SAI UPDATE

DIGITAAL TIJDSCHRIFT VOOR SAI.BE-LEDEN | JUNI 2025 | SAI

EXCLUSIEF ONDERZOEK BIJ SAI.BE-LEDEN

DE GROTE SOFTWARE DEVELOPMENT UPDATE

UITDAGINGEN, TEAMS, TALEN, METHODOLOGIEËN, TOOLS EN... AI

pag. 21

SAI RESET IT
4 DECEMBER 2025
VOLLEDIG PROGRAMMA BEKEND

En verder:

5 VRAGEN AAN CISO'S | CASE IT-MIGRATIE MEDIAHUIS | SUPPLYCHAINAANVALLEN | SECURITY VOOR ONTWIKKELAARS | LEGACY & AI | CASE DATA BIJ VOETBALCLUB UNION | ENERGIEVERBRUIK BELGISCHE DATACENTERS | SECURITYBUDGETTEN | WIKIPEDIA ONDER DRUK VAN AI-SCRAPERS

WELKE **IT-OUTSOURCER** KIEZEN?
pag. 13

HR EN IT VERSMELTEN
ONDER DRUK VAN AI
pag. 16

E-MAILPROTOCOLLEN
ALS VERDEDIGINGSLINIE
pag. 37

EDITO

ONZEKERHEID, HOOP EN HET BELANG VAN VERTROUWEN IN DE TOEKOMSTIGE DIGITALE WERELD

Ik kreeg onlangs de kans om een keynote bij te wonen van professor Frederik Anseel, decaan van de Australische UNSW Business School, tijdens een bijeenkomst in Heverlee. Hij beschreef op bijzonder treffende wijze – met sprekende voorbeelden en een scherpe analyse – hoe we ons vandaag bevinden op een kruispunt: tussen ongekende technologische mogelijkheden enerzijds, en een groeiend gevoel van onzekerheid en onrust anderzijds, vooral bij medewerkers op de werkvloer.

Zijn woorden bleven hangen. Want inderdaad, we staan als samenleving, als bedrijven, als individuen voor grote keuzes. De opmars van artificiële intelligentie, de dominantie van enkele technologische giganten, de toenemende complexiteit van regelgeving én de eerste signalen van digitale vermoeidheid creëren een gelaagde realiteit – vol belofte, maar ook vol vragen. De digitale revolutie versnelt, maar neemt ons niet altijd mee in het verhaal.

Zijn betoog zette me aan het denken over dat kruispunt. Want ja, er is dat knagende gevoel dat technologie ons soms ontglipt. Dat we niet meer volledig begrijpen wat er onder de motorkap gebeurt. Werkvloeren ondergaan diepe transformaties: functies verdwijnen of veranderen razendsnel. De roep om “meer digitale vaardigheden” klinkt dwingend en soms beklemmend. Tegelijk groeit de onrust over de ethische aspecten van AI, over het verlies van privacy, over de groeiende afhankelijkheid van systemen die steeds minder transparant zijn. Artificiële intelligentie raakt niet alleen bedrijven – ze beïnvloedt ook beleidsvoering, onderwijs, gezondheidszorg, veiligheid en zelfs onze democratische processen. De vraag rijst: zijn we als samenleving voldoende voorbereid?

“Optimism is a moral duty.”
Immanuel Kant (1724-1804)

Toch mogen we ons niet laten verlammen door deze onzekerheid. Integendeel. Net in die schijnbaar instabiele periode groeit er ruimte voor iets fundamenteels: ***hoop***. Hoop op vernieuwing, op samenwerking, op technologie die mensen versterkt in plaats van vervangt. Die hoop vindt haar wortels in creativiteit, in kritische reflectie en in moedige keuzes. En vooral: in **vertrouwen**. Zonder vertrouwen – in elkaar, in het leervermogen van organisaties, in de ethische kaders van technologie – komt geen vooruitgang tot stand. Vertrouwen is geen vanzelfsprekendheid, maar een bewuste investering. Het is de brug tussen wat we vandaag nog niet zeker weten en wat we morgen samen willen bouwen.

