11

SAI UPDATE

DIGITAAL TIJDSCHRIFT VOOR SAI-LEDEN | SEPTEMBER 2022 | SAI

GOED VOOR UW SECURITY, MAAR GEEN WONDERMIDDEL

MULTIFACTORAUTHENTICATIE: HET GLAS IS HALFVOL

pag. 9

En verder:

EEN ARCHITECT VOOR ELK DOMEIN BIJ BOL.COM

pag. 17

TIEN TIPS OM JE SOFTWARE-PROJECT TE DOEN KELDEREN

pag. 26

EIGHT IS GREAT: LAAG 8 IN HET OSI-MODEL

pag. 30

EDITO

FOCUS VERFIJNEN

De vakantie is weer bijna vergeten en ook SAI herneemt z'n nuttige en leerrijke activiteiten met brandend actuele thema's.

Om je nog beter te kunnen bedienen en je concrete verwachtingen voor de komende maanden te ontdekken, hebben we tussen juni en juli 2022 een grote peiling uitgevoerd. Mijn grote dank voor de massale reactie, want bijna 32 procent van alle leden heeft meegedaan.

Een eerste vaststelling is dat de opdeling in zes kerndomeinen in de smaak valt, met als populairste domeinen: emerging technologie, data & AI en architectuur. We houden hier zeker rekening mee in de selectie van de sprekers en thema's. Regelmatig zullen we online technologie-events promoten die beantwoorden aan jullie verwachtingen en aan de hoge kwaliteitsstandaarden van SAI, waarbij je als SAI-lid meestal gratis kunt deelnemen dankzij een SAI-code.

Een tweede duidelijke vaststelling is dat jullie massaal kiezen voor online webinars, events en workshops. Waar je ook bent, de SAI-events zijn gemakkelijk online te volgen. Tot vlak voor de start van een SAI-event kun je inschakelen en na afloop keer je meteen terug naar je andere professionele of persoonlijke activiteiten.

Als je niet kon deelnemen aan de online SAI-events, dan lag dat ofwel aan het thema dat je minder belangrijk vond ofwel aan het tijdstip. De opnames van een SAI-event worden achteraf vaak bekeken via onze website. We zijn zeer tevreden dat we een catalogus van opnames kunnen aanbieden, die je kunt bekijken wanneer je wilt. Uiteraard kun je alleen tijdens een live-event reageren of vragen stellen aan de spreker(s).

Als je toch fysiek aanwezig wilt zijn, dan blijven de SAI-avondconferenties de voorkeur wegdragen in de drie bekende steden van SAI: Diegem/Brussel, Antwerpen en Gent. Ook dit blijven we trouw.

Voorts is er vraag naar kortere SAI-workshops, minder dan de gebruikelijke zeven uur en met meer duidelijkheid rond de kennis die wordt aangeleerd tijdens de workshop. Voor de komende SAI-workshops – zowel online als fysiek – houden we hiermee rekening.

Het magazine SAI Update valt bijzonder in de smaak en wordt door vier op de vijf SAI-leden gelezen. Onze leden zijn zeer tot uiterst tevreden over de kwaliteit van de artikels in het magazine. Aangezien er veel werk kruipt in de creatie van SAI Update, ben ik samen met de andere bestuurders supertevreden met deze appreciatie.

De vorig jaar opgestarte podcast SAI.NT (afkorting voor SAI New Technology, www.sai.be/account/profiel/podcast) is voorlopig nog niet zo bekend bij de SAI-leden, maar de luisteraars vinden de kwaliteit zeer goed. Ook dit initiatief zetten we voort, met meer gasten.

Bij deze dank ik alle deelnemers aan onze peiling om onze focus nog te verfijnen voor de komende periode.

Ten slotte wil ik hier Prof. Dr. Jacques Vandenbulcke van harte danken namens alle leden en bestuurders voor wat hij de afgelopen decennia heeft gerealiseerd voor SAI. Hij heeft gevraagd om vervangen te worden als SAI-penningmeester. Sinds augustus 2022 heeft Prof. Wim De Keyser die rol overgenomen. Uiteraard blijft Jacques erelid en we hopen nog vele jaren een beroep te kunnen doen op zijn kennis en expertise.

Ik wens je veel leesplezier en nog veel gezonde, succesvolle en leerrijke maanden.

Marc Vael
Voorzitter raad van bestuur SAI

INHOUD

“

ALS JE EEN SOFTWAREPROJECT ECHT WILT DOEN MISLUKKEN, ZEG DAN DAT HET NIEUWE SYSTEEM PRECIES HETZELFDE MOET DOEN ALS HET OUDE.

CHRISTIANE VANDEPITTE
BUSINESSANALIST EN SOFTWAREDESIGNER
OP PAGINA 27

GEBREK AAN IT-KENNIS BIJ RECRUITERS FRUSTREERT IT'ERS MATELOOS

Recruiters en IT'ers: het blijft een lastige match. Uit nieuw onderzoek blijken IT'ers zich zelden begrepen te voelen door de mensen die hen willen aanwerven. Slechts een minderheid van de IT'ers vertrouwt recruiters in de zoektocht naar nieuw werk.

IT'ers zijn loslopend wild op de arbeidsmarkt. Het tekort is groot. Voor bedrijven die hard op zoek zijn naar techtalent is investeren in rekrutering dus onvermijdelijk. Vaak komen dan ook recuiters op de proppen. Iedereen die ook maar iets van IT in zijn LinkedIn-profiel heeft staan, wordt platgebeld door recruiters op zoek naar een snelle match. Maar wat als die recruiter bijvoorbeeld het verschil tussen Java en JavaScript niet eens kent? Of Python verwisselt met PHP?

Veel IT'ers blijken niet tevreden over die recruiters en hun aanbiedingen. Dat blijkt uit de 23ste editie van het jaarlijkse salarisonderzoek van AG Connect en Berenschot onder zo'n 400 IT'ers. Ruim 52 procent van de IT'ers is simpelweg van oordeel dat recruiters onvoldoende kennis hebben om hen een relevant aanbod te doen, aldus het onderzoek. Niet gek dus dat slechts 13 procent op recruiters vertrouwt in de zoektocht naar nieuw werk. Het eigen netwerk (37 procent) en online vacatures (33 procent) worden veel vaker aangehaald als middel om een andere baan te zoeken.

52 PROCENT

van de IT'ers
dicht recruiters
onvoldoende IT-kennis toe

Nieuw is de ergernis overigens niet. Klassiek zijn de zwarte lijsten van recruiters die op internet te vinden zijn. En er is *shit-recruiters-do*, een site waarop IT'ers delen op wat voor manieren zij allemaal benaderd worden. "Betreurenswaardige berichten die jonge developers zoal in hun LinkedIn-inbox vinden", staat er bovenaan deze website. Zoals ene Jari die benaderd werd door een recruiter met een aanbod om "*als frontend developer in te staan voor het ontwerp van backend interfaces.*"

DEZE TIEN PROGRAMMEERTALEN HEBBEN HUN BESTE TIJD GEHAD

Programmeertalen zijn als automerken: sommige blijven populair, andere waren het ooit of waren veelbelovend, maar deemsteren nu weg.

Het vakblad Computable zette tien programmeertalen die op hun retour zijn op een rijtje. Het blad focuste hierbij op programmeertalen die qua gebruik of verwachtingen best wel hoge ogen gooiden.

1/ VB.NET

Visual Basic.NET of kortweg VB.NET is een taal ontwikkeld door Microsoft. Het heeft een syntaxis die lijkt op Basic en een coderingsstijl die lijkt op die van C#. De taal werd voorgesteld in 2002. Nu ontwikkelaars actief zijn overgegaan op .NET en C#, zou deze taal weleens heel snel op de schroothoop kunnen terechtkomen.

2/ PASCAL

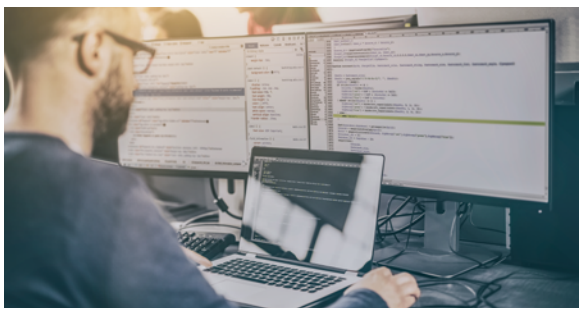
Pascal werd onderwezen aan universiteiten of hogescholen. Bekend is ook Turbo Pascal, een toepassing van de programmeertaal Pascal van het softwarebedrijf Borland. Toen later Delphi op het toneel verscheen, werd de taal Pascal naar de hoek gedrongen.

3/ ELM

Elm kwam tien jaar geleden uit en kreeg meteen de nodige aandacht als domein-specifieke taal om web-browser-gebaseerde grafische gebruikersinterfaces te creëren. Intussen lijkt Elm de strijd met andere talen, zoals Typescript, te hebben verloren.

4/ COLD FUSION

Midden jaren negentig ontworpen door de gebroeders Allaire, meteen ook de naam van hun bedrijf. Maar mede door de slechte kwaliteit van debugging en het gebrek aan een package manager, verloor het geleidelijk zijn populariteit. De overname van Allaire door Adobe deed Cold Fusion geen goed.



5/ ERLANG

Verwierf grote populariteit onder ontwikkelaars vanwege zijn vermogen om enorme aantallen gelijktijdige verzoeken te verwerken en parallelle verwerking te ondersteunen. Maar ondanks zijn lange geschiedenis heeft Erlang nooit een grote aanhang van gebruikers gekregen.

6/ HASKELL

Haskell kwam uit in de jaren negentig, als een culminatie van niet zo populaire talen, bijvoorbeeld Miranda en Clean. Facebook en Github namen er hun toevlucht toe. Maar de laatste jaren lijkt het op de terugweg.

7/ COFFEE SCRIPT

Ontwikkeling in Coffee Script loopt netjes en efficiënt als het om destructuring gaat. Maar het mist, volgens Analytics Insight, een aantal belangrijke functies, bijvoorbeeld rond explicit scoping en real functions. In vergelijking met andere scriptingtalen doen Javascript en Typescript het mede daarom beter.

8/ COBOL 60

In de jaren zeventig was Cobol nog zowat de meest gebruikte programmeertaal in de wereld, maar nu is de taal toch definitief op de terugweg. Zeker de eerste editie Cobol 60 telt niet meer mee. Vanwege de sterke typeregels en de moeilijkheden bij het zogenaamde parsing, kiezen bedrijven vandaag voor andere talen. Het moest wijken voor de meer comfortabele static typing van Java of dynamic typing van Python.

9/ PERL

Perl is een programmeertaal ontworpen door Larry Wall die eigenschappen van de scripttalen C en UNIX verenigt. Van Perl is als minpunt bekend dat het de capaciteit van de CPU opslokt. Andere moderne talen zoals PHP, Ruby, Java of Python kwamen in de plaats.

10/ OBJECTIVE-C

Ooit een populaire taal voor het ontwikkelen van Apple-applicaties, al wordt deze vervangen door Swift. Meer ontwikkelaars verkiezen Swift namelijk boven Objective-C, omdat Swift meer functies en features bevat. Toch is Objective-C van alle talen uit deze lijst nog het meest aanwezig, dankzij de legacycode.

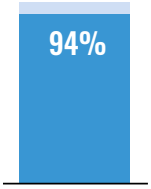
BIJNA ELK BEDRIJF BESTEEDT TE VEEL IN DE CLOUD

94 procent van de bedrijven geeft te veel uit in de cloud, blijkt uit een onderzoek van HashiCorp-Forrester. Die overconsumptie komt voort uit een combinatie van factoren, zoals onderbenutte en overbezette resources, en een gebrek aan vaardigheden.

In het onderzoek waaraan meer dan duizend IT-besluitvormers in Noord-Amerika, Europa, het Midden-Oosten en Azië-Pacific deelnamen, zei 94 procent van de respondenten dat hun organisaties aanzienlijke, vermijdbare clouduitgaven hadden door een combinatie van factoren, waaronder onderbenutte en overbezette resources, en een gebrek aan vaardigheden om cloud-infrastructuur te gebruiken.

Onderbenutte resources behoorden tot de belangrijkste redenen voor te hoge uitgaven, zo bleek uit het rapport. Meer dan 66 procent van de respondenten noemden dit als reden. Respectievelijk 59 procent en 47 procent van de respondenten beweerden dat overprovisioned resources en een gebrek aan benodigde vaardigheden de verspilling veroorzaakten.

Daarnaast geeft 86 procent van de respondenten aan afhankelijk te zijn van cloud operations- en strategieteams, die cruciale taken uitvoeren, zoals het standaardiseren van clouddiensten, het creëren en delen van best practices en beleidslijnen, en het centraliseren van cloud-beveiliging en compliance.



94 PROCENT
doet aan cloud overspending

Ook opvallend: **bijna 60 procent van de respondenten** (voornamelijk grote organisaties) **zegt al een multicloud-infrastructuur te gebruiken**. Nog eens 21 procent zegt binnen de komende twaalf maanden over te stappen op een dergelijke architectuur. Tekort aan vaardigheden was de belangrijkste belemmering voor de overstap naar multicloud: 41 procent van de respondenten noemde dit als de belangrijkste reden. Andere barrières die door respondenten werden genoemd, waren onder meer teams die in silo's werken, compliance, risicobeheer en het gebrek aan training.

IT-CARTOON LECTRR

RECORDBEDRAG VAN 1 MILJARD VOOR DUITS GROEIBEDRIJF IN PROCESS MINING

Het grootste Duitse groeibedrijf van de laatste tien jaar is Celonis. Het bedrijf haalt een miljard dollar binnen om klanten met procesverbeteringen te helpen.

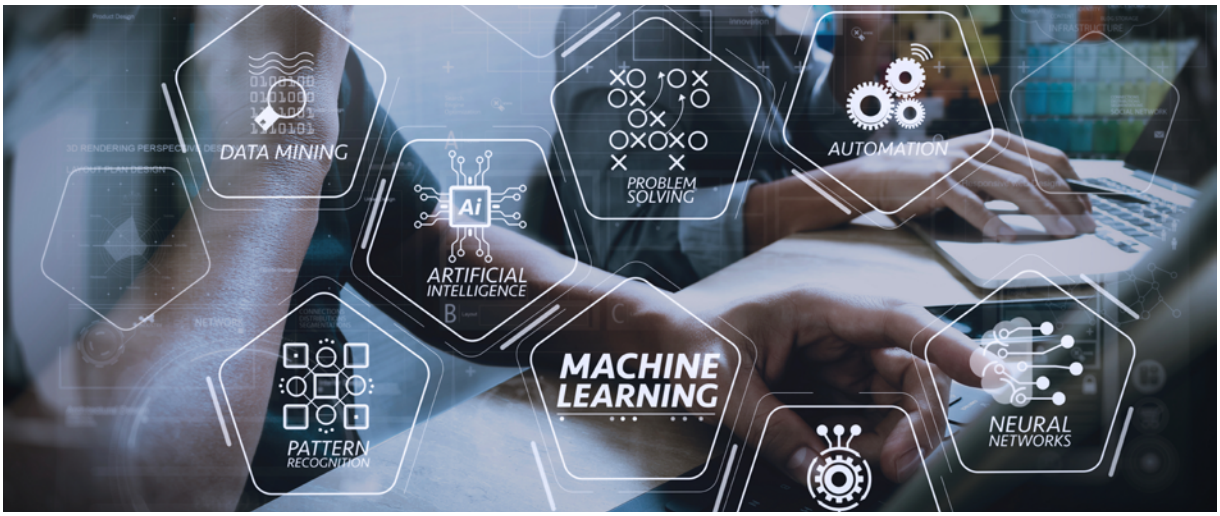
Het gaat om een nieuwe kapitaalronde van Celonis, dat zichzelf omschrijft als de marktleider in process mining software, waarmee het de operationele efficiëntie van bedrijven kan verbeteren. “We hebben nog nooit zo’n urgentie van klanten ervaren om onze oplossingen te gebruiken om procesproblemen op te sporen en op te lossen die tientallen tot honderden miljoenen aan geld- en tijdbesparingen kunnen opleveren”, aldus Alex Rinke, co-CEO en medeoprichter van Celonis in een persbericht naar aanleiding van de kapitaalinjectie.

