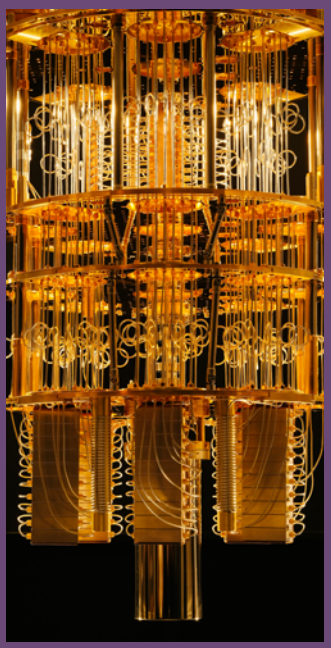
Het Fraunhofer-Gesellschaft, in 1949 gesticht in Duitsland, telt 74 researchinstituten. Het heeft een budget van 2,8 miljard euro en is een leider in toegepast onderzoek. Op 15 juni 2021 vond er de inauguratie plaats van het eerste IBM Quantum System in Europa, dat nu ten dienste staat van al de Fraunhofer-organisaties voor ondersteuning van onderzoek en ontwikkeling. Het toestel bevindt zich in een datacenter nabij Stuttgart.

Over de auteur: Eric Michiels is Executive Architect bij IBM Belgium en ook IBM Quantum Distinguished Ambassador. Als Qiskit Advocate staat hij zowel ontwikkelaars als datawetenschappers te woord.

WIE NEEMT DE LEAD IN QUANTUM COMPUTING?

De ontwikkelingen rond quantum computing worden uitgevoerd door de meest vooraanstaande technologiebedrijven van de wereld. De race is volop aan de gang. In 2017 gaf IBM aan nog binnen enkele jaren quantum computers met 50 qubits te willen aanbieden, bijna een verdubbeling tegenover de Quantum System One, die het Duitse onderzoeksinstituut Fraunhofer-Gesellschaft als eerste buiten IBM in gebruik nam. Zelf nam het zowat een jaar geleden een computer met 65 qubits in gebruik. En in 2023 wil IBM de eerste computer met 1.000 qubits klaar hebben.

IBM is niet het enige bedrijf dat commerciële quantum computers ontwikkelt. Ook Google, Intel en Microsoft zijn daar druk mee bezig. Zo kondigden bedrijven als deze systemen met 49 à 50 qubits aan, tot pakweg 100 qubits of meer. Ook Amazon Web Services (AWS) roert zich en gaat quantum computers voor de cloud ontwikkelen. De Amerikaanse hyperscaler heeft al een volledig beheerde dienst (Amazon Braket) waarmee wetenschappers tests kunnen doen met hardware van andere fabrikanten. AWS ziet zoveel potentieel in deze technologie dat het in dit kader nu ook aan eigen technologie werkt. Daartoe wordt binnen AWS een *Center for Quantum Computing* opgericht.



DECOMMISSIONING: HET ONDERSCHATTE ONDERDEEL VAN DE IT-LEVENSCYCLUS

Wanneer bedrijven aan infrastructuurplanning doen, gaat de meeste aandacht vaak naar het toevoegen van nieuwe apparatuur en nieuwe technologie. Maar hoelang denken ze na over wat ze zullen doen met oude apparatuur die niet langer nodig is?

Soms blijft oude apparatuur gewoon ergens staan, al is dat doorgaans niet de beste manier om ermee om te gaan. Want oude toestellen die niet langer worden ondersteund, krijgen geen nieuwe beveiligingspatches. Terwijl ze wel kwetsbaar kunnen zijn voor nieuwe beveiligingsrisico's.

KOSTENPOST

"Als ze actief blijven, zijn ze kwetsbaar voor aanvallen, zelfs als je ze niet meer voor bedrijfsfuncties gebruikt", aldus James Lagattuta van Prescient Solutions, dat zich in decommissioning specialiseert. Dat is sneller dan vaak wordt gedacht. Weet dat Microsoft sinds anderhalf jaar niet meer in security-updates of ondersteuning voorziet voor dit besturingssysteem. Terwijl bij bedrijven vaak (ergens) ook toestellen op basis van oudere besturingssystemen staan.