En dan is er **optimisme**. Niet als naïeve wensdroom, maar als morele houding. Een keuze om te geloven dat technologie beter, eerlijker en menselijker kan. Vandaag zien we tal van initiatieven ontstaan die inzetten op ethische AI, duurzame IT-infrastructuur en transparantie in algoritmes. Start-ups floreren die maatschappelijke meerwaarde verkiezen boven winstmaximalisatie. Beleidsmakers, onderzoekers en ontwikkelaars durven steeds vaker “trager maar juister” te denken. Het zijn tekenen van een shift – geen massabeweging misschien, maar wel een richting die vertrouwen verdient.

Ook jij en ik – gebruikers van al die technologie – hebben een rol. Door kritische vragen te stellen, digitaal bewust te leven, te blijven leren en actief deel te nemen aan het debat over onze digitale toekomst, maken we die toekomst mee. Vertrouwen is niet blind. Het groeit uit transparantie, wederkerigheid en de keuze om niet weg te kijken.

Ja, de digitale toekomst is onzeker. Maar onzekerheid is geen bedreiging, het is een uitnodiging. Een uitnodiging tot vernieuwing, tot ethiek, tot menselijke keuzes in een steeds technologischere wereld. Hoop groeit uit vertrouwen, en vertrouwen groeit uit optimisme.

Laten we daarom deze zomer benutten om niet alleen bij te tanken, maar ook om te reflecteren. Waar willen we naartoe? Wat bouwen we – en voor wie? Hoe behouden we grip, zonder de snelheid te verliezen? Hoe blijven we mens in een wereld van data? Want uiteindelijk is het niet de technologie die richting geeft, maar **de mensen erachter**.

Marc Vael
Voorzitter raad van bestuur SAI.BE

INHOUD

“

IK ZIE VAAK TWEE SOORTEN SECURITYPROFESSIONALS.

RIK BOBBAERS,
TECHNICAL CISO BIJ ING GLOBAL

OP PAGINA 8

ENERGIEVERBRUIK BELGISCHE DATACENTERS RIJST STILAAN DE PAN UIT

De elektriciteitsvraag van Belgische datacenters staat op het punt te exploderen, met een verwachte groei van twee- tot vijfvoudig binnen dit en tien jaar. Dat voorspelt Boston Consulting Group. De oorzaak moeten we niet ver zoeken: artificiële intelligentie.

Het is vooral de opkomst van AI die een enorme honger naar rekenkracht creëert. Internationale datacenter-operators kijken daarom verder dan de overvolle traditionele Europese hubs en zien België als een veelbelovend alternatief.

Historisch gezien domineerden Frankfurt, Londen, Amsterdam, Parijs en Dublin (de zogenaamde FLAP-D) de datacenterindustrie. Maar door beperkingen in ruimte, netwerkcapaciteit en politieke steun, zoeken ontwikkelaars nu naar nieuwe locaties. België is aantrekkelijk door zijn centrale ligging binnen de FLAP-D-corridor en een relatief minder overbelast energienet. Hoewel ons land geen specifieke beleidsstimulansen heeft, profiteert het van de verzadiging in de topmarkten.

Het rapport van Boston Consulting Group, *The Power of Compute: the effects of data center growth on Belgium's energy system*, voorspelt dat de elektriciteitsvraag van datacenters kan stijgen van zo'n 3 TWh nu naar 7 TWh tot 15,5 TWh tegen 2035. Dit betekent een toename van **hun aandeel in het totale Belgische elektriciteitsverbruik van circa 4 procent naar meer dan 10 procent**. Tegen 2050 kan de vraag zelfs oplopen naar 10,5 TWh tot 34 TWh. Hoewel deze groei kansen biedt voor economische impact en digitale veerkracht, werpt hij, volgens Boston Consulting Group ook uitdagingen op voor het Belgische energiesysteem.

» *Bekijk of herbekijk **hier** de SAI Shorts over infrastructuur en **hier** die over Data & AI.*

Het datacenter van Google in Saint-Ghislain is het grootste van het land.

INFRASTRUCTUURUITGAVEN STIJGEN MET 50%

AI-SCRAPERS JAGEN WIKIPEDIA OP KOSTEN

Wikipedia wordt geconfronteerd met fors stijgende infrastructuurkosten, grotendeels veroorzaakt door AI-bots die automatisch grote hoeveelheden data ophalen.