Met zijn financiering is het bedrijf de meest waardevolle Duitse start-up in de voorbije tien jaar. Celonis is intussen 13 miljard waard en in die hoedanigheid een *decacorn*, de term voor een bedrijf dat 10 miljard waard is. Het bedrijf laat zelfs de bekende neobank N26 achter zich.

Celonis is het toonbeeld van de groeiende en consoliderende sector van process mining vendors, stelt Jochen De Weerdt, als professor beleidsinformatica aan de KU Leuven gespecialiseerd in process mining, als reactie op de hoge financieringswaarde het bedrijf.

“Technologie voor process mining laat bedrijven toe om op een datagedreven manier bedrijfsprocessen te analyseren en te verbeteren. **Een groeiend aantal bedrijven ziet mogelijkheden om klassieke procesverbeteringstrajecten te vervangen door een meer datagedreven aanpak via process mining software.** Bovendien biedt process mining technologie de mogelijkheid om processen nagenoeg in real-time op te volgen en veel sneller te interveniëren.”

Het gebeurt niet zo vaak dat een relatief nieuw bedrijf in zakelijke technologie al meteen zulke hoge ogen gooit en een deel van zijn markt inpalmt. “Celonis neemt als marktleider ook actief deel aan de consolidatiestrategie die sinds een tweetal jaar gevolgd wordt in de sector, bijvoorbeeld door de acquisitie van PAF, een process mining start-up die sterk focust op integratie met de Microsoft-suite”, weet Jochen De Weerdt. “Het groeibedrijf toont aan dat het wereldwijd nieuwe klanten kan aantrekken die actief zijn in een grote diversiteit aan sectoren, gaande van de voedings- en maakindustrie tot financiële dienstverlening en e-commerce.”



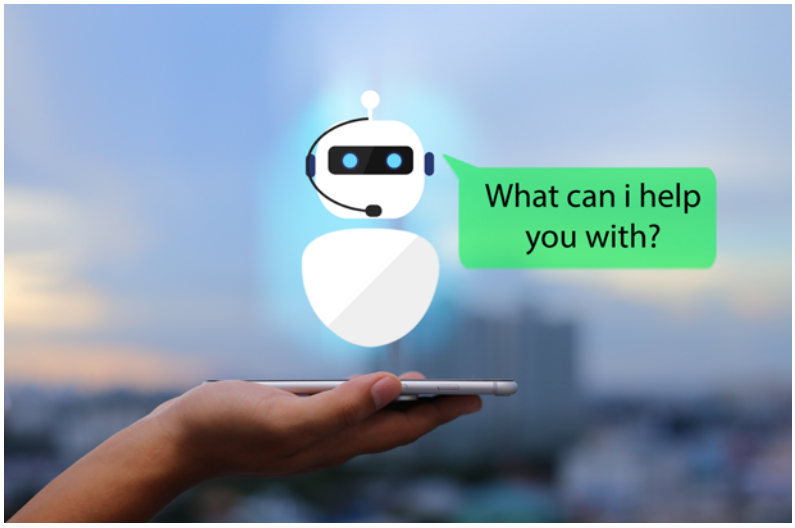
“ARBEIDSKOSTEN CONTACT-CENTERMEDEWERKERS DALEN MET 80 MILJARD DOLLAR DANKZIJ CONVERSATIONAL AI”

Tegen 2026 zullen toepassingen van conversational artificial intelligence (AI) in contactcenters de arbeidskosten van medewerkers met 80 miljard dollar verminderen. Dat voorspelt onderzoeksbureau Gartner. Het bureau ziet de bestedingen aan conversational AI in 2022 zowat 2 miljard dollar uitmaken.

“We schatten dat er vandaag wereldwijd ongeveer 17 miljoen contactcenteragenten zijn”, zegt Daniel O'Connell, VP-analist bij Gartner. “Veel organisaties worden uitgedaagd door een tekort aan agentpersoneel en de noodzaak om de arbeidskosten, die tot 95 procent van de contactcenterkosten kunnen uitmaken, te beperken. Conversational AI kan hierbij een hulp zijn. Het maakt agenten efficiënter en effectiever, terwijl het tegelijk de klantervaring verbetert.”

POLISNUMMER

Gartner voorspelt dat **tegen 2026 veruit één op de tien agentinteracties geautomatiseerd zal zijn, een stijging ten opzichte van de geschatte 1,6 procent van de interacties** die vandaag geautomatiseerd zijn met behulp van AI. Conversational AI kan een klantinteractie van een contactcenter geheel of gedeeltelijk automatiseren via zowel spraak- als digitale kanalen, door middel van voicebots of chatbots. Er wordt verwacht dat dit binnen twee jaar de organisaties op het gebied van klantenservice en ondersteuning ook echt zal transformeren.



“Hoewel het automatiseren van een volledige interactie – ook bekend als *call containment* of *deflection* – zorgt voor aanzienlijke kostenbesparingen, is er ook waarde in gedeeltelijke containment, zoals het automatiseren van de identificatie van een naam, een polisnummer en de reden waarom een klant belt. Door deze informatie met behulp van AI vast te leggen, kan tot een derde bespaard worden van de interactietijd die normaliter door een menselijke agent zou worden ondersteund”, weet O'Connell.

COMPLEX EN GEFRAGMENTEERD

Hoewel de voordelen van conversational AI best overtuigend zijn, is de **technologie nog in ontwikkeling**. Door het gefragmenteerde leverancierslandschap en de complexe toepassingen blijft de adoptie de komende twee jaar wellicht gematigd. “Het gebruik van conversational AI vereist dure professionele middelen voor data-analyse, knowledge graphs en natuurlijk taalbegrip”, zegt O'Connell. “Eenmaal gebouwd, moeten de conversational AI-mogelijkheden voortdurend worden ondersteund, bijgewerkt en onderhouden, wat resulteert in extra kosten.”

Complexe, grootschalige conversational AI-toepassingen kunnen meerdere jaren in beslag nemen omdat er meer callflows worden uitgebouwd en bestaande callflows worden verbeterd. Gartner schat de integratiekosten op 1.000 tot 1.500 dollar per conversationele AI-agent, hoewel sommige organisaties kosten noemen die kunnen oplopen tot 2.000 dollar per agent. Daarom zullen in het begin vooral grote contactorganisaties met 2.500 of meer agenten en voldoende IT-budgetten, gebruikmaken van conversational AI, oordeelt Gartner.

Tegen 2026 wordt

1 op de 10

interacties met agenten in een contactcenter geautomatiseerd

Met dat laatste is Hessel Wellema van Botz4u, dat zich in chatbots specialiseert, het toch niet helemaal eens. “Ik zie in onze contreien, zoals in Nederland, meer dan genoeg voorbeelden van kleinere ondernemingen die chatbots en AI op een slimme manier inzetten”, oppert Wellema. “Het staat of valt met de aanpak. Mijn aanbeveling is altijd: begin klein maar zorg wel dat je vanaf dag één capaciteit reserveert om de chatbot te trainen, trainen en nog eens trainen.”

CENTRE FOR
CYBER SECURITY
BELGIUM

Safeonweb.be

De Europese maand van cyberbeveiliging wordt 10 jaar! Voor het tiende achtereenvolgende jaar organiseert het Agentschap voor Cyberbeveiliging van Europa (ENISA) tijdens oktober de #CyberSecMonth: een jaarlijkse campagne om cyberbeveiliging onder burgers en organisaties te bevorderen en actuele informatie over online-beveiliging te verstrekken door middel van bewustmakingsactiviteiten en het delen van goede praktijken.

2022 thema's:

RANSOMWARE

PHISHING

https://safeonweb.be/nl/campagnemateriaal

#ThinkB4UClick

MULTIFACTOR-AUTHENTICATIE: HET GLAS IS HALFVOL

Voor veel securityproblemen die de ronde doen bij organisaties wordt multifactorauthenticatie of kortweg MFA als oplossing aangereikt. Het glas lijkt vandaag halfvol: het gebruik is beperkt, maar neemt toe. Het securityniveau wordt ermee opgekrikt, maar MFA is niet altijd even zaligmakend. Een stand van zaken, met zowel groeicijfers en aanbevelingen als praktische problemen en waarschuwingen.

HOE ZIT HET MET MFA BIJ BELGISCHE ORGANISATIES?

Om hierop een zicht te krijgen, kijken we naar het rapport The State of Industrial Security in 2022 van aanbieder Barracuda. Voor het onderzoek werden 800 senior IT-managers, senior IT-securitymanagers en project-managers ondervraagd (uit de VS en Europa, waaronder België) die binnen hun organisatie verantwoordelijk zijn voor industriële IT en internet of things.

Daaruit bleek dat multifactorauthenticatie (MFA) nog weinig gebruikt wordt: **slechts een op de vijf (21 procent) van de ondervraagde Benelux-organisaties** beperkt de netwerktoegang en vereist MFA voor toegang van buiten-af tot OT-netwerken.

EN WAT BIJ KRITIEKE TOEPASSINGEN?

Zelfs in kritieke industriesectoren is het gebruik van MFA nog eerder beperkt. Wereldwijd staat volgens Barracuda bijna de helft (47 procent) van de kritieke industriesectoren (zoals de energiesector) nog altijd volledige toegang op afstand toe zonder MFA.

Die cijfers liggen in lijn met het onderzoek van het Unit 42 Threat Intelligence team bij Palo Alto Networks. Dat rapport biedt inzichten uit een steekproef van meer dan 600 Unit 42 Incident Response (IR)-gevallen. **In de helft van alle IR-zaken ontdekten onderzoekers dat organisaties niet beschikten over multifactorauthenticatie op kritieke internetgerichte systemen** zoals bedrijfswebmail, VPN-oplossingen (Virtual Private Network) of andere oplossingen voor toegang op afstand.

HOE IS DE EVOLUTIE?

Qua MFA lijkt het glas halfvol en is de evolutie van tel. “Organisaties maken er almaar meer gebruik van”, zegt Martin Lee van Cisco Talos Intelligence Group, een van de grootste private threat intelligence teams in de wereld, op basis van eigen cijfers. “Bij ondernemingen steeg van juni 2020 tot en met mei 2021 het aantal gemiddelde dagelijkse authenticaties voor cloudapplicaties met meer dan 65 procent tegenover het gemiddelde in diezelfde periode van een jaar ervoor.”

In een rapport van oktober 2021 over een toekomst zonder wachtwoorden, stelt Duo Security (de MFA-toepassing die Cisco een paar jaar geleden inlijfde) dat het gebruik van Webauthn (een Web Authentication API) **sinds april 2019 vervijfvoudigd** is. De groeiende trend wordt ook bevestigd door een ander, recent rapport van Allied Market Research, aldus Martin Lee. Dat rapport stelt dat de wereldwijde markt van multifactorauthenticatie goed was voor 10,30 miljard dollar in 2020. En tegen 2030, zo berekent Allied Market Research, zal die markt doorgroeien naar 40 miljard dollar, met een CAGR (compound annual growth rate) van 18 procent in de periode 2021-2030.

“Helaas zijn gebruikersnamen en wachtwoorden nooit een bijzonder veilige methode geweest voor de authenticatie van gebruikers”, stelt Lee. “De toevoeging van MFA creëert voor aanvallers een extra horde die ze moeten nemen als ze gebruikers willen compromitteren. Met elke extra verdedigingslaag maken we het voor aanvallers dus moeilijker én kunnen cybersecurityteams aanvallen vroegtijdig identificeren en verhelpen voor het kwaad geschiedt.”

“Veel bedrijven denken na over hoe ze hun huidige MFA-aanpak kunnen professionaliseren.”

Ook in België ziet **Steven De Ruyver** van Cisco een toenemende maturiteit in MFA. “Veel bedrijven gebruiken het al op een of andere manier en nog veel meer bedrijven denken na over hoe ze hun huidige MFA-aanpak kunnen ‘professionaliseren’. Vandaag kijken we met klanten overigens verder dan MFA, bijvoorbeeld naar adaptieve toegang en single sign-on.”

ER IS NOG WERK

Tijdens hun keynote op *re:Inforce 2022*, de conferentie van techgigant AWS met focus op security, riep Amazon CSO **Steve Schmidt** op tot actie inzake beveiliging,

“De zogenaamde authenticator app zoals die van Google wordt veel gebruikt om tijdelijke codes te genereren. Maar wat als je smartphone wordt gestolen of beschadigd?”, zegt Herman Maes, data protection officer en techblogger.

Amazon CSO Steve Schmidt: "Een al te toegeeflijke omgeving staat garant voor hoofdpijn."

waaronder het inschakelen van MFA en het blokkeren van publieke toegang. Hij stimuleert ook nieuwe initiatieven, zoals het aanbieden van gratis beveiligingssleutels, die deze oproepen moesten ondersteunen. Schmidt benadrukte hoe belangrijk toegangscontrole is voor cloudbeveiliging. "Een van de belangrijkste vragen is: wie heeft toegang tot wat en waarom? Een al te toegeeflijke omgeving staat garant voor hoofdpijn", zei Schmidt tijdens de keynote. "**Wat hebben je mensen nodig om hun werk te doen? Noodzaak is hier het sleutelwoord, en dat moet strikt worden gehandhaafd**."

Dit wordt nog belangrijker als je kijkt naar de groeiende omvang van potentiële aanvallen. Schmidt zei dat AWS momenteel per maand quadriljoenen events bijhoudt, dat is een getal met 24 nullen. MFA is een van de eenvoudigste en beste manieren om een extra beveiligingslaag toe te voegen voor toegang tot de cloud, oppert hij. Als bijvoorbeeld referenties op GitHub worden gecompromitteerd, zullen gebruikers nog altijd beschermd zijn als MFA is ingeschakeld. Hij adviseerde om MFA ook in te schakelen voor AWS-accounts, voor gebruik in het dagelijkse persoonlijke leven. "MFA is een must", klinkt het. "Accounts die beschermd zijn met MFA zijn aanzienlijk veiliger dan accounts die dat niet zijn."

EN DE (SHADOW) CLOUD?

Forrester Research senioranalist **Jess Burn** erkent dat veel organisaties nog altijd worstelen met het inschakelen van MFA in de hele organisatie en het blokkeren van publieke toegang tot hun cloud instances. Bovendien, stelt Burn, heeft de uitbreiding van het aanvalsoppervlak in de cloud een extra laag van urgentie toegevoegd voor zowel ondernemingen als overheidsinstanties.

"**Het aanvalsoppervlak wordt groter omdat er zo veel clouddiensten zijn**. Het gaat niet alleen om instanties en infrastructuur, maar ook om kleine apps en diensten. En je weet niet of een cloud-app een kwetsbaarheid of een verkeerde toegangsconfiguratie heeft als je niet weet dat je hem gebruikt", zei ze, verwijzend naar het zogenaamde schaduw-cloudgebruik binnen organisaties.

NIET ZALIGMAKEND

Zaligmakend is MFA niet. De menselijke factor speelt altijd. Bij de recente hack bij Uber werd wel MFA gebruikt, maar zou de hacker contact hebben opgenomen met een Uber-medewerker - zogezegd als IT-medewerker van Uber - met het verzoek om hem toegang te verlenen. Daarnaast zijn er natuurlijk meerdere vormen **(zie pagina 13)**. Bovendien is het vaak een behoorlijke logistieke operatie om het uit te rollen in een organisatie. Veel gebruikers vinden het alvast lastig en minder gebruiksvriendelijk dan de klassieke wachtwoorden. Communicatie is dus essentieel bij de introductie van MFA in organisaties, net als IT-support.