Bovendien zijn inactieve apparaten, zo oppert James Lagattuta, ook

een kostenpost. Denk maar aan de stroom of de opslagruimte. En als je de licenties van je oude machines niet overzet op de nieuwe, heb je mogelijk onnodige softwarekosten.

Dan is er nog een ander risico. Een machine die nog is aangesloten en aanstaat, kan nog worden gebruikt. “Als je die niet afsluit en ontkoppelt, kun je onbewust kritieke processen of gegevens op servers hebben staan, die niet langer worden bewaakt of geback-upt.”

WEG ERMEE?

Helaas blijkt het in de praktijk niet zo eenvoudig om te beslissen of het zinvol is om oude apparatuur weg te doen. De oude hardware mag dan niet waardevol zijn, de gegevens die erop staan, zijn dat vaak wel. “De beste manier om een oude schijf te beschermen, is om toepassingen te verwijderen en daarna software te gebruiken die de gegevens herhaaldelijk overschrijft. De schijf moet dan fysiek worden vernietigd, zodat niemand bij de gegevens kan komen”, aldus James Lagattuta van Prescient Solutions.

Zorg er wel voor dat je, voordat je de schijf wist, een goede back-up maakt en veiligstelt van de uiteindelijke inhoud, benadrukt hij. “Misschien heb je die nodig om aan de voorschriften te voldoen, of moet je de data herstellen ter ondersteuning van een toekomstig project.”

STAPPEN

Bij het buiten gebruik stellen van hardware zijn standaard en goed gedocumenteerde praktijken van cruciaal belang. De stappen die hiervoor worden beschreven, vormen een leidraad qua aanpak.

De ontmanteling van hardware (door veroudering, defecten of om een andere reden) valt onder de bevoegdheid van de IT-afdeling, die samenwerkt met alle betrokken eigenaars/stakeholders (bijvoorbeeld financiën als het om een boekhoudsysteem gaat of HR als het om salarisgegevens gaat).

Besluit je afstand te doen van technologie, dan kan de IT-afdeling overgaan tot schenking (bijvoorbeeld via initiatieven als *Close the gap* of Digital for Youth) of het apparaat laten recyclen of vernietigen (bijvoorbeeld via bedrijven als *Out of Use*). De keuze die hier wordt gemaakt, hangt af van het apparaat, het betrokken personeel en het beveiligingsbeleid en de beveiligingsprocedures, dus dit verschilt zowel per geval als per bedrijf. “Indien van toepassing, moet de beveiligingsafdeling worden geraadpleegd om ervoor te zorgen dat de juiste stappen worden genomen om de organisatie, de gegevens en de activa te beschermen.”

Of hoe in IT niet alleen *cutting edge* technologie, maar ook oude technologie zo zijn aandacht verdient. Kwestie van je vingers er niet aan te snijden.

» *Bekijk ook het eerdere SAI webinar over sustainability en Green IT.* ***Je vindt het hier.***

CHECKLIST: WEG ERMEE OF NIET?

Soms is de beslissing over het al dan niet buiten gebruik stellen van hardware eenvoudig, maar in andere gevallen ligt het antwoord moeilijker. Bij twijfel moet de beslissing gebaseerd zijn op onder meer de volgende vragen:

- ☑ Is het apparaat verouderd, overbodig en niet langer de beste keuze voor gebruik?
- ☑ Presteert het toestel of de toepassing slecht en/of veroorzaakt het storingen of onderbrekingen van de dienstverlening?
- ☑ Wordt de technologie niet langer ondersteund?
- ☑ Kan het toestel worden gerepareerd/geüpgraded?
- ☑ Welke diensten zullen worden beïnvloed door dit apparaat te verwijderen? Kunnen zij elders worden ingezet of zijn zij elders vervangen?
- ☑ Kan het apparaat elders worden gebruikt (bijvoorbeeld een testlab of oefenopstelling)?

ZERO TRUST SECURITY: HYPE OF DE WEG VOORWAARTS?

Het is jaren geleden dat een thema nog zo voor beroering zorgde in de wereld van security. Maar is zero trust echt van tel voor security, organisaties en IT-afdelingen? SAI Update deed een brede rondvraag: in de markt en bij securityverantwoordelijken. "Persoonlijk vraag ik me af of het voor sommige organisaties überhaupt mogelijk is om zero trust toe te passen."

WAT HOUDT ZERO TRUST ECHT IN?

Afhankelijk van de leverancier wordt zero trust weleens anders benaderd. Daarom gaan we even terug naar de basics. Zero trust is een principe ontwikkeld door John Kindervag in 2010. De basisgedachte luidt: *never trust, always verify.* Bij een zero-trustprincipe worden het netwerk en de *endpoints* als potentieel vijandig beschouwd. Alle toegang moet worden gecontroleerd en geautoriseerd, stelt Tom De Laet, incident response analyst bij Check Point. Hij was ervoor incident response & digital forensics analyst bij de Belgische Defensie.

De Laet haalt nog enkele basisprincipes aan. “Zo moet bij zero trust het netwerk altijd als vijandig worden beschouwd, zijn interne en externe dreigingen altijd aanwezig en is het interne netwerk is niet genoeg als trust-factor. Daarnaast moeten elke gebruiker, elk toestel en elke netwerkflow gecontroleerd en geverifieerd worden en moeten de policy’s dynamisch zijn.”

IS ZERO TRUST ECHT WEL ZO’N REVOLUTIE?

Bij een rondvraag van het vakblad Computable bleek onlangs dat lezers zero trust als de op een na belangrijkste securitytrend zagen, kort na multi-factorauthenticatie. Wel gek voor een concept dat eigenlijk al ruim tien jaar bestaat.

Maar volgens Simen Van der Perre, solution specialist bij Orange Cyberdefense, moet net onze inschatting rond trust worden herzien. “Een aantal technologische ontwikkelingen hebben gezorgd voor een toevoeging van cloud- en Internet of Things-toepassingen aan de IT-omgeving. Die gingen zich ook buiten het datacenter bevinden”, stelt Van der Perre. Volgens hem is, mede door deze verschuivingen, trust jammer genoeg een fundamenteel probleem geworden in security. “Een aantal recente cyberaanvallen waarbij trust gecompromitteerd werd, heeft dat pijnlijk duidelijk gemaakt. We moeten onze manier van denken over trust bij het bouwen van een IT-architectuur herzien. Alleen al hierom zorgt zero trust dus effectief voor een revolutie in security.”

EN KOMT DAT ALLEMAAL DOOR CORONA?

Volgens Van der Perre heeft de coronapandemie ervoor gezorgd dat gebruikers vooral van thuis werken, waardoor zij vooral vanuit een ‘untrustzone’ toegang tot IT-systemen en hun data nodig hebben. “De technologische ontwikkelingen en coronapandemie zorgden dus voor een aantal grote gamechangers voor de securitystrategie van organisaties, zoals een cloud-firststrategie, home office en een explosie van IoT-toestellen”, stelt hij. Al speelt er volgens hem ook meer: “Organisaties gaan zich bovendien meer focussen op hun corebusiness, waardoor ze met meer derde partijen samenwerken en toegang moeten verlenen.”

Voor Tom Olislagers, head of enterprise pre-sales bij Dell Technologies, zijn er drie zaken die naar zero trust leiden: de COVID-19-pandemie, edgelocaties en het feit dat cybercriminaliteit een succesvol businessmodel geworden is. Enerzijds wordt de gedistribueerde toegang tot en het genereren van data nog versterkt door de opkomst van edge. “Denk hierbij aan fabrieken, telefoonmasten maar ook bijvoorbeeld zelfrijdende auto’s. Gartner stelt dat tegen 2025 driekwart van de bedrijfsdata gecreëerd en verwerkt zal worden buiten het datacenter of de cloud. Deze evolutie geeft cybercriminelen een scala aan nieuwe mogelijkheden, want de te beschermen perimeter is een heel stuk groter dan voordien.”

Cybercriminelen werken op verschillende manieren. “Naast ransomware attacks zetten cybercriminelen meer en meer phishingaanvallen, valse applicaties, trojans, backdoors, cryptominers en botnets in”, stelt hij. “We zien dan ook dat cybercriminaliteit meer en meer een business-

Simen Van der Perre (Orange Cyberdefense): “We moeten ons denken over trust herzien.”