En dan zijn er nog praktische problemen die bij veel vormen van MFA komen kijken. "De zogenaamde authenticator app zoals die van Google wordt veel gebruikt om tijdelijke codes te genereren. Maar **wat als je smartphone wordt gestolen of beschadigd?",** haalt de Belgische data protection officer en techblogger **Herman Maes** aan. "In dat geval wil je liefst een authenticator app, die toch ergens een back-up heeft. De veel gebruikte Google Authenticator-app heeft wel een *transfer feature*, maar in de voorgaande gevallen heb je hier niets meer aan", stelt Maes. Hij verwijst naar de app Authy (of Lastpass Authenticator). "Deze app gaat een *encrypted backup* in de cloud maken, maar daarnaast is er ook een multi multi-authenticatie feature om de 2FA-codes (2 factor) over verschillende toestellen te gebruiken."

MFA VIA SMS

Ook MFA via sms heeft praktische bekommernissen. "Bijvoorbeeld als je van werkgever verandert en je gsm-nummer moet overgezet worden. Meer dan eens

loopt het dan administratief mis, waardoor je gsm-nummer niet meer werkt voor 24 à 48 uur terwijl je voor een nieuwe laptop uiteraard 2FA nodig hebt. Maar op dat moment heb je dus geen toegang tot je 2FA sms-codes", vertelt Maes.

"Een al te toegeeflijke security-omgeving staat garant voor hoofdpijn."

En dan is er natuurlijk ook sim-swapping, waarbij aanvallers je gsm-nummer laten overzetten naar een nieuwe simkaart om je accounts te kunnen hacken. "Ook in België is er al een mobiele operator veroordeeld voor het te laks doorgeven van een mobiel nummer."

EN DE BEVEILIGING ZELF?

Bovendien is MFA op securityvlak niet altijd even waterdicht. Multifactorauthenticatie lijkt een geweldige manier om cybercriminelen op afstand te houden, maar sommigen worden blijkbaar behoorlijk goed in het omzeilen van dit type bescherming door applicatie- en browsersessiecookies te ontvreemden.

Cyberbeveiligingsonderzoekers van Sophos stelden bijvoorbeeld een toenemende interesse in cookies vast onder malware van alle geraffineerde niveaus. Van infostealers zoals *Racoon Stealer*, of *RedLine Stealer* tot destructieve trojans zoals *Emotet*: steeds meer virussen en malware krijgen cookiestelende functionaliteiten.

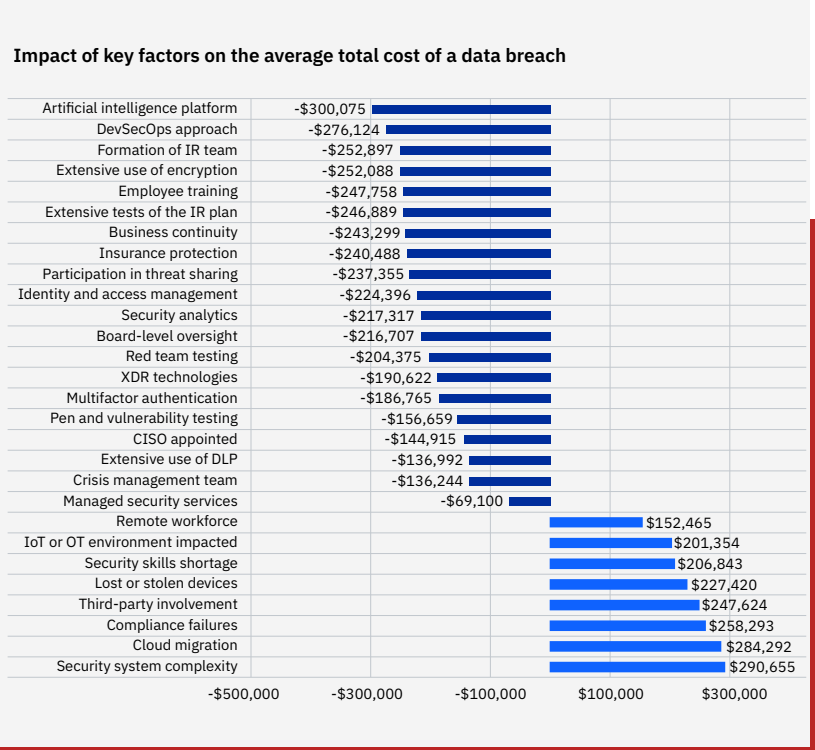
Door sessiecookies te stelen, kunnen bedreigers multifactorauthenticatie omzeilen omdat de dienst met de cookies de gebruiker al als geauthenticeerd beschouwt en gewoon meteen toegang verleent. Sophos heeft gezien dat cookies werden verkocht op het online platform Genesis, waar leden van de afpersingsgroep Lapsus$ er een kochten die resulteerde in een grote gegevensdiefstal bij videogamegigant EA. Na de aankoop van een Slack session cookie van Genesis slaagde de bedreiger erin een bestaande login van een EA-medewerker te spoofen en het IT-team van het bedrijf te verleiden netwerktoegang te verlenen. Hierdoor konden ze 780 GB aan gegevens stelen, waaronder broncode voor games en grafische engines, die later werd gebruikt bij een poging tot afpersing.

OP ZOEK NAAR DE BALANS

Het grootste probleem met cookies is dat ze relatief lang meegaan, vooral bij toepassingen als Slack. Een cookie die langer meegaat, betekent dat bedreigers meer tijd hebben om te reageren en een endpoint in gevaar te brengen. IT-teams kunnen hun browsers en apps programmeren om de geldigheidstijd van cookies te verkorten, maar dat heeft een nadeel: dat betekent dat gebruikers zich vaker opnieuw moeten authenticeren. IT-teams moeten dus de perfecte balans vinden tussen beveiliging en gebruiksgemak. Maar toegegeven: dat is een eeuwige afweging in security.

WAT BEPAALT DE KOSTEN VAN EEN DATA BREACH?

De impact van een data-inbreuk is een belangrijk aspect binnen security. Gebruik van multifactorauthenticatie kan de gemiddelde kosten van een data-inbreuk doen verminderen, maar op dat vlak lijkt het maar een middenmotor. Vooral AI en DevSecOps maken hier een grote impact, blijkt uit het *Cost of a Data Breach Report 2022*, uitgegeven door IBM. Nefast voor de kosten bij zo'n data breach is een hoge graad van complexe securitysystemen.



Bron: IBM, Cost of a Data Breach Report 2022.

DE VELE GEZICHTEN VAN MULTIFACTOR-AUTHENTICATIE

De recente perikelen bij hogeschool Vives zetten multifactorauthenticatie (MFA) meteen een stuk hoger op de agenda. Multifactorauthenticatie ondervindt wel nog enkele hindernissen in de praktijk. “Het is zowel een motivatie- als een capaciteitskwestie.” Bovendien kent MFA vele gezichten.

Enkele weken geleden lag hogeschool Vives onder het vizier van hackers. Het was geen al te destructieve cyberaanval en ook geen ransomware. **Al weken merkte de hogeschool dat cybercriminelen probeerden binnen te raken in hun computersystemen.** Begin april probeerden ze de wachtwoorden van het datamanagement van de school over te nemen. Daarop werd beslist het systeem volledig plat te leggen, om erger te voorkomen. Vives kon en kan zijn zowat 17.000 studenten en 1.500 docenten niet via mail bereiken. De hogeschool kon tegen het einde van de paasvakantie, dus een tweetal weken later, zijn systeem weer online krijgen.

MFA ALS OPLOSSING

Opvallend was dat de Vives-directeur had aangegeven dat zijn specialisten **nu ook een multifactorauthenticatie (MFA) installeren**, een extra code tijdens het inlogproces, als bijkomende beveiliging. “Wat vandaag nog bijna geen enkele hogeschool doet”, zo klonk het. Bij Vives zouden hackers geprobeerd hebben om binnen te dringen met het wachtwoord van een leerling.

Zwakke wachtwoorden en gebrekkig wachtwoordgebruik zijn een van de belangrijkste oorzaken van inbraken. “Cyberaanvallers richten zich actief op gecompromit-

De cyberperikelen brachten hogeschool Vives ertoe om multifactorauthenticatie (MFA) te installeren.

teerde wachtwoorden en maken er gebruik van, niet alleen om toegang te krijgen tot systemen, maar ook om stilletjes te opereren en organisaties te verkennen, zodat ze ongemerkt hun doelen kunnen bereiken", vertelt Lance Spitzner, een senior instructor bij het SANS Institute met meer dan twintig jaar ervaring in cybersecurity. "**Zelfs al heb je het langste, veiligste wachtwoord van de wereld, dan nog kunnen cyberaanvallers volledige toegang krijgen tot je account, systeem en gegevens** als dat wachtwoord gecompromitteerd wordt."

VERSCHILLENDE TERMEN

Microsoft schat dat MFA 99 procent van de op authenticatie gebaseerde aanvallen weerstaat. Hoewel MFA dus niet 100 procent waterdicht is, is het zonder twijfel een van de meest effectieve stappen die organisaties kunnen nemen om het risico op inbraak drastisch te verminderen. Op zijn eenvoudigst is MFA een vorm van authenticatie op meerdere niveaus, waarbij iemand zich niet alleen authenticeert met een wachtwoord (iets dat hij kent), maar ook met een soort unieke code of een apparaat (waarover hij beschikt).

"We slagen er slecht in om cyberbeveiliging eenvoudig te maken."

Er zijn om te beginnen veel verschillende termen om MFA te beschrijven. Sommige organisaties of verkopers noemen het tweestapsverificatie, tweefactorauthenticatie (2FA), eenmalig wachtwoord (OTP of One Time Password) of sterke authenticatie. "Ze impliceren allemaal hetzelfde: authenticatie waarbij twee of meer vormen van authenticatie nodig zijn. Meestal is het een wachtwoord en nog iets anders, zoals een unieke code die naar je mobiele apparaat wordt gestuurd of door dat apparaat wordt gegenereerd."

Momenteel is niet duidelijk hoeveel organisaties in België of in Europa MFA gebruiken. "Ik weet eerlijk gezegd niet wat de adoptiegraad van MFA is, die zal zowel per regio als per sector verschillen", stelt Lance Spitzner. "MFA is echter erkend als een van de meest effectieve middelen om cyberaanvallers te stoppen. **Het wordt in snel tempo vereist voor veel normen en voorschriften, zoals de nieuwe PCI-DSS. En het is ook de belangrijkste aanbeveling van verschillende autoriteiten**, zoals het CISA in de Verenigde Staten en het NCSC in het Verenigd Koninkrijk. We zullen dus zeker een versnelde adoptie zien, vooral in industrieën die een zeer lage tolerantie voor risico's hebben of die zwaar gereguleerd zijn."

HINDERPALEN

Als (bijna) iedereen overtuigd lijkt van het nut van MFA, waarom gebruikt dan nog niet iedereen het? En wat houdt hen tegen? "Het is zowel een motivatie- als een capaciteitskwestie. Mensen realiseren zich misschien niet hoe kwetsbaar stand-alone wachtwoorden zijn", stelt Spitzner. "Mogelijk denken ze dat MFA ingewikkeld of moeilijk is. **We moeten mensen uitleggen hoe ongelooflijk kwetsbaar hun accounts zijn en hoe slechts één verandering met het inschakelen van MFA een enorm verschil kan maken**. Misschien moeten mensen het eerst inschakelen voor hun belangrijkste accounts, van bankrekeningen tot e-mail, en dat dan na verloop van tijd uitbreiden."

Anderzijds is het natuurlijk een kwestie om de technische noden te voorzien en uit te rollen. Een grote belemmering komt volgens hem ook voort uit de beveiligingsgemeenschap. "We slagen er slecht in om cyberbeveiliging eenvoudig te maken", vindt hij. "We hebben bijvoorbeeld talloze verschillende termen voor MFA en discussiëren vaak over wat de beste manier is om het te gebruiken. Het is dus belangrijk dat organisaties door de ruis heen prikken en MFA zo eenvoudig mogelijk maken voor hun personeel."

WELKE VORMEN VAN MFA BESTAAN ER?

Er bestaat niet één toepassingsvorm van multifactorauthenticatie, er zijn meerdere manieren om MFA te gebruiken. Lance Spitzner overloopt enkele van de meest voorkomende methoden.

1

SMS-CODE

Een eenmalige, unieke code wordt via sms naar je mobiele apparaat gestuurd. Je gebruikt deze code dan samen met je wachtwoord om je te authenticeren en in te loggen. “Dit is de meest gebruikte methode, waarschijnlijk omdat ze het gemakkelijkst is: een individuele gebruiker hoeft alleen zijn mobiele telefoonnummer te registreren in zijn account. Bij het inloggen met gebruikersnaam en wachtwoord wordt er dan een code naar het mobiele apparaat gestuurd, als tweede authenticatiemiddel.”
Deze aanpak is weliswaar gemakkelijk, maar houdt, volgens Spitzner, ook een risico in. “Als iemand op de een of andere manier het telefoonnummer kan omleiden of de controle erover kan overnemen (zoals via sim-swapping), krijgt de aanvaller je unieke code. Bij een andere aanvalsmethode doen cyberaanvallers zich voor als een bank of IT-support en verleiden ze slachtoffers ertoe deze unieke code door te geven, waarna ze de code snel gebruiken om in te loggen in naam van het slachtoffer.”

2

CODEGENERATOR

Bij deze methode gebruik je een authenticatie-app, zoals Google Authenticator, die je downloadt op je mobiele apparaat en die unieke eenmalige codes genereert. Om MFA in te schakelen voor je accounts synchroniseer je de authenticatieapp met elke account. Deze apps kunnen honderden accounts tegelijk ondersteunen. Een andere mogelijkheid is dat je een fysiek token krijgt dat de eenmalige, unieke codes genereert. “Het gebruik van een mobiele app of een fysiek token om codes te genereren, wordt veiliger geacht dan sms-codes, aangezien het hierbij onmogelijk is voor cyberaanvallers om je telefoonnummer over te nemen. Anderzijds is deze methode nog altijd kwetsbaar voor cyberaanvallers die mensen misleiden of overtuigen om hun unieke code te delen.”

3

AUTHENTICATIENOTIFICATIES

Sommige mobiele authenticatieapps, bijvoorbeeld Authenticator van Microsoft, zorgen er ook voor dat wanneer je op bepaalde websites inlogt er geen eenmalige code gevraagd wordt maar een authenticatieverzoek naar je mobiele app gestuurd wordt om te bevestigen dat jij effectief probeert in te loggen, en niet iemand anders. “Dit is een aanpak die bijvoorbeeld vaak gebruikt wordt in het Apple-ecosysteem. Het wordt beschouwd als een veiligere aanpak, omdat er geen code is waarmee cyberaanvallers mensen kunnen misleiden. Wel kan een cyberaanvaller, wanneer hij je wachtwoord in handen krijgt, in jouw naam proberen in te loggen, in de hoop dat je het authenticatieverzoek goedkeurt.”

4

FIDO

Bij deze methode krijg je een fysiek apparaat dat op je laptop of computer wordt aangesloten en vervolgens geregistreerd wordt bij de websites waarop je regelmatig inlogt. Wanneer het apparaat op je computer wordt aangesloten (via de USB-poort) of ermee verbindt (via NFC-technologie) en je deze websites bezoekt, verifieert het apparaat je. “Yubikey is een veelgebruikt en vrij beschikbaar voorbeeld van een dergelijk fysiek apparaat dat de FIDO-norm ondersteunt. Deze aanpak is de veiligste en volgens velen meest phishing-bestendige authenticatiemethode, aangezien er geen unieke code of authenticatieverzoek is en cyberaanvallers hun slachtoffers niet kunnen misleiden”, weet Spitzner. “Daartegenover staat dat deze methode voor organisaties vaak ook de meest complexe is om te gebruiken en ondersteunen. Bovendien zijn veel websites nog niet compatibel met de FIDO-authenticatiestandaard.”

ZO GEBRUIK JE MFA BINNEN JOUW ORGANISATIE

Voor welke aanpak kiest je organisatie het best? Meestal wordt die beslissing genomen door het team dat instaat voor beveiliging en risicobeheer. “Welke methode het ook wordt, weet dat ze stuk voor stuk beter zijn dan alleen wachtwoorden”, stelt Spitzner. Hij overloopt enkele belangrijke algemene doelstellingen – die je best in acht neemt om MFA effectief toe te passen:

- Maak duidelijk en **herhaal voldoende hoe mensen baat hebben** bij deze methode, door te helpen in de verdediging tegen de meerderheid van de op authenticatie gebaseerde aanvallen.

- Probeer het concept van **MFA zo eenvoudig mogelijk te houden**. “Er zijn zoveel verschillende termen en variaties van MFA in omloop, dat mensen er vaak van in de war raken. Overstelp mensen dus niet met nodeloze info, leer hen alleen wat ze moeten weten.”

- Benadruk hoe MFA **niet alleen een oplossing is op het werk**, maar iets dat mensen beter ook thuis toepassen om hun belangrijkste accounts te beschermen, zoals voor hun bank, pensioen, investeringen of persoonlijke e-mail.

Lance Spitzner (SANS): “MFA is sowieso beter dan alleen wachtwoorden.”

Wil je jouw organisatie trainen in het gebruik van MFA en de voordelen ervan, bereid je dan voor door het zelf uit te proberen, besluit Spitzner. “Stel MFA niet alleen in voor jouw professionele maar ook voor persoonlijke accounts zoals Gmail of Amazon. Zo raak je niet alleen meer vertrouwd met de technologie, maar maak je ook kennis met de verschillende methodes en benaderingen om MFA toe te passen.”

ARCHITECTUUR BIJ BOL.COM

EEN ARCHITECT VOOR ELK DOMEIN

Hoe plaats je architectuur en de rol van een architect in een organisatie? Bol.com kiest alvast voor een decentrale aanpak. Coördinatie wordt tot een minimum beperkt. “Het geeft een goed beeld van de evolutie en rol van architectuur in organisaties.”

Paul Teeuwen, zelfstandig consultant in enterprise architecture en TOGAF (The Open Group Architecture Framework, een methode om de enterprisearchitectuur te ontwikkelen en beheren) overliep tijdens een webinar voor SAI een aantal cases rond enterprisearchitectuur.

1 DOMEINEN

Eén case die in het oog sprong, was de aanpak rond architectuur bij de bekende online retailer bol.com. De organisatie gelooft namelijk heel erg in het inschakelen van kleine (en agile) teams. “Die kleine teams werken iets uit, waar vervolgens uit moet blijken of dat ook op grotere schaal kan werken binnen de organisatie of niet. Als het werkt, gaat het verder scale-up”, omschrijft Paul Teeuwen.

Elk businessdomein bij bol.com heeft meerdere zulke teams. Zo’n businessdomein omschrijven ze bij bol.com als product, wat een beetje een afwijkende terminologie is. Elke business owner (van zo’n businessdomein dus) beschikt ook over een (product)architect én ook een technical lead. “De productarchitect kun je eerder zien als een businessarchitect, terwijl de technical lead eerder de rol van de klassieke IT-architect invult.”

Voorbeelden van businessdomeinen (of producten dus, in het bol.com-jargon) zijn onder meer advertising, klantenservice, logistiek, marketing, productcatalogus, partnerservice, data, supply chain, customer journey of security. In totaal zijn er een vijftiental. Elk van deze domeinen heeft een eigen (product)architect. De filosofie is dat zo’n architect verantwoordelijk is voor dat specifieke product, maar dat ze bij bol.com met z’n allen verantwoordelijk zijn voor de hele organisatie.

2 TEAMS

De architecten zijn ervoor verantwoordelijk dat alles goed blijft lopen. Wat ze bij bol.com niet of eerder beperkt doen, is alles met alles in verbinding brengen en trachten om een totaaloverzicht te hebben op de totale architectuur binnen de groep. “Daar is het bedrijf enerzijds te groot voor geworden en anderzijds verandert de omgeving te snel daarvoor.”

Oorspronkelijk had een architect twee tot drie agile teams ter beschikking, wat nog werkbaar was.

Maar zodra de onderneming sterk groeide, werd deze aanpak dus onhoudbaar. Op een bepaald moment gingen ze naar negen teams met drie architecten. “Dat werd te veel. Dan loop je als architect achter je eigen staart aan”, merkt Teeuwen op.

Uiteindelijk koos bol.com voor een andere aanpak en hierbij staat DevOps centraal: *build, test, release & run*, met de architect die coördineert. “Daarnaast hadden ze nog enkele andere specialisten zoals voor *user interface & opportunity analysis*. Wat ze uiteindelijk gedaan hebben, is de andere mensen ook in de teams getrokken. Maar de rol van de zogenaamde solution architect is bij de senior designers terechtgekomen.” Terwijl de rol van de productarchitect dus dichter bij de domeinbeheerder of product owner is komen te liggen.

3 COÖRDINATIE

Hoe coördineren ze dan onderling? “Ze opteren voor een product owner en een backlog”, legt hij uit. “Ze werken met microservices waardoor je vragen kunt stellen en als je vraag belangrijk genoeg is, dan komt die vraag hoog op de backlog”, klinkt het. Ze coördineren tussen de individuele domeinen en ze coördineren niet *overall*. “Wij kunnen niet alles coördineren, is de inschatting.”

In die opvatting kan Paul Teeuwen zich voor een stuk ook wel vinden. “Coördinatie is ook *overhead*. Het kost geld en mankracht. En ook vaak politiek kapitaal. Als je iets niet hoeft te coördineren, hoef je het ook niet te doen”, stelt hij. “Je hoort soms: we moeten het samen doen, want dan is het beter. Ja, maar dat samendoen op zich is niet genoeg. Je moet met dat samenwerken op bepaalde aspecten ook echt kunnen verbeteren. Het is beter omdat het bijvoorbeeld minder risico’s telt. Of het is beter omdat we bijvoorbeeld zaken kunnen doen die we anders niet zouden kunnen bewerkstelligen.”

“Met alleen IT-kennis red je het niet meer als architect.”

PAUL TEEUWEN
Zelfstandig consultant
in enterprise architecture

In hun niet-coördinatie, daar zijn ze bij bol.com ook wel een tijdje vrij extreem in geweest, weet de consultant. “Iedereen mocht zijn eigen infrastructuur hebben onder het motto: dit zijn DevOps-teams dus die weten toch wel wat ze nodig hebben. Die aanpak is toch weer een beetje teruggedraaid. Ze hebben nu wel gezamenlijke infrastructuur.”

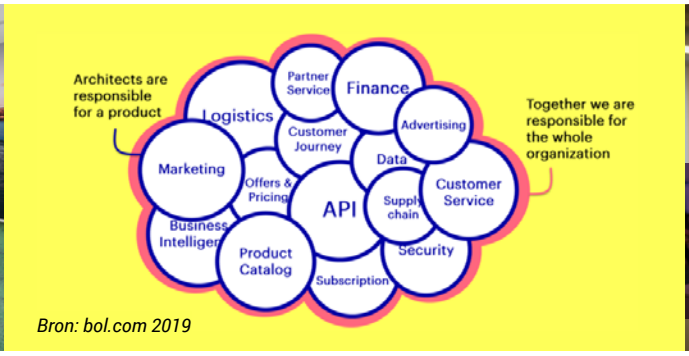
4 ARCHITECT

De case bij bol.com geeft tegelijk een stand van zaken ten aanzien van architectuur en de rol van de architect, ook al valt die (zoals in deze case blijkt) in diverse hoedanigheden. Wat is ten slotte de waarde van architecten? “Ze brengen visie op lange termijn, zorgen dat er coördinatie is waar nodig en zijn *trusted advisors*”, vat hij samen. “We zijn als architecten nog altijd de bewakers van het IT-landschap en eigenlijk ook van het businesslandschap, maar doen het wel op een andere manier.”

Zelf heeft Teeuwen de rol van de architect ook wel zien veranderen. “De architect gaat aan de slag met de mensen in het project. In zo’n enterprisearchitecture-afdeling is het standaard dat je de helft van je tijd in grote sleutelprojecten en in teams meedraait”, oppert Teeuwen. Hij stelt wel vast dat de tevredenheid over de architect is achtergebleven. “Terwijl we het beter doen dan vroeger. Maar de verwachting is veel meer gestegen.”

De nieuwe architect moet dan ook een soort van businessconsultant zijn, al verschilt de mate waarin hier en daar. “Met alleen IT-kennis red je het niet meer. Maar of je als architect, zoals je weleens hoort, tegelijk systeemprogrammeur of projectmanager moet zijn, een MBA behaald moet hebben en bij McKinsey moet kunnen werken? Het zou mooi zijn, maar daar zijn er niet veel van. Je moet daar als architect ook je eigen rol in zien én nemen, tussen business en IT.”

» *Herbeluister **hier** het SAI-webinar over ‘wat heeft enterprisearchitectuur ons opgeleverd?’ en andere cases.*



Bron: bol.com 2019


De rol van de architect bij bol.com bevindt zich op het niveau van diverse domeinen.

DE COMEBACK VAN SQL

Naar IT-normen is de query-taal SQL al behoorlijk op leeftijd. Toch lijkt SQL om diverse redenen een comeback te beleven. "Vergis je niet: SQL is nooit helemaal weggeweest."

Het opzet van SQL of Structured Query Language is bekend. Het is een gestandaardiseerde taal voor onder meer het bevragen en aanpassen van gegevens in een relationele database. SQL kan met bijna alle moderne relationele databaseproducten worden gebruikt.

Met de opmars van nieuwe technologieën en alternatieve databanken en databanksystemen, genre NoSQL, kwam SQL in de hoofden van heel wat IT'ers in het verdomhoekje terecht. Al is dat een kwestie van perceptie. Intussen lijkt SQL een heuse comeback te beleven. Velen blijken SQL uiteindelijk niet zo slecht te vinden voor gebruik. Veel hedendaagse data- en databasemanagementsystemen zoals Snowflake en Dremio gaan volop met SQL aan de slag. **In de context van werk en IT-jobs legt SQL ook de brug tussen de datawereld en de ontwikkelwereld.**

MODE VERSUS POPULARITEIT

"Als je vraagt naar het feit of SQL een comeback beleeft, gaat de vraag eigenlijk of SQL opnieuw modieus is. Je vraagt eigenlijk naar mode, niet naar populariteit", reageert Bill Karwin, datawetenschapper en auteur van *SQL Antipatterns: Avoiding the Pitfalls of Database Programming*. "Modieus betekent dat de technologie door veel mensen wordt besproken. Populair betekent dat de technologie door

veel mensen wordt gebruikt", stelt Karwin resoluut.

Zijn opmerking spreekt boekdelen: volgens Karwin heeft SQL nooit aan populariteit ingeboet. "De overgrote meerderheid van databasetoepassingen gebruikt SQL en dat is nooit veranderd. **Zelfs toen sommige bedrijven NoSQL aan het uitproberen waren, heeft dit er niet toe geleid dat SQL aan populariteit heeft ingeboet**. De meeste bedrijven die NoSQL inschakelden, gebruikten dat voor nieuwe projecten. SQL vervangen door NoSQL voor bestaande projecten gebeurde niet zo vaak."

Bovendien groeit de totale markt voor softwareprojecten in een hoog tempo, beklemtoont Karwin. "Terwijl NoSQL in sommige projecten werd uitgeprobeerd, waren er ook beginnende projecten die nog altijd SQL gebruikten. Het absolute gebruik van zowel SQL als NoSQL nam tegelijkertijd toe, omdat de vraag naar databasetoepassingen in het algemeen voortdurend toeneemt."

NETFLIX

SQL heeft nooit een echte comeback nodig gehad, oppert ook Greg Kemnitz, staff database engineer bij FitBit (intussen overgenomen door Google), op Quora. "Zelfs op het hoogtepunt van de NoSQL-hype, werd een grote meerderheid van de productie van datawerelden ingezet in relationele database engines van een of ander type, en de overgrote meerderheid van deze gebruikten SQL", stelt hij.

"De overgrote meerderheid van databasetoepassingen gebruikt SQL en dat is nooit veranderd."

Vaak springen voorbeelden van bepaalde toepassingen in het oog. Zo werd Netflix bijvoorbeeld vaak aangehaald als NoSQL-gebruiker. "Ik weet wel dat Netflix een gebruiker is geweest van Apache Cassandra voor delen van zijn infrastructuur en ook andere SQL-gebaseerde databases voor andere toepassingen heeft gebruikt", oppert Kemnitz. "Er was een periode van ongeveer anderhalf jaar waarin NoSQL-fans dachten dat ze op de een of andere manier zouden *winnen* en SQL zouden vervangen door deze of gene NoSQL DB-engine", weet hij. "**Maar vergeet niet dat er voor elk web-scale applicatiedomein duizend salarisadministratie-databases, inventaris-databases, werknemers-databases, financiële databases, productcatalogus-databases en dergelijke zijn**."

SCALING

Wim Van Leuven, big data solutions architect bij Dataroots, erkent dat voor klassiek gebruik en een beperkt systeemaanbod SQL wellicht geschikter is. "Maar als je specifieke toepassingen hebt en bijvoorbeeld geoptimaliseerde queries wenst, dan kun je wellicht vertrouwen op de NoSQL-variant." Die specifieke noden zijn divers, zoals scaling (een behoefte die de laatste jaren overigens alleen maar is toegenomen) en **de diversiteit van het NoSQL-landschap** met de varianten die vaak opduiken: *key-value stores, document stores, column family data stores* en *graph databases*. Ook Greg Kemnitz erkent dat. "NoSQL DB's zijn geweldig in een aantal dingen en dan denk ik vooral aan extreme scaling van relatief eenvoudige non-joiney document-type datastores", haalt hij aan. "Tegenwoordig is het vrij gebruikelijk voor grote webdatawerelden om hybride oplossingen te gebruiken die SQL en NoSQL databases combineren. Het beste van de twee datawerelden dus."

Elke grote organisatie zal honderden of duizenden databases hebben, zo besluit hij. "Ze zullen alles gebruiken, van Access en Excel tot Postgres en MySQL en mogelijk IBM-mainframes. Het is tegenwoordig zeldzaam om één enkele standaard databasetechnologie te hebben voor alle organisaties, behalve de kleinste. De databasetechnologieën die goed werken voor human resources of finance, zijn niet noodzakelijk de beste voor klantgerichte websites, en vice versa."

HET VERHAAL VAN SQL: EERST BEDOELD VOOR EINDGEBRUIKERS

SQL werd in de loop van de jaren zeventig ontwikkeld door IBM. In de jaren tachtig werd SQL gestandaardiseerd en vervolgens kreeg het diverse versies en smaken. Bijna elk DBMS heeft zijn eigen extra functies toegevoegd aan SQL-92. Dit maakt dat computerprogramma's waarbij de database-interface werd geschreven met behulp van SQL **niet noodzakelijk zonder problemen kunnen worden gemigreerd van de ene naar de andere SQL-compatibele database**. In vele gevallen werd door de ontwikkelaar van de software een SQL-functie gebruikt die alleen bestaat in de SQL-implementatie van één specifiek DBMS.