Tom Olislagers (Dell Technologies): "Streven naar stapsgewijs toepassen van zero-trustprincipes."

model wordt, waarbij doelbewust data wordt gestolen of onbruikbaar gemaakt als een gemakkelijke manier van geld verdienen, denk aan cryptolockers. Ook deze ontwikkelingen zorgen dat er nood is aan een nieuwe aanpak rond security."

HOE MOEILIJK IS HET OM MET ZERO TRUST TE STARTEN ALS ORGANISATIE OF IT-AFDELING?

"Dat hangt ervan af hoe je het wilt aanvliegen", stelt Rudolf de Schipper, delivery director EU bij Unisys. "Met een oplossing die zero trust als uitgangspunt heeft, kun je al vrij snel starten. Maar als je te maken hebt met een heel heterogeen IT-landschap of speciale situaties, of geen grote veranderingen wenst door te voeren, dan kan het wel een aardig traject worden." Als grote hinderpaal ziet Rudolf de Schipper altijd het interne change-management. "En dat kan heel diep zitten. Zo zweert bijvoorbeeld de IT-afdeling bij de firewalls. Of willen ze geen endpointoplossingen uitrollen tot de gebruikers die graag overal toegang willen houden."

Veel hangt ook af van de IT- en beveiligingsmaturiteit van de organisatie. "Vaak hebben organisaties al componenten die ingezet kunnen worden voor zero trust", oordeelt Tom Olislagers van Dell Technologies. "Organisaties moeten streven naar het stapsgewijs toepassen van zero-trustprincipes, procesveranderingen en technologische oplossingen die hun data-assets en bedrijfsfuncties per *use case* beschermen. Een *use case* waarmee vaak gestart wordt, is de digitale werkplek uitbouwen", oppert hij. "Het in kaart brengen van zo veel mogelijk contextuele informatie – bijvoorbeeld over hoe endpoints geconfigureerd zijn en in welke mate processen verlopen – geeft security operations center (SOC)-administratoren veel meer inzicht en de mogelijkheid om een *prioritering* te doen van securityincidenten."

Volgens Chris McCormack, senior product marketing manager bij Sophos, is het helemaal niet zo moeilijk om ermee te starten. "De eerste stap die veel organisaties nemen, is overstappen van een ouderwetse VPN voor toegang op afstand naar een ZTNA-oplossing (*zero trust network access*, n.v.d.r.) om hun gebruikers in staat te stellen naadloos verbinding te maken met de netwerktoepassingen en -bronnen die ze nodig hebben, zonder het impliciete vertrouwen dat met VPN gepaard gaat. ZTNA-oplossingen zijn zeer eenvoudig toe te passen en veel gemakkelijker te beheren dan traditionele VPN."

ZET ZERO TRUST DE KLASSIEKE BEVEILIGINGSTECHNOLOGIE ZOALS ENDPOINT, FIREWALL EN (VOORAL) VPN ONDER DRUK?

Zero trust is absoluut een goede vervanging voor VPN in functie van toegang op afstand, vindt Chris McCormack van Sophos. "Hoewel VPN in de toekomst in sommige situaties nog een rol kan blijven spelen, wordt ZTNA de belangrijkste technologie voor remote gebruikers om toegang te krijgen tot bedrijfsgegevens", stelt hij. "Maar ZTNA is een aanvulling op firewalls en endpoints, die nog altijd een belangrijke rol spelen. Zo zullen firewalls de perimeter bescherming blijven bieden voor on-premise netwerken, die nergens heen gaan. Endpointbescherming zal altijd een kritische IT-securitycomponent zijn die eigenlijk op een gecoördineerde manier moet werken met zero trust om inzicht te bieden in de toestand van apparaten en compliance."

Het is vooral die gecoördineerde manier die een rol speelt, vindt Frederick Verduyckt, senior VCN solution engineer bij VMware. "Uiteraard hebben de verschillende technologieën verschillende doeleinden en individueel zijn ze allemaal zeer sterk. Maar telkens pakken ze meestal maar één specifiek stuk van de puzzel aan", oppert hij. "Al die

puzzelstukken combineren, is belangrijk om tot een zero-trustbeleid te komen. Nog belangrijker is het om inzichten te verkrijgen uit deze combinatie. Deze inzichten openen immers de deur naar automatisering en orchestratie van zero trust." Alleen ligt volgens Verduyckt de tekortkoming van de verschillende klassieke technologieën nu net daar. "Geen interactie met de andere lagen van bescherming en dus vrijwel onmogelijk om te automatiseren als één geheel."