In eerste instantie werd SQL ontwikkeld als een vraagtaal voor de eindgebruiker. Het idee was dat businessmanagers SQL zouden gebruiken om bedrijfsgegevens te analyseren. Achteraf is gebleken dat SQL te complex is om door eindgebruikers toegepast te worden. Het gebruik van SQL impliceert immers een volledige kennis van de structuur van de te ondervragen database. Daarom bleef het binnen de context van IT en database administration. Die context deinde geleidelijk wel uit. **SQL is een belangrijke en interessante vaardigheid voor een resem profielen** van business analysts, datawetenschappers en software engineers.

DE TWEEDUIZEND NIEUWE WERKPLEKKEN VAN MARC O'POLO

Het modelabel Marc O'Polo bouwt een digitale werkplek voor zijn tweeduizend medewerkers. Niet alleen samenwerking maar ook beveiliging geven VDI of virtual desktop infrastructure (opnieuw) een duwtje in de rug.

Marc O'Polo is een van 's werelds toonaangevende premiummerken voor moderne vrijetijdskleding. Het modebedrijf werd in 1967 in Stockholm opgericht en de merkfilosofie hecht waarde aan individuele persoonlijkheden. "De vrijheid om jezelf te zijn", is het leidende principe van het bedrijf en vormt de basis van de bedrijfscultuur. Die vrijheid slaat eigenlijk ook op de werkcultuur. Het in Stockholm gevestigde modelabel oordeelde dat de switch naar werken op afstand, die met corona een boost kreeg, geen tijdelijke trend was. Ze begonnen met het ontwerp van een digitale workspace. "Het is ons doel om een werkomgeving te creëren waarin onze tweeduizend werknemers wereldwijd hun creativiteit kunnen ontwikkelen en zo goed mogelijk vanaf iedere locatie kunnen samenwerken", zegt Matthias Holzner, manager IT application & collaboration bij Marc O'Polo.

Om zijn doel te bereiken, gebruikt Marc O'Polo een reeks van Citrix digital workspace-oplossingen waarmee het team waar dan ook constante, veilige en betrouwbare toegang heeft tot systemen, applicaties en data. Deze Citrix-oplossingen zijn onder andere: Citrix Virtual Apps and Desktops, Citrix Gateway, Citrix Analytics for Security en Citrix Analytics for Performance. **Citrix lag de voorbije jaren als bedrijf, mede door security-perikelen, weleens onder vuur. Maar naar aanleiding van corona en de opmars van het thuiskantoor kwamen het bedrijf en zijn oplossingen (opnieuw) in het vizier van menig IT-verantwoordelijke**.

RANSOMWARE

Om te zorgen dat de collecties tijdig bij de meer dan dertig retailpartners belanden, is een betrouwbare toegang nodig tot een groot aantal grafische en creatieve applicaties én de Enterprise Resource Planning-software die alle productie- en verkoopprocessen van het bedrijf controleert. "We zijn voorbereid op iedere manier van hybride werken en kunnen optimaal een flexibele werkstrategie ondersteunen", zegt Holzner. "Door de nieuwe infrastructuur kunnen onze werknemers vanaf iedere locatie inloggen en hun creatieve werk uitvoeren."

Werknemers kunnen bovendien veilig werken, wat een belangrijk aandachtspunt was en is. Nadat het bedrijf in 2019 werd getroffen door een ransomware-aanval, begonnen Holzner en zijn team aan een volledige vernieuwing van de IT-infrastructuur om de beveiliging te verbeteren. Het beheer van de omgeving is overgeheveld naar Citrix Cloud, zodat alleen servers met virtuele applicaties nog on-premises draaien. "Deze vernieuwing zorgt ervoor dat alle updates en securitypatches automatisch worden geïnstalleerd en de IT-omgeving altijd geüpdatet is", zegt Holzner. De nieuwe infrastructuur voorziet ook in continue monitoring en optimalisatie van de beveiliging en prestaties van de digitale werkplekken van Marc O'Polo via Citrix Analytics for Security. Volgens Holzner speelt dat een centrale rol in de hele beveiligingsstrategie van het bedrijf.

Een dashboard geeft een overzicht van mogelijke risico's en gebruikt verkeerslichten om aan te duiden waar het nodig is om in te grijpen. "Zo kunnen veel acties via beleidsregels geautomatiseerd worden", zegt Holzner. "Als een gebruiker die geregistreerd staat in Stephanskirchen bijvoorbeeld een paar uur later inlogt vanaf een adres in Azië, dan wordt de account direct geblokkeerd en krijgt het team een notificatie binnen."

GEBRUIKERSERVARING.

Bedrijven en medewerkers die aan de slag gaan met Citrix opperen weleens dat het een alles-of-niks-benadering is. Vermits het principe draait om een zogenaamde *thin client*-benadering zijn een vlotte (online) werking, verbinding en gebruikerservaring cruciaal. Ligt het systeem plat (of werkt het niet naar behoren), dan heeft dat meteen een flinke impact voor de eindgebruiker en de organisatie in het algemeen.

Marc O'Polo wil een betrouwbare ervaring bieden aan medewerkers die hen in staat stelt het beste uit hun werk te halen. Door alle relevante prestatiegegevens met het gebruik van Citrix Analytics for Performance samen te voegen in één overzicht, moet de service waardevolle inzichten opleveren en concrete aanbevelingen voor troubleshooting. Het team van Marc O'Polo kan die gebruiken om snel problemen te identificeren en op te lossen en de impact ervan te beperken. "We gebruiken Analytics for Performance om onze gebruikersondersteuning te optimaliseren, aangezien we snel willen kunnen achterhalen waarom responstijden van applicaties niet toereikend zijn voor individuele gebruikers," zegt Holzner. "Zo vonden we bijvoorbeeld verouderde software op de apparaten van een eindgebruiker die de inlogtijden flink vertraagden. Dat hebben we verholpen."

Keuze voor technologie à la Citrix is een uitgesproken keuze voor organisaties en hun IT-afdelingen, die bedrijven tegelijk ook doet standaardiseren. De nieuwe Citrix-omgeving heeft de IT drastisch vereenvoudigd, klinkt het bij Marc O'Polo, dat naar eigen zeggen mikt op een werkomgeving die altijd beschikbaar en up-to-date is. "We besteedden gemiddeld één uur per dag om ieder systeem te checken", zegt Holzner.

IGEL EN CITRIX: TWEE VDI-PARTIJEN EN HUN TROEVEN

Een blik op de markt: we vroegen aan twee vooraanstaande specialisten in (onder meer) *vitual desktop infrastructure* wat hun troeven zijn in vergelijking met de concurrenten. Al spreken ze bij Igel liever over *end user computing*.

JED AYRES (CEO VAN IGEL)
WAT ZIJN DE USP'S OF TROEVEN VAN IGEL?

"Ons *Igel ready program* is zeker een troef. We hebben meer dan 120 tech-partners in ons ecosysteem, zodat onze klanten met vertrouwen diensten en producten kunnen afnemen bij ons. Daarnaast is er ons ontwikkelingsteam. **We beschikken over expertise en tientallen jaren ervaring in end user computing met een team dat al meer dan honderd medewerkers telt en nog altijd groeit.** Daarnaast bieden wij een Day One-ondersteuning voor Citrix- en VMware-clients en Linux-client naar keuze voor AVD en Windows 365. We zijn ook gepassioneerd om ervoor te zorgen dat Microsoft Teams en unified communications werken voor onze klanten."

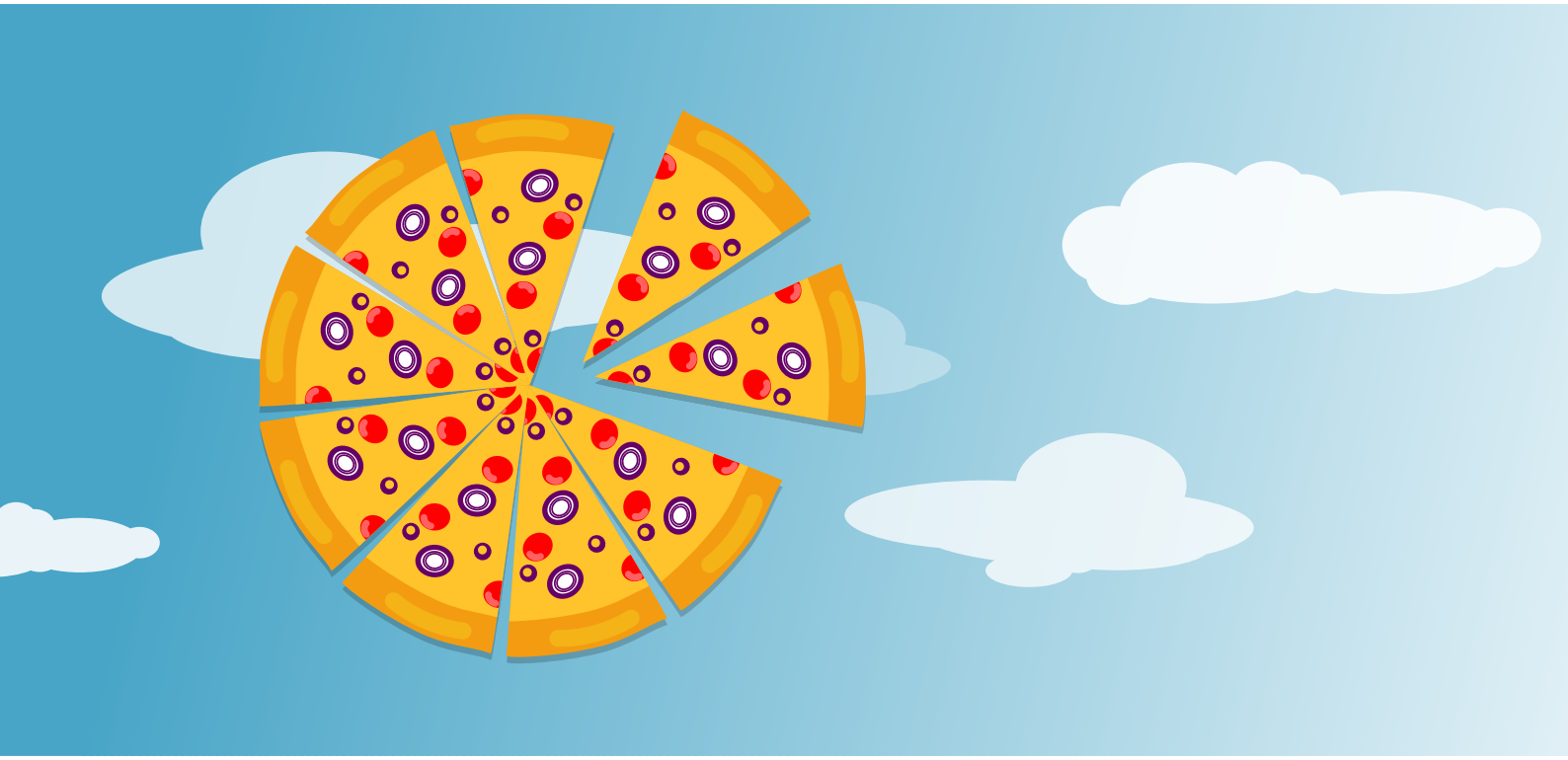
"Onze diensten en ondersteuning omvatten technical relationship managers (TRM's) om klanten te helpen hun Igel-toepassingen te schalen tot meer dan 100.000 zetels. Daarnaast hebben we een groeiend kanaal en partnerships met wereldwijde systeemintegrators (GSI's). In 2022 brengt de *DISRUPT On Tour event series* het *end user computing*-ecosysteem samen in meer dan 22 steden over de hele wereld."

NIEK BOEVINK (LEAD PRE-SALES ENGINEER BIJ CITRIX)
WAT ZIJN DE USP'S OF TROEVEN VAN CITRIX?

"Citrix is samen met cloud-technologie geëvolueerd. We doen meer dan virtual desktops. Met onze Desktop-as-a-Service leveren we applicaties en content in de breedste zin van het woord. Nu softwareleveranciers de transitie naar SaaS-modellen maken, bieden wij een framework met één look & feel die op elk apparaat op een veilige manier iedere content en applicatie kan leveren. VDI is daar een onderdeel van, maar ook web- en SaaS-applicaties integreren we in dat framework. Dat oogt als een portaal en is met een mobile app te gebruiken. Het framework zorgt er kortgezegd voor dat je device-onafhankelijk op een veilige manier kunt werken."

"Als toevoeging daarop kunnen we ook in single sign-on voorzien, én we leveren een aanvullende securitylaag. Zo kunnen we de gehele workspace beveiligen tegen screenscrapers en keyboardloggers, ook in het geval van web- en SaaS-applicaties. Daarbij kunnen we ook zaken uitschakelen als *knippen/plakken, opslaan als en printen*. Bovendien verrichten we **contextuele toetsing: bij open WiFi-netwerken kun je bijvoorbeeld vertrouwelijke datatoegang beperken. Het is ook mogelijk om een onderscheid te maken tussen vertrouwde devices en privédevices en verschillende functionaliteit en datatoegang te leveren op basis van gebruikersprofielen**. Dat maakt ons uniek. We kunnen data en applicaties uniform aanbieden en de veiligheid borgen, zelfs voor apps die niet door ons beheerd worden.

Daarbovenop bieden we een laag waarmee we inzichten kunnen verschaffen over performance en security. Over de performance-as geven we inzichten aan beheerders en helpdesk over de eindgebruikerservaring, zodat ze geïnformeerd ondersteuning kunnen bieden aan gebruikers. Daarnaast geven we hen handvaten waarmee ze meer grip op hun werknemerservaring krijgen. Langs de security-as bieden we inzicht in de veiligheid van gebruikersnetwerken en devices. Wat speelt er op privédevices van gebruikers? Misschien werken ze wel op een jailbroken device? Dat komt met zekere security-overwegingen. Tot slot is Citrix in staat omgeving- en applicatie-agnostisch een optimale en veilige gebruikservaring te bieden, of apps nu in de cloud leven of on-prem, op Google of op AWS."



VAN PIZZA DAY TOT CLOUDMONEY

Laszlo Hanyecz postte op 18 mei 2010 op het forum Bitcointalk een klein verzoek: hij wilde als gerenommeerde bitcoin-adept graag twee grote pizza's kopen voor 10.000 bitcoin. De totale waarde toen: 41 dollar. Laszlo gaat de geschiedenis in als de persoon die de hoogste prijs heeft betaald voor pizza's. Omgerekend naar vandaag, zouden ze bijna 220 miljoen dollar waard zijn.

Ook al was bitcoin in 2010 een zeer weinig bekende technologie, toch bleken veel mensen geïnteresseerd in het pizza-aanbod van Laszlo. Op 22 mei 2010 kreeg hij zijn langverwachte pizza's thuis geleverd door Jeremy Sturdivant. Die transactie maakte van Laszlo de eerste persoon die een goed kocht met bitcoins en van Jeremy de eerste persoon die iets verkocht. Zoals Jeremy zelf later zou zeggen: "Geef een man een pizza en hij heeft eten voor een dag; laat hem pizza kopen met bitcoins en het zal een revolutie teweegbrengen in de economie."

VUILNISBELT

Bitcoin Pizza Day is vandaag quasi een cryptofeestdag. Maar het is niet het enige onwaarschijnlijke verhaal dat er over bitcoins de ronde doet. Een ander berucht verhaal is de vuilnisbelt in Newport. Over James Howells, een IT-medewerker, die in 2009 op zijn persoonlijke laptop bitcoins begon te mijnen. De laptop ging stuk, maar hij hield de harde schijf bij. Hij gebruikte die om bitcoins te verzamelen.

Tijdens een grote schoonmaak in 2013 gooide Howells zijn harde schijf boordevol bitcoins per ongeluk in de afvalbak. De inhoud ervan kwam terecht op de plaatselijke vuilnisbelt in Newport, Zuid-Wales. Sinds Howells foutje werd er per jaar 50.000 ton afval op de vuilnisbelt bijgestort. Het zoeken naar de schijf zou een complexe onderneming zijn, en James staat te popelen om te beginnen graven, maar de gemeente laat het nog altijd niet

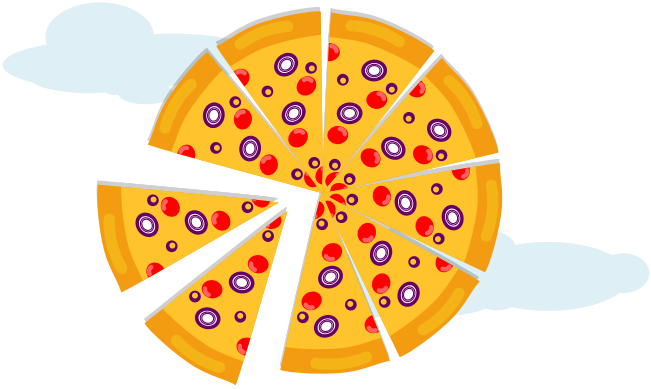
toe: de impact op het milieu zou te groot zijn. En de 7.500 bitcoins op zijn laptop? Die zijn vandaag vele miljoenen euro's of dollars waard.

De voorbeelden staan in het boek *Bitcoin & crypto* van Gwen Busseniers, waarbij de auteur op een laagdrempelige manier in de cryptowereld duikt. Een goede aanvulling op je algemene kennis. "Zo schuilt er achter de meer dan 18.000 cryptocurrency's een boeiend en uitgebreid universum – web 3.0 of de blockchain – met eigen wetten, gewoontes en verhalen", klinkt het. "Het gaat om een disruptieve technologie die een heuse impact heeft op onze maatschappij, gezien het de nood aan centraal validerende partijen, zoals banken, notarissen, bepaalde overheidsdiensten, helemaal kan uitsluiten."

CLOUDMONEY

Specifiek over de financiële sector en de wereld van geld gaat het in het boek *Cloudmoney* (ook vertaald naar het Nederlands, met overigens dezelfde titel) van Brett Scott, die zowel journalist, activist, monetair antropoloog als voormalig broker is. *Cloudmoney* behandelt het samengaan van Big Tech en Big Finance. "Een fusie én een acquisitie tegelijk", stelt Scott. "Wat fuseert is Big Tech en Big Finance, wat wordt geacquireerd is macht: **zodra deze fusie is afgerond, zullen Big Tech en Big Finance een mate van macht over ons hebben die in de hele geschiedenis haar weerga niet kent."**

Beide partijen hebben groot belang bij de digitalisering van geld. "Er woedt een *war on cash*", stelt Scott vast. In zijn boek legt hij bloot wat de verschillende vormen van geld van elkaar onderscheidt – op technisch, politiek

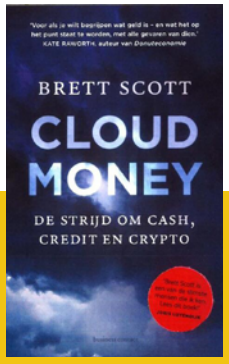


en cultureel vlak – en wat de gevolgen van deze *war on cash* zijn voor de samenleving.

Wie onze digitale voetafdruk beheert, beheert ons leven. En wie ons de toegang tot ons geld kan ontzeggen, kan ons onze vrijheid ontnemen. Deze digitale (r)evolutie werpt vragen op. Wie halen de meeste winst uit een cashloze samenleving en wie raken erdoor op achterstand? Betekent het einde van cash ook het einde van privacy? "Je moet al die verhalen over de zogenaamde onvermijdelijke vooruitgang van digitaal geld en finance niet zomaar voor zoete koek slikken", oppert hij.

Brett Scott duikt in de verschillende vormen van geld en laat zien wat de strijd om cash, credit en crypto betekent voor de samenleving. "Wie goed kijkt, ziet dat bedrijven uit Big Tech en Big Finance elkaar vooruitstuwen naar posities binnen een gestaag uitdijend mondiaal supersysteem." Eén boodschap duikt alvast her en der op in zijn boek: **het afbouwen of afvoeren van een cashloze samenleving is minder onschuldig dan velen zouden denken.** Want wat gebeurt er als alles van waarde traceerbaar is?

Bitcoin & crypto
van Gwen Busseniers,
Uitgever: Borgerhoff & Lamberigts,
ISBN: 9789463937306



Cloudmoney, de strijd om cash, credit en crypto
van Brett Scott,
Uitgever Business Contact,
ISBN: 9789047013099

TIEN MUST-HAVES OM JE SOFTWAREPROJECT TE DOEN KELDEREN

Naar aanleiding van het SAI-webinar *500k gespendeerd aan een gefaald softwareproject?* geven we een (ironische) handleiding met tips om het aanstaande softwareproject in je organisatie danig in de gracht te rijden. Experts uit binnen- en buitenland delen hun visie.

IT-afdelingen en -teams storten zich vaak met de beste bedoelingen in nieuwe softwareprojecten. Dan is het extra vervelend of frustrerend dat zo'n project niet loopt zoals het zou moeten, of erger nog: compleet ontspoort. Daarom zijn de IT-deelnemers zich best op voorhand bewust van de potentiële valkuilen. Kwestie van verspilling van tijd, inspanningen en budgetten te voorkomen. Dit zijn tien veelvoorkomende redenen (must-haves, zo je wil) waarom softwareprojecten mislukken én wat tech-teams ertegen kunnen doen. Het zijn zeker niet de enige must-haves, maar ze duiken zelfs anno 2022 nog vaak op om je project ten gronde te richten.

FAIL FACTOR 1

LAAT DE EINDGEBRUIKER LINKS LIGGEN

Een van de redenen waarom softwareprojecten nog vaak mislukken, is het gebrek aan begrip van de behoeften van de business en het ontbreken van een gedetailleerde uitleg. De business moet nu eenmaal duidelijk de eisen in detail meegeven. Kenmerken en functies moeten nauwkeurig worden afgestemd op hun behoeften.

"Het toewijzen van een doorgewinterde businessleider aan het projectteam is essentieel voor succes", zegt Wesley Crook, chief executive officer bij FP Complete, een full-stack technologiebedrijf, in het zakenblad *Forbes*.

FAIL FACTOR 2

FORMULEER DE EISEN ZO ONDUIDELIJK MOGELIJK

In het verlengde hiervan zijn onduidelijke vereisten ook een vaak voorkomende reden waarom softwareprojecten mislukken "Verwarring

over het doel van het project is een klassieker. Als de ene manager ervan uitgaat dat het IT-project georganiseerd wordt om het aantal personeelsleden te verminderen, en de andere dat het erom gaat de dienstverlening aan de klant te verbeteren, dan ben je goed vertrokken om het project te doen mislukken", haalt Christiane Vandepitte aan. Zij is consultant, businessanalist, softwaredesigner en auteur van het boek *Informatiseren zonder omwegen*.

Heel vaak weten klanten zelf niet precies wat ze willen zien en hierdoor kan het project niet verder of heeft het geen nut. Meer dan eens beginnen softwareprojecten met een geweldig idee dat (op tijd of te laat) wordt toegepast en opgeleverd, om er vervolgens achter te komen dat het probleem dat ze hebben opgelost eigenlijk niet het probleem was dat de klant wilde oplossen.

FAIL FACTOR 3

DISCUSSIEER EINDELOOS OVER DE PRIORITEITEN

Het primaire doel van een softwareproject is de problemen van een bedrijf oplossen. Dit vereist niet alleen effectief en efficiënt projectmanagement en *stakeholder expectation management*, maar ook een duidelijke consensus van de gehele groep van stakeholders over de definitie van het bedrijfsprobleem en een robuuste uitvoeringsstrategie om software op te leveren die de bedrijfsdoelstellingen oplost. Als geen van de hierboven genoemde aspecten wordt aangepakt, leidt dat tot een ontspoord project.

Een veel voorkomende reden, waarom softwareontwikkelingsprojecten mislukken, is namelijk wanneer de projectsponsors en projectteams niet duidelijk op één lijn zitten over de topprioriteiten voor het project, stelt ook Christiane Vandepitte vast. Het onderverdelen van deze prioriteiten in 'must-haves', 'should-haves' en 'could-haves' kan bijvoorbeeld

"Verwarring over het doel van het project is een klassieker bij het falen van softwareprojecten", stelt Christiane Vandepitte.

een houvast bieden voor de oplevering van bepaalde onderdelen.

FAIL FACTOR 4

HOU ALTIJD VAST AAN DE VOOROPGESTELDE SCOPE, OOK TEGEN BETER WETEN IN

Hoewel het belangrijk is om het probleem te begrijpen en de use cases vooraf te definiëren, kan bijna geen enkel project als succesvol worden beschouwd als het zich niet aanpast aan (eventueel) veranderende *business requirements* tijdens de ontwikkeling. Agile werken en denken is dus een must. "Helaas blijven sommige technische teams vasthouden aan het oorspronkelijke doel, waardoor hun inspanningen ineffectief worden of zelfs mislukken", zegt Song Bac Toh, vice president product management bij netwerkbedrijf Tata Communications.

FAIL FACTOR 5

CHANGE MANAGEMENT LINKS LATEN LIGGEN

Softwareprojecten gaan over change management, over veranderingen in bedrijfsprocessen. Bij de ingebruikname van de nieuwe toepassing verandert het werk van het personeel: er zijn andere taken en ze moeten anders verdeeld worden. Ook dat deel wordt onderschat. "Als je een project echt wilt doen mislukken, vermijd je vooral vergaderingen over mogelijke verbeteringen van de bedrijfsprocessen. Zeg dan bijvoorbeeld dat het nieuwe systeem precies hetzelfde moet doen als het oude", stelt Christiane Vandepitte met een flinke dosis ironie. Ook vaak onderschat is het testen van het systeem. "Wil je mislukken, geef dan de toekomstige gebruikers van de toepassing zo veel werk dat ze geen tijd hebben om de toepassing te testen voor ze ingevoerd wordt."

FAIL FACTOR 6

WERK ZO VEEL MOGELIJK IN SILO'S

Dat teams op pad gaan om iets te bouwen dat ofwel geen bedrijfsbehoefte heeft, ofwel niet het juiste probleem aanpakt, is het gevolg van een slechte afstemming tussen de business en de technologie. Om dit te voorkomen, is het cruciaal om het probleem te identificeren dat de business probeert op te lossen en vervolgens samen te werken met de business en niet in een silo.

Veel softwareprojecten lopen vertraging op of mislukken door een gebrek aan goede coördinatie en gedetailleerde planning. Werken in silo's is ook een kwestie van communicatie *(zie ook must-have 9: soft skills)*. "Wat ook bijdraagt tot

mislukkingen, is dat je gebruikers naar de vergaderingen over de nieuwe toepassing stuurt, die hun werk zo vanzelfsprekend vinden, dat ze het niet kunnen uitleggen. En daar tegenover staan dan informatici die alleen interesse hebben voor tools en technologie", stelt Vandepitte met een kwinkslag.

Bij communicatie hoort overigens ook documentatie. Vandepitte: "Wanneer een organisatie een nieuwe softwaretoepassing nodig heeft, dan is de eerste stap: de bestaande situatie documenteren. Soms probeert men deze stap over te slaan. Of probeert men deze stap uit te voeren, maar is de kennis verdwenen. Niemand in de organisatie weet nog wat de software doet, op welke manier de toepassing de bedrijfsprocessen ondersteunt. Zo'n project mislukt beslist."

FAIL FACTOR 7

VERWACHT EEN WONDERMIDDEL

Te vaak ontstaat enthousiasme in een softwareproject uit de valse overtuiging dat een spreekwoordelijke *silver bullet* een bepaald probleem zal oplossen. Maar goede oplossingen zijn zelden eenvoudig. Ze zijn een mix van methodologie, strategie en teamondersteuning, niet het resultaat van één enkele actie, technologie of idee.

"Vaak denken we dat software kan worden aangepast tot een niveau dat aan alle behoeften voldoet", aldus Bhavna Juneja, global CEO bij Infinity, een bedrijf dat zich specialiseert in IT-diensten rond biotech en life sciences, in een blog. "Dat is een misvatting. Realistisch zijn is belangrijk. Definieer de vereisten met betrekking tot de mogelijkheden van de software."

FAIL FACTOR 8

KIES VOOR EEN ONDUIDELIJKE ROLDEFINITIE

Ongedefinieerde rollen zorgen vaak voor wrijving in projectteams. Probeer vanaf het begin een framework te gebruiken om duidelijk te definiëren wie waarvoor bevoegd is. "Voor vastgelopen projecten kan het herijken van wie *driver, approver, contributor & informed* is binnen het project als een harde reset fungeren, wat hernieuwde samenwerking en autonomie inspireert", suggereert Leore Avidar van Lob.com Inc, dat zich specialiseert in direct mail, in Forbes.

FAIL FACTOR 9

SCHUIF DE SOFT SKILLS OPZIJ

Softwareprojecten draaien om techniek, maar evenzeer om andere skills. Daarom is het aangewezen dat je die skills evenzeer vooropstelt. "Ik heb veel softwareprojecten in verschillende categorieën en in verschillende soorten en maten organisaties in de problemen zien komen omdat ze super gefocust waren op het technische werk, maar niet genoeg energie besteedden aan training, coaching, teambuilding en *soft skills*", oppert Amith Nagarajan van softwarebedrijf rasa.io.

Te veel focus op technologische kwesties is overigens voor geen enkel softwareproject een goed idee. "Sommige softwaretoepassingen doen aan dataprocessing. Sommige softwaretoepassingen doen aan business data analytics, denk aan business intelligence of data science. Maar ook die lopen fout", oppert Vandepitte. "Vaak is er te veel aandacht voor de technische uitdagingen, zoals data warehouses, werken met SAS, R of Python. Maar ze verliezen de oorspronkelijke vraag van de business uit het oog."

FAIL FACTOR 10

LAAT DE DISCIPLINE COMPLEET LOS

Wat voor een bouwproject geldt, telt ook voor software: discipline is onvermijdelijk om een project te laten lukken. Dat betekent ook het overzicht bewaren en niet meer projectleden erbij betrekken dan nodig. Bepaal (en beperk) wie er vanaf dag één bij betrokken is, of je nu in-house bouwt of niet. Soms is een groot projectteam onvermijdelijk, zoals voor grotere technologiebedrijven met complexe processen en communicatiekanalen. Maar in kleinere omgevingen is een dergelijke complexe projectstructuur een groot nadeel.

Een perfect scenario om de teugels te laten varen? "Neem eerst zes maanden de tijd om te beslissen of het project doorgaat of niet, en zeg dan dat alles absoluut klaar moet zijn voor het begin van het nieuwe boekjaar. Begin er gewoon mee, zonder te wachten op de goedkeuring van het budget door de directie", besluit Vandepitte met een knipoog.

WEBINAR OVER FOUTEN BIJ SOFTWAREPROJECTEN

Kom meer te weten over fouten bij softwareprojecten en over het ontdekken van de juiste vereisten voor het juiste probleem in het webinar over *500k gespendeerd aan een gefaald softwareproject?* van Pieter Hens, digital product manager, trainer en coach bij Gokotta op 5 oktober 2022 om 13 uur.

Over onder meer onze traditionele manier van softwareanalyse (en waarom die niet meer werkt), over vereisten die je moet ontdekken (wat je beter niet alleen doet) én over het duidelijke verschil tussen een koelkast en een diepvriezer.

» Inschrijven kan **hier**!

HOE DECENTRAAL ZIJN DAO'S ECHT?

Gedecentraliseerde autonome organisaties (DAO's) zijn in het leven geroepen om een nieuwe, gedemocratiseerde managementstructuur te bieden aan bedrijven, projecten en gemeenschappen. Toch blijkt dat ze centraler opereren dan je zou denken.