"Veel securityvendoren proberen hun product te vereenzelvigen met zero trust, en dat is jammer."

Klassieke beveiligingstechnologieën krijgen in een zero-trustarchitectuur vooral een andere rol en veelal ook een andere locatie, vult Simen Van der Perre van Orange Cyberdefense aan. "Slimme firewalls worden nog altijd gebruikt, al staan die in een zero-trustarchitectuur veel dichter bij de data. Endpointtechnologie wordt nog altijd gebruikt om de context van het endpoint door te geven aan een zero-trust-architectuur en een rol te spelen in de verificatie", weet hij. "Er zijn zero-trustarchitecturen waar VPN geen rol meer speelt, maar ook zero-trustarchitecturen waar een beveiligd kanaal van het toestel van de gebruiker tot aan de data vanuit een *untrusted* netwerk aan belang wint."

IS ZERO TRUST NIET EERDER EEN FILOSOFIE DAN DAT HET GAAT OM TECHNOLOGIE EN PRODUCTEN?

Van der Perre beaamt dat. "Zero trust is in de eerste plaats een filosofie, eerder dan dat het om technologie en producten gaat. Zero trust is vooral een strategisch initiatief dat ondersteund dient te worden met een aanpak in meerdere fases. Een zero-trustarchitectuur dient uiteraard gebouwd te worden met technologie en producten."

YANNICK HERREBAUT, HAVENBEDRIJF ANTWERPEN

WAT ZEGT DE CISO?

"In mijn ogen is zero trust een strategie die je als bedrijf kunt aannemen en een model waarop je je securityarchitectuur baseert. Bij Port of Antwerp zijn we zeker en vast met zaken bezig die je onder de noemer zero trust kunt plaatsen, al is dat niet de speerpunt van onze strategie", aldus Yannick Herrebaut, Cyber Resilience Manager – CISO DI/CR bij Havenbedrijf Antwerpen.

Met prioriteiten governance/ecosystem, protect, defend en resilience wil zijn organisatie, zo benadrukt Herrebaut, inzetten op mensen, processen en technologieën. "En dit voor zowel preventie als reactie."

Ook Herrebaut erkent de uitdagingen. "Om een volledige IT-omgeving met zero trust te bereiken, heb je echter een zeer hoge mate van maturiteit nodig. Dit is bovendien niet eenvoudig in een zeer diverse *brownfield* omgeving", stelt hij. Bovendien is hij kritisch voor de markt. "Persoonlijk vraag ik me zelfs af of het voor sommige organisaties überhaupt mogelijk is om zero trust toe te passen. Daarnaast proberen veel securityvendoren hun product te vereenzelvigen met zero trust, waardoor het begrip – jammer genoeg – meer een marketingterm is geworden dan wat anders."

Volgens Tom De Laet van Check Point is zero trust als concept ook eerder een strategie? En een strategie is, zo stelt hij, net iets wat je niet van vandaag of morgen verandert of toepast. “Een probleem of uitdaging met de toepassing van een zero-truststrategie is dat dit niet eenvoudig is. *All network access* als *untrusted* beschouwen en een controlesysteem toepassen, is moeilijk in de hedendaagse digitale omgevingen. Het is dan ook zeer onwaarschijnlijk dat ondernemingen een volledig zero-trustprincipe kunnen toepassen.”

Een van de redenen is dat veel oplossingen vandaag nog altijd zeer gericht zijn op perimetersecurity. “*Zero trust as baseline in designing a practical implementable zero trust strategy* zou voor mij een meer toepasselijke leuze zijn voor de evolutie die we zullen zien bij ondernemingen die dit concept willen toepassen. We moeten een balans zoeken en kijken in hoeverre we de netwerken en systemen als untrusted gaan beschouwen”, aldus De Laet.