Nog even samenvatten: een DAO of *decentralized autonomous organization* is een organisatie die wordt 'gereguleerd' door regels in de vorm van computeralgoritmes, de zogeheten 'smart contracts'. Zo'n organisatie gebruikt de blockchaintechnologie als veilig digitaal grootboek ('smart ledger') om (financiële) transacties over het internet op te volgen. De beveiliging komt dan vooral door het principe van timestamping en het gebruik van een gedistribueerde database. Daarom praat men soms ook over *distributed autonomous organization.*

GEDECENTRALISEERD?

Vaak heeft men het over Web3, als een soort van nieuwe golf in de wereld van technologie en internet. De klemtoon komt dan zogenaamd (terug) op het decentrale karakter te liggen. Gedecentraliseerde autonome organisaties (DAO's) zijn namelijk in het leven groepen om een nieuwe, gedemocratiseerde managementstructuur te bieden aan bedrijven, projecten en gemeenschappen. Elk lid kan stemmen over organisatorische beslissingen, simpelweg door zich in te kopen in het project.

In zijn recente ***State of Web3 Report*** heeft blockchain-dataplatform Chainalysis deze DAO's geanalyseerd. Hieruit blijkt dat **de eigendom van web3 alsnog verrassend geconcentreerd is**. Dat is op zich best opmerkelijk, want deze mate van concentratie is in strijd met de grondbeginselen van web3, waar decentralisatie juist vooropstaat.

DE ONE PERCENT

De belangrijkste bevinding uit het rapport is dat gemiddeld minder dan 1 procent van alle houders 90 procent van de stemrechten bij DAO's heeft. De impact op het DAO-bestuur is enorm: als slechts een klein deel van deze 1 procent samenwerkt, kunnen zij theoretisch gezien de resterende 99 procent overstemmen bij elke beslissing.

Een gebruiker moet tussen 0,1 procent en 1 procent van de uitstaande tokenvoorraad bezitten om een voorstel te doen, en moet tussen 1 procent en 4 procent bezitten om het aan te nemen. "Als we deze onder- en bovengrenzen hanteren, kunnen we stellen dat tussen 1 op 1.000 en 1 op 10.000 DAO-houders genoeg tokens hebben om een voorstel te doen", klinkt het bij Chainalysis.

VOORDELEN VAN DAO'S

De voordelen van een dergelijke *decentralized autonomous organisation* werden al vaak besproken (ook in SAI Update overigens) wanneer het over blockchain gaat: met het digitaal grootboek heb je een technische oplossing om akkoorden of transacties te bekrachtigen, zonder dat hiervoor een derde partij, een notaris bijvoorbeeld, moet worden ingeschakeld of dat er officiële documenten in veelvoud moeten worden opgeslagen. Zo spaar je geld uit en maak je transacties ook eenvoudiger. Hierdoor kun je op termijn ook sneller schakelen.

LAAG 8: OP ZOEK NAAR DE INTENTIE IN SECURITY

Om legitiem dataverkeer te kunnen onderscheiden van fraude, helpt het om de intentie van de eindgebruiker te begrijpen, zoals die blijkt uit zijn gedrag. "Sommigen omschrijven die eindgebruikerslaag boven layer 7 van het OSI-model als layer 8. En zoals het liedje in Sesamstraat luidt: *eight is great.*"

Jarenlang berustte beveiligingsmonitoring op het verzamelen van gegevens van laag 4 van het OSI-model. Maar omdat de gegevens van laag 4 betrekking hebben op de transportlaag, zijn ze niet de meest informatieve of interessante. Gedurende een bepaalde periode waren het de gegevens waar beveiligingsteams op een betrouwbare manier toegang tot konden krijgen en die ze efficiënt konden bevragen. "Toen de technologie verbeterde, kregen beveiligingsteams toegang tot een veel rijkere gegevensverzameling: gegevens van laag 7. Proxy-logboeken, DNS-logboeken, packet capture (PCAP) en andere gegevensbronnen van laag 7 kwamen beschikbaar. Dit was een doorbraak voor beveiligingsteams", oppert Joshua Goldfarb, fraud solutions architect bij F5.

Met gegevens over laag 7 kunnen we de zogenaamde *application layer* ondervragen. In het bijzonder met betrekking tot digitale kanalen, zoals internet en mobiele telefoons, geven gegevens over laag 7 inzicht in wat er precies gebeurt binnen de applicatiesessie van de eindgebruiker.

"Dit geeft ons essentiële context rond de activiteit van de eindgebruiker. Helaas geven data van laag 7 ons geen inzicht in het *hoe* achter wat er gebeurt. Denk aan vragen zoals hoe de eindgebruiker zich gedraagt. Of: wat is de intentie? En vooral: is dit een legitieme eindgebruikersactiviteit? Zulke vragen kunnen alleen beantwoord worden door verder te kijken dan laag 7."

Om de intentie te begrijpen – het *hoe* achter het *wat* – moeten we het gedrag van de eindgebruiker tijdens de sessie nauwkeurig onderzoeken, oppert Joshua Goldfarb. Dit aanvullende inzicht in gedrag is namelijk cruciaal voor het vermogen van een onderneming om legitiem verkeer te onderscheiden van fraude. Met andere woorden: het verschil tussen het legitieme gebruik van een toepassing en misbruik van die toepassing (fraude dus) is de intentie van de eindgebruiker die verantwoordelijk is voor de activiteit. “Als we het begrip fraude op deze manier bekijken, is het gemakkelijk te zien dat inzicht in wat de eindgebruiker binnen de applicatiesessie doet, niet voldoende is. We moeten ook inzicht hebben in de manier waarop hij dat doet, het *hoe* dus.”

EIGHT IS GREAT

Het basisidee is: er zijn gedragsverschillen tussen legitieme gebruikers en fraudeurs. “Sommige mensen noemen deze eindgebruikerslaag boven layer 7 van het OSI-model layer 8.” Het idee van layer 8 is in securitytermen overigens al langer aangehaald. Zo heeft Bruce Schneier, een bekende cryptospecialist, het al langer over layer 8 in het OSI-model als de laag van het individu. “Zoals het liedje in Sesamstraat luidt, *eight is great*”, zegt Goldfarb met een knipoog. Zijn suggestie is om te kijken naar een aantal manieren waarop gegevens van laag 8 kunnen helpen om fraude beter op te sporen.

De fraud solutions architect wijst op bepaalde verdachte activiteiten of handelingen (zie kader), zoals muis- of toetsenbordbewegingen. Of het gebruik van bepaalde keys. “Geen van deze gedragingen op zich kan ons met 100 procent zekerheid vertellen of een bepaalde sessie legitiem of frauduleus is. Maar ze kunnen ons wel een waardevol inzicht geven in het *hoe* achter het *wat*”, benadrukt hij. “En dat kan ons dan weer helpen om veel nauwkeuriger te beoordelen wat fraude is. Inzicht in het gedrag van eindgebruikers – gegevens van laag 8 dus – stelt ons in staat om onze opsporingspercentages te verhogen en tegelijkertijd onze fout-positieve percentages te verlagen.”

DEZE GEDRAGINGEN KUNNEN WIJZEN OP FRAUDULEUS GEBRUIK

Fraudeurs hebben vaak een specifiek gedrag. Ze passen vaak spoofing en andere trucs toe om zich voor te doen als legitieme gebruikers. Ook de volgende handelingen kunnen verdacht zijn.

1 **Geoptimaliseerde muisbewegingen.** Legitieme gebruikers hebben de neiging om zeer willekeurige muisbewegingen te maken bij de interactie met een applicatie. “Dat is ook logisch, want legitieme gebruikers werken niet professioneel met de applicatie en hebben vaak geen behoefte of prikkel om hun muisbewegingen super te optimaliseren”, aldus Joshua Goldfarb. Fraudeurs daarentegen, die misschien proberen frauduleus toegang te krijgen tot tientallen, honderden of duizenden accounts, hebben alle redenen om hun muisbewegingen te optimaliseren om tijd te besparen. Ze doen namelijk talloze keren hetzelfde.”

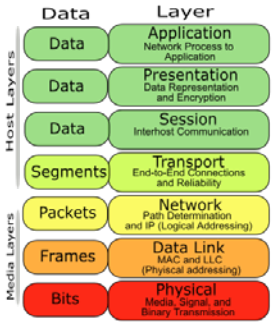
2 **Signature device.** Fraudeurs hebben meestal een of enkele favoriete apparaten die ze precies hebben geconfigureerd zoals ze willen. “Zij zullen diezelfde apparaten vaak gebruiken om in te loggen op een relatief groot aantal accounts op dezelfde applicatie. Daarom kunnen we, door te investeren in nauwkeurige en betrouwbare device-identificatie en aanmeldingen per apparaat te traceren, die kennis gebruiken om te begrijpen wanneer we mogelijk te maken hebben met een frauduleuze sessie.”

3 **Minder evidente keys.** “Als je een legitieme gebruiker bent, is de kans groot dat je een standaard set van letters, cijfers en speciale tekens gebruikt wanneer je met een applicatie communiceert. Het is vrij onwaarschijnlijk dat je functietoetsen, sneltoetsen of andere ongebruikelijke combinaties zou gebruiken. Fraudeurs die tijd willen besparen, doen echter vaak precies dat.”

4 **Copy-paste.** “De meeste legitieme gebruikers knippen en plakken niet vaak hun gebruikersnaam en wachtwoord of voor- en achternaam uit een tekstbestand”, stelt Goldfarb. “Fraudeurs doen dit vrij vaak, vooral als het gaat om een zogenaamde *account takeover* of ATO.”

OSI MODEL

Het OSI-model met zijn zeven lagen.



QUANTUM ADVANTAGE OF QUANTUM SUPREMACY?

QUANTUM COMPUTING, HET EINDE VAN ONZE DIGITALE PRIVACY?

Quantum computing is een onderzoeksveld waarin de laatste jaren grote vooruitgang geboekt werd. Niet alleen privébedrijven investeren massaal in onderzoek naar quantum computing, ook nationale overheden hebben steeds meer belangstelling in deze technologie. Quantum computing kan zaken mogelijk maken die met de actuele technologie minder evident zijn. Maar is het ook een gevaar voor onze privacy?

Het belang van quantum computing is groot. Zo tekende de Amerikaans president Joe Biden recent nog een besluit dat van het behoud van de superioriteit in dit veld en de bescherming tegen de risico's van quantum computing een nationale prioriteit maakte.

Quantum mechanica is de theorie dat materie bestaat uit een verzameling 'quantum states', ofwel mogelijke configuraties van eigenschappen. Deze states interfereren met elkaar zoals golven in een wateroppervlak, waardoor we alleen de som van al deze states kunnen observeren. Het observeren van

alle quantum states afzonderlijk is onmogelijk.

HET ONTSTAAN

Het idee om te rekenen met quantum states is ontstaan uit de intentie om ze te simuleren. Natuurkundigen wilden quantum-mechanische processen kunnen simuleren, maar botsten al snel op limieten. Stel je een systeem voor met 40 plaatsen waar een elektron aanwezig kan zijn of niet, en we willen dit simuleren. Het gaat al snel om 240 mogelijke configuraties of states. Als de computer al deze mogelijke states in het geheugen wil houden, is er maar liefst 130 GB geheugen nodig. Voor 241 is dit al 260 GB. **Voor een systeem van enkele honderden elektronen is het nodige aantal bits aan geheugen groter dan het aantal partikels in het universum**. Enkele honderden plaatsen met mogelijkheid op een elektron, geeft al meer mogelijke configuraties dan er deeltjes zijn in het universum.

Uit deze observatie vloeide het idee om van deze moeilijkheid een sterkte te maken. Als we hardware kunnen ontwikkelen die quantumeffecten als fundamentele operaties heeft, zouden we daarmee dan wel de fysische processen die voortvloeien uit diezelfde effecten kunnen simuleren?

QUANTUMCOMPUTERS

De onderzoekswereld is dan ook op zoek gegaan naar modellen om met quantum-fysische processen te kunnen rekenen. Dit heeft geleid tot twee grote modellen, met elk hun eigen hardware. Het idee achter het eerste model, *quantum circuits of gate*-based computation, is gelijkaardig aan dat van onze bestaande, klassieke computers. Het beoogt het ontwerpen van een 'quantum turing machine'. Dit gebeurt door het aaneenschakelen van quantum gates, naar circuit-analogie van de logische poorten in een klassieke machine. Quantum circuit-systemen gebruiken de welgekende qubits.

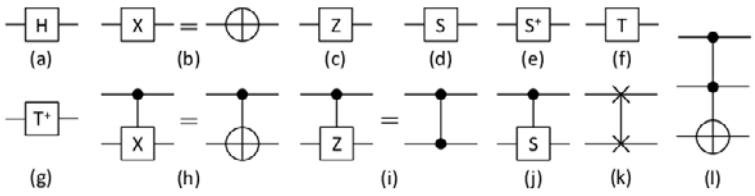
Een tweede methode is adiabatische quantum computing. Hierbij wordt het probleem eerst op een eenvoudige wijze gesimuleerd en een optimale oplossing bepaald. Vervolgens wordt deze oplossing met behulp van een quantum effect, quantum tunneling genaamd, op het originele, complexere probleem geschaald. Ze zijn gemakkelijker te maken dan gate-based quantumcomputers.

Van beide types zijn er al verschillende, werkende producten op de markt. Zo heeft de firma D-wave adiabatische quantumcomputers en zijn ze volop gate-based systemen aan het ontwikkelen. IBM heeft dan weer het quantum circuit met het grootste aantal qubits, 127.

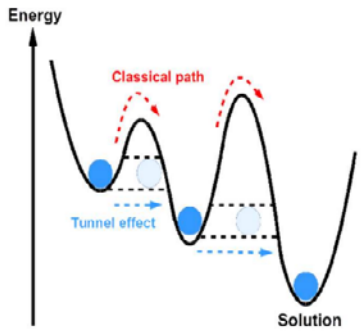
Zij bieden ook cloudapplicaties waarmee je software voor hun quantumcomputers kunt schrijven en laten runnen.

MOEILIJKE PROBLEMEN

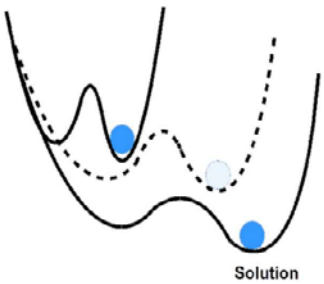
Het probleem met elektronen is vooral een gedachtenoefening rond de enorme kracht van quantumcomputers. Interessanter wordt het wanneer we fysische interacties gaan simuleren die we dan kunnen toepassen in de echte wereld. Levende organismen bouwen hun lichaam voornamelijk uit verschillende proteïnen. Ze hebben een werking in het lichaam en vervullen elk een specifieke functie. DNA is de blauwdruk voor al deze verschillende eiwitten. Op basis van de informatie in het DNA worden proteïnen aangemaakt uit een reeks van bouwstenen: aminozuren. Deze bouwstenen plooien



Quantum gates: (a) Hadamard gate (b) Pauli-X gate (c) Pauli-Z gate (d) S (phase) gate (e) inverse S gate (f) T (π/8) gate (g) inverse T gate (h) CNOT gate (i) CZ gate (j) CPhase gate (k) SWAP gate (l) Toffoli gate



Quantum tunneling



Adiabatic evolution

door elkaar onder invloed van de natuurkundige krachten die ze op elkaar uitoefenen en vormen zo een werkzame proteïne.

Soms ontstaan er echter fouten en vouwen de aminozuren niet op de juiste manier samen, en werken ze hierdoor soms niet of minder. Zogenaamde *folding errors* liggen aan de basis van een heleboel ziekten, zoals bepaalde kankers, parkinson en alzheimer. Door het vouwen van de aminozuren onder allerlei omgevingsfactoren te simuleren, kan achterhaald worden welke omstandigheden de aanleiding zijn tot fouten. **Momenteel gebeuren deze simulaties met behulp van supercomputers of distributed supercomputers. Deze aanpak heeft zijn limieten.** Vanaf enkele honderden aminozuren wordt het aantal mogelijkheden opnieuw ontzaglijk groot, net als in bovenstaande denkoefening met elektronen. Dankzij nieuwe algoritmen voor quantumcomputers, en een voldoende sterke quantumcomputer om ze op uit te voeren, zouden toch oplossingen voor deze nu nog onoplosbare vouwpuzzels gevonden kunnen worden.

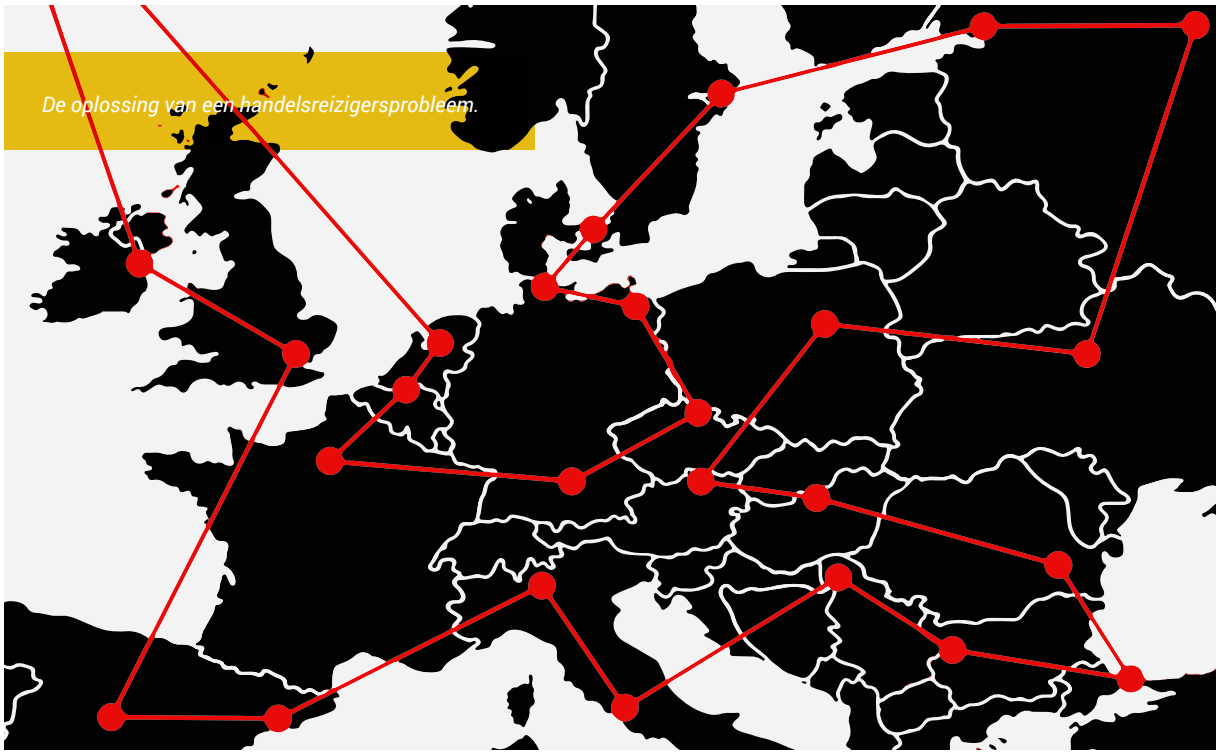
DE OPTIMALE ROUTE

Ook in de logistiek, een prioriteit voor veel bedrijven, zijn er moeilijke problemen die we niet kunnen oplossen met onze huidige supercomputers, maar wel met een quantumcomputer. Het handelsreizigersprobleem, waarbij een handelaar of leverancier in een minimale afgelegde weg een aantal bestemmingen moet bereiken, is er één met een enorm aantal mogelijkheden. Telkens je een bestemming aan het probleem toevoegt, vergroot het aantal mogelijkheden exponentieel.

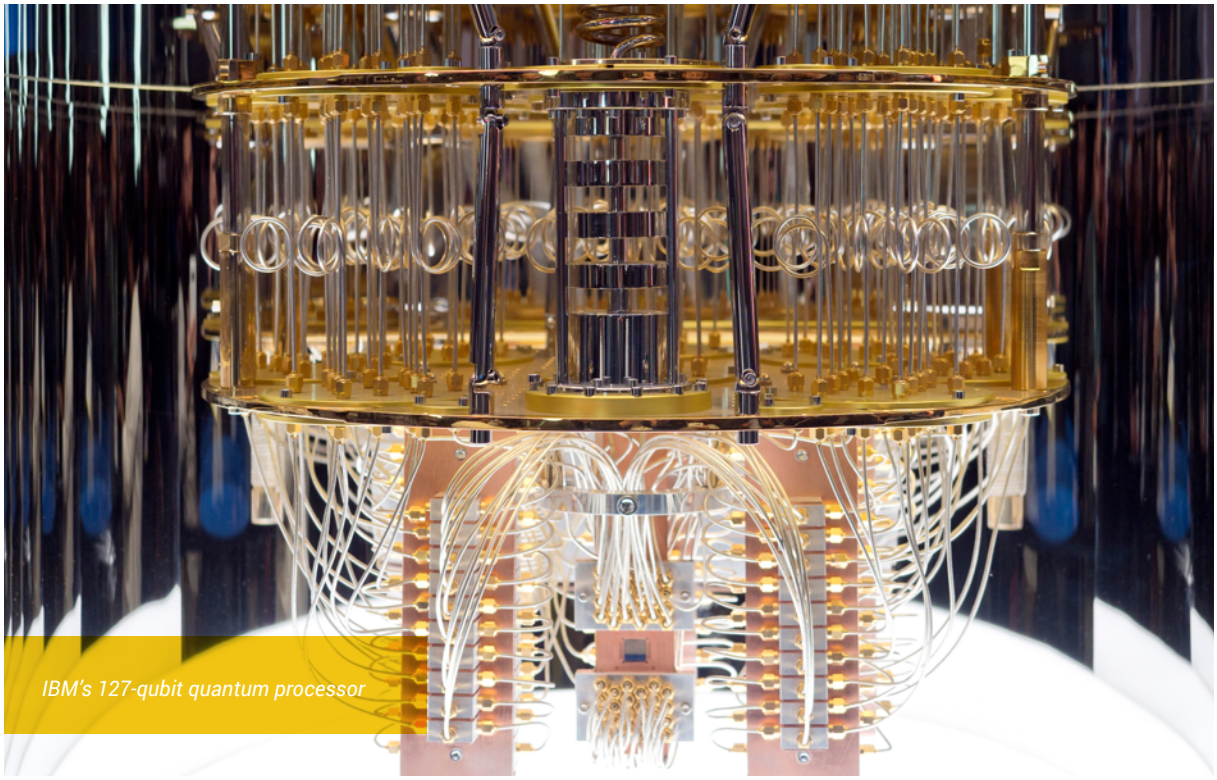
Er is wel een enorm potentieel. **Onze huidige algoritmes om dit handelsreizigersprobleem op te lossen, voldoen niet om de beste oplossing te vinden. Er zijn immers te veel mogelijkheden om ze allemaal af te toetsen en zo de kortste route te bepalen. Met een quantumcomputer zou dit wel kunnen**. De optimale weg is de meest economische én de meest ecologische. Deze weg altijd kennen, zou een enorme besparing betekenen voor bijvoorbeeld pakketjesbezorgers. Zij vliegen en rijden de wereld rond met vliegtuigen en wagens, die pakketjes ophalen en afleveren. De optimale route vinden om al deze handelingen zo efficiënt mogelijk uit te voeren, is voor hen van onschatbare waarde.

EINDE VAN ONZE PRIVACY?

Een specifieke discussie is encryptie, die alomtegenwoordig is in ons computergebruik. Het is een veelgebruikt principe bij gegevensbescherming en authenticatie. Een doorbraak in quantum computing zou weleens het einde kunnen betekenen van heel wat encryptiealgoritmen. De meest gebruikte vorm van encryptie is deze met een private- en publieke sleutel. Hierbij gebeurt de encryptie met de publieke sleutel die door iedereen gekend is, en de decryptie met behulp van de private sleutel. Bijvoorbeeld het bekende encryptiealgoritme RSA maakt gebruik van deze methode.



De oplossing van een handelsreizigersprobleem.



IBM's 127-qubit quantum processor

Dit principe is alleen mogelijk dankzij hashes, dit zijn niet-omkeerbare operaties die gebruikt worden bij het versleutelen. Als de operatie omkeerbaar zou zijn, dan zou het mogelijk zijn om het versleutelde berichtje weer leesbaar te maken met behulp van de publieke sleutel, die voor iedereen bekend is. Je kunt dan immers simpelweg de omgekeerde bewerking doen. Dankzij de niet-omkeerbaarheid van de hashes is dit echter alleen mogelijk met de private sleutel, die alleen de rechtmatige ontvanger van het berichtje in bezit heeft. **Met een voldoende krachtige quantumcomputer zou het echter gemakkelijk zijn om deze hashes toch om te keren. Daarom wordt een nationale prioriteit gemaakt van de ontwikkeling van quantumcomputers**. De eerste die er immers een voldoende krachtige kan ontwikkelen, kan alle op deze wijze versleutelde gegevens openen en lezen. Dit is een enorm strategisch voordeel, dat grootmachten liefst sneller dan hun concurrenten in handen hebben.

QUANTUM SUPREMACY

De sterkste quantumcomputer op dit moment heeft 127 qubits. Dit wil zeggen 127 bits waarop quantumberekeningen kunnen worden uitgevoerd. Dit is nog niet voldoende om *quantum supremacy* te bereiken, het moment waarop een quantumcomputer problemen kan oplossen die voor een gewone supercomputer onoplosbaar zijn.

Het is pas als we dit punt bereiken, dat quantumcomputers doorbraken zullen realiseren die tot nu toe onbereikbaar waren. Tot op heden is er echter alleen sprake van *quantum advantage*. Dit wil zeggen dat, voor bepaalde problemen, een quantumcomputer de oplossing gemakkelijker kan berekenen dan een supercomputer. Er zijn zelfs stemmen die zeggen dat quantum supremacy nooit bereikt kan worden, omdat de foutenmarge van een quantumcomputer steeds toeneemt telkens je qubits toevoegt. Deze foutenmarge wordt gecorrigeerd door een aantal qubits op te geven voor foutencorrectie. Op een bepaald moment zou volgens sceptici de toename in aantal qubits nodig voor de foutencorrectie, groter worden dan het aantal qubits dat je aan het systeem hebt toegevoegd. Toch zijn er steeds meer bemoedigende experimenten die erop lijken te wijzen dat deze doorbraak wel degelijk bereikt zal kunnen worden.

Quantum supremacy is er dus nog niet. Momenteel hoef je je dan ook nog geen zorgen te maken dat men je encryptie zou kraken met behulp van een quantumcomputer. Tot nu toe kan dat immers nog niet beter met een quantumcomputer dan met een gewone, klassieke computer.

Dit is een gastbijdrage voor SAI Update van Stijn Hardy, consultant bij Formica NV. Dit artikel schreef hij in het kader van een afstudeerproject aan het flextraject voor professionele bachelor toegepaste informatica aan de Karel de Grote Hogeschool (KdG).

VOLGENDE EVENTS VOOR SAI

21 SEP 2022
Online – 13.00 – 14.00 uur
DE KLANT CENTRAAL: ENTERPRISE SERVICE MANAGEMENT ALS ENABLER VOOR DIGITALISATIE
Webinar
*Meer info vind je **hier***

29 SEP 2022
Speciaal event
18.00 – 21.00 uur
CYBERWAR AND PSYCHOLOGICAL MALWARE: TALES FROM UKRAINE
BeVenue Conference Centre (BeVenue)
*Meer info vind je **hier***

05 OKT 2022
Speciaal event
08.30 – 18.00 uur
SECURITY LEADERSHIP CONFERENCE
Partner event
Gratis voor SAI-leden
*Meer info vind je **hier***

05 OKT 2022
Online – 13.00 – 14.00 uur
500K GESPENDEERD AAN EEN GEFAALD SOFTWARE PROJECT?
Webinar
*Meer info vind je **hier***

06 OKT 2022
Online
SECURITY EU MITRE ATT&CK COMMUNITY
Partner event
Webinar
*Meer info vind je **hier***

11 OKT 2022
Online – 13.00 – 14.00 uur
GREENFIELD IT: HOE I-FORCE HUN DATA VERWERKINGSTIJD MET 95% VERMINDERDE
Webinar
*Meer info vind je **hier***

19 OKT 2022
Online – 13.00 – 14.00 uur
THE DIGITAL TRANSFORMATION COOKBOOK
Webinar
*Meer info vind je **hier***

26 OKT 2022
Online – 13.00 – 14.00 uur
DEVSECOPS - EEN STAND VAN ZAKEN
Webinar
*Meer info vind je **hier***

10 NOV 2022
Online – 13.00 – 14.00 uur
GOVERNANCE CHALLENGES DURING DIGITAL BUSINESS TRANSFORMATIONS
Webinar
*Meer info vind je **hier***

25 NOV 2022
Online – 13.00 – 14.00 uur
DE TOEKOMST VAN ONZE ARBEIDSMARKT EN DE ROL VAN DIGITALE COMPETENTIES HIERIN
Webinar
*Meer info vind je **hier***

12 DEC 2022
Avondconferentie
19.00 – 20.30 uur
IT-TRENDS THAT WILL BECOME MAINSTREAM IN 2023
Van Der Valk Brussels Airport Hotel
*Meer info vind je **hier***

Voor nieuwe events:
*neem zeker een kijkje op **sai.be***

COLOFON
Werkten mee aan dit nummer: William Visterin (coördinatie), Robin Van den Bogaert, Stef Gyssels, Stijn Hardy en Marc Vael.

De missie van SAI.BE is om actuele en relevante IT kennis te delen op een objectieve en kwalitatieve manier met alle informatici in Vlaanderen en Brussel

Architecture

- Enterprise Architecture
- Data Architecture
- Business Capability Mapping
- BPMN / UML
- Decision Modelling
- IT Governance
- Distributed Systems
- Microservices Architecture

Cloud & Infrastructure

- Smart Cloud Deployment
- CASB
- Kubernetes
- Automation & Orchestration
- Open Service Mesh

Security

- Applied DevSecOps
- Zero Trust Implementation
- Cybersecurity Compliance Certifications
- Trusted Digital Identity Management
- Adaptive Security Awareness
- Intelligent Privacy Governance Automation
- SAST / SCA

Software Development

- Knowledge Graphs
- API management
- Low Code / No Code
- Composable Applications
- Customer Experience (CX)
- Code Quality

Data & AI

- Data Quality Management Tools
- Predictive Analytics Tools
- Data Scraping & Data Tracking
- Advanced Data Visualisation
- Regression-based Forecasting
- Machine Learning
- Data & AI Ethics By Design

Emerging Tech & Topics

- VR / AR / MR / XR
- Intelligent Process Automation
- Federated Learning
- The Autonomous Enterprise
- Sustainable IT
- Blockchain / NFT
- Quantum Computing
- The Future of Work

- ✓ SAI.BE begeleidt duizenden informatici **sinds 1967** doorheen een immer wijzigend IT landschap
- ✓ SAI.BE organiseert jaarlijks **gemiddeld 50 events**, waaronder avondconferenties, workshops, webinars, focus-meetings, speciale events en ook podcasts

SAI.BE publiceert elk kwartaal **het tijdschrift "SAI Update"** voor informatici, IT-experten, en IT beslissings-makers

MEER WETEN OF LID WORDEN?
Ga naar **www.sai.be/pagina/lidmaatschap/**

NEEM CONTACT OP
voorzitter@sai.be