“Het is zeer onwaarschijnlijk dat ondernemingen een volledig zero-trustprincipe kunnen toepassen.”

Daarom spreekt men, volgens hem, ook al niet meer van een ‘binair’ trustsysteem, maar eerder van een ‘variable trust’: *access controlled by variable trust*. “Zo zullen bijvoorbeeld punten worden bedeeld voor verschillende parameters. Een gekend toestel is dan 10 punten waard, waarbij een gekende locatie of gebruikersauthenticatie met gebruikersnaam en wachtwoord ook 10 punten waard is. Maar aanvullende authenticatie, zoals multifactor, is dan 20 punten. Dit variable trust-systeem kan je dan gebruiken om bijvoorbeeld toegang te geven tot bepaalde resources. Zo vereist PCE- of PII-data 40 punten.”

WAT ZIJN DE TECHNISCHE HINDERPALEN?

Tom De Laet haalt er enkele aan. “Enerzijds zijn de meeste oplossingen nog niet volledig ontwikkeld, met name om zo’n ‘variable trust’-systeem ook echt mogelijk te maken.” Daarnaast ziet hij er nog enkele specifieke vraagstukken. Een daarvan is *credential rotation*. “Volgens het zero-trustprincipe moeten *credentials* regelmatig wor-

den veranderd. Want je moet ervan uitgaan dat *credentials* gecompromitteerd kunnen zijn. Een probleem bij het steeds moeten veranderen van *credentials*, is dat werknemers geagiteerd geraken, en dus ook snel gemakkelijke paswoorden gaan gebruiken, omdat ze die elke keer moeten onthouden."

"Technologische ontwikkelingen en de coronapandemie zorgden voor een aantal grote gamechangers voor de securitystrategie van organisaties."

Nog een technische uitdaging of vraagstuk ziet hij bij *securing traffic*. "Zero trust gebiedt bijvoorbeeld dat alle *traffic flows end-to-end encrypted* moeten zijn. Encryptie zoals TLS (*Transport Layer Security*, n.v.d.r.) is vaak a *one-way trust*: als een client een verbinding maakt met een website via HTTPS wordt er vanop de client gecontroleerd of de server wel is wie hij beweert te zijn. Maar TLS kan ook gebruikt worden om de client te valideren. Voor externe *unknown clients* houdt dit geen steek, maar voor een interne client is dit zeer bruikbaar en kan dit waardevol zijn", klinkt het. Een andere kwestie ziet De Laet in het gebruik van netwerk-based firewalls versus endpoint-based firewalls. "Die laatste maken het mogelijk om een zeer granulaire controle te hebben over endpointlevel netwerkrestricties."

Dit zijn dan nog maar enkele technische aandachtspunten, want in de praktijk komt er veel bij kijken. Bovendien is een belangrijk aandachtspunt – zoals eerder al aangehaald – het changemanagement.

ZIJN BELGISCHE ORGANISATIES OOK ECHT BEZIG MET ZERO TRUST?

En dan de realitycheck. Enerzijds gaan er steeds meer middelen naar security. Een doorsnee Belgische organisatie besteedt vandaag meer dan een vijfde (21 procent) van zijn IT-budget aan cyberbeveiliging. Dat blijkt uit het *Hiscox Cyber Readiness Report 2021*, een referentie als het gaat om onderzoek naar security-middelen en -inspanningen. Vorig jaar ging in ons land 13 procent van het IT-budget naar cybersecurity.

Maar de vraag is of zero trust ook echt op de radar staat. De meeste gesprekspartners zien voorzichtige interesse of eerste stappen. "Traditioneel zijn wij, Belgen, zeer conservatief als het over nieuwe technologie of beveiligingsmodellen gaat. We gaan vaak eerst kijken wat onze buren doen en daarna beslissen we om het zelf toe te passen", oppert Frederick Verduyckt van VMware.

Al ziet hij toch een verschuiving in deze benadering. "De pandemie heeft hier wat verandering in gebracht, waardoor veel organisaties al minstens interesse tonen om zero trust te hanteren over de hele organisatie heen. De beveiligingsbewuste organisaties waren hier vóór de pandemie al lang mee aan de slag."

FORRESTER: KWART BEDRIJVEN ZIET ZERO TRUST ALS PRIORITEIT. WAT ZEGT DE ANALIST?

Ongeveer een kwart van de Europese besluitvormers op het gebied van beveiliging in verschillende industriesectoren zegt dat de toepassing van een zero-truststrategie het komende jaar een topprioriteit is voor hun bedrijf. Dit blijkt uit onderzoek van Forrester. Organisaties die het zero-trustmodel voor IT-security willen invoeren, dienen te beginnen met identiteit- en apparaatbeheer als dat nog niet volwassen is. Zo schrijft analist Paul McKay in het rapport *Zero Trust Adoption In Europe*.

Europese CISO's moeten zero trust behandelen als een algemeen programma, in plaats van een reeks afzonderlijke technische initiatieven. Forrester ziet als een van de grootste en meest voorkomende belemmeringen het uiteenlopende begrip van wat zero trust betekent binnen een organisatie en wat de algemene bedrijfsarchitectuurstrategie voor zero trust is. "Dit leidt vaak tot concurrerende initiatieven van verschillende delen van IT, verspilt investeringen en beperkt de vooruitgang", aldus McKay.

VOLGENDE EVENTS VOOR SAI

Charlie and the chocolate factory - Tales of a career in technology
Avondconferentie (Brussel)
05/10/2021
Meer info: https://www.sai.be/event/details/57/charlie-and-the-chocolate-factory-tales-of-a-career-in-technology/

A Xperian Strategy Game
Avondconferentie (Gent)
12/10/2021
Meer info: https://www.sai.be/event/details/58/xperian-strategy-game/

Putting Enterprise Architecture to Work to Transform Cybersecurity Into a Business Executive's Opportunity
Avondconferentie (Antwerpen)
13/10/2021
Meer info: https://www.sai.be/event/details/59/putting-enterprise-architecture-to-work-to-transform-cybersecurity-into-a-business-executives-opportunity/

Boekvoorstelling: De Cyber Arena
Avondconferentie (Brussel)
26/10/2021
Meer info: https://www.sai.be/event/details/68/boekvoorstelling-de-cyber-arena/

Securitycertificatie: wat, waarom en hoe?
Workshop (Antwerpen)
09/11/2021
Meer info: https://www.sai.be/event/details/60/security-certificatie-wat-waarom-en-hoe/

Knowledge Graphs
Avondconferentie (Brussel)
16/11/2021
Meer info: https://www.sai.be/event/details/61/knowledge-graphs/

A new way of approaching architecture
Webinar (online)
17/11/2021
Meer info: https://www.sai.be/event/details/186/a-new-way-of-approaching-architecture/

Hands-on met process mining
Workshop (Gent)
18/11/2021
Meer info: https://www.sai.be/event/details/62/hands-on-met-process-mining/

The Digital Accelerator
Avondconferentie (Antwerpen)
23/11/2021
Meer info: https://www.sai.be/event/details/63/the-digital-accelerator/

Machine Learning Essentials
Workshop (Brussel)
25/11/2021
Meer info: https://www.sai.be/event/details/64/machine-learning-essentials/

Security @ Microsoft
Avondconferentie (Antwerpen)
30/11/2021
Meer info: https://www.sai.be/event/details/65/security-microsoft/

Aan de slag met DMN en decision modeling
Workshop (Brussel)
02/12/2021
Meer info: https://www.sai.be/event/details/66/aan-de-slag-met-dmn-en-decision-modeling/

API-management: aanpak, tools en beveiliging
Workshop (Brussel)
07/12/2021
Meer info: https://www.sai.be/event/details/67/api-management-aanpak-tools-en-beveiliging/

Teaser: SAI afsluiter
Speciaal event (Brussel)
15/12/2021
Meer info: https://www.sai.be/event/details/54/teaser-sai-afsluiter/

JUISTE ANTWOORDEN QUIZ (vorig nummer)
Antwoord 1: Catalana | Antwoord 2: Tibco
Er waren deze keer geen juiste inzendingen.

» *Meer info op **SAI.be***

COLOFON
Werkten mee aan dit nummer: William Visterin (coördinator), Robin Van den Bogaert, Stef Gyssels, Eric Michiels en Marc Vael.