Sinds januari 2024 zijn de kosten voor het draaiende houden van de encyclopedie met maar liefst 50 procent gestegen. Dat meldde Maciej Artur Nadzikiewicz, bestuurslid bij Wikipedia, in een publieke verklaring. Volgens Nadzikiewicz is inmiddels 65 procent van het duurste dataverkeer van Wikipedia afkomstig van bots, terwijl zij slechts een derde van de totale paginaviews vertegenwoordigen. Vooral AI-scrapers die grote delen van de vrij beschikbare Wikipedia-content downloaden om AI-modellen te trainen, drijven de kosten op.

Hoewel het aantal menselijke bezoekers toeneemt, drukt vooral het automatische verkeer zwaar op de servers van de Wikimedia Foundation. “Onze infrastructuur is

gebouwd om pieken in menselijk verkeer op te vangen, bijvoorbeeld bij grote nieuwsgebeurtenissen”, schrijft Nadzikiewicz. “Maar de schaal en intensiteit van het scraperverkeer is ongekend en vormt een groeiend risico voor de beschikbaarheid van Wikipedia.”

De stichting benadrukt dat de inhoud van Wikipedia gratis is, maar de middelen om die wereldwijd toegankelijk te houden zijn dat allerminst. De groeiende druk vanuit de AI-industrie lijkt het vrije kennismodel van Wikipedia op de proef te stellen.

GEMIDDELD GAAT 19% VAN HET ICT-BUDGET NAAR SECURITY

Dat blijkt uit het jaarlijkse onderzoek van Computable en Enigma Research bij 337 bedrijven in Nederland en België. Vooral de overheid en de zorg besteden hun budget voor cybersecurity meer extern dan intern.

Bij de overheid wordt 60 procent extern besteed, waarbij ze één of meerdere partners onder de arm nemen. Ook zorginstellingen besteden meer extern (56 procent) dan intern (44 procent). ICT-organisaties besteden juist een groter percentage van het securitybudget intern (61 procent). Het kantelpunt voor meer uitbesteden lijkt te liggen bij de overgang van een kleine naar een middelgrote organisatie.

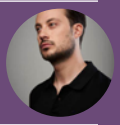
Cybersecurity kan grofweg verdeeld worden in vijf deelgebieden: *identify*, *protect, detect*, *respond* en *recover*. Net als vorig jaar is volgens de ondervraagden protect de post waar gemiddeld het grootste gedeelte van het securitybudget aan uitgegeven wordt (36 procent). Overheidsorganisaties (47 procent) en organisaties in de gezondheids- en welzijnszorg (45 procent) besteden hier zelfs bijna de helft aan.

» *Bekijk of herbekijk **hier** de SAI Shorts over security.*

SAI RESET IT 2025

VOLLEDIG PROGRAMMA BEKEND

SAI.BE presenteert in zijn eindejaarconferentie RESET IT 2025 alle cruciale technologietrends in een boeiende namiddag. Op het programma staan zeven toppresentaties en twee panelgesprekken die alle SAI.BE-thema's zullen behandelen. Deze jaarafsluiter wil je niet missen.

TIJDSTIP	ONDERWERP	SPREKER	
12:30 - 13:00	Aankomst en registratie		
13:00 - 13:05	Verwelkoming	**Guido Thys** Master of Ceremony	
13:05 - 13:15	Introductie	**Marc Vael** Voorzitter SAI.BE	
13:15 - 13:45	Keynote 1: On the future of AI	**Prof. dr. Tijl De Bie** Professor AI UGent	
13:50 - 14:20	Keynote 2: Vision on cybersecurity	**Chris Kubecka** Chief Hacktress Unit6 Technologies	
14:25 - 14:55	Keynote 3: The future of digital trans-formation	**Prof. dr. Stijn Viaene** Head Technology and Operations Management Vlerick Business School	
15:00 - 15:30	Panelgesprek		
15:30 - 16:15	Networking met eten en drank		
16:15 - 16:45	Keynote 4: Application architecture - what's next?	**Davide Cioccia** Founder en Principal Security Consultant DCDOCX	
16:50 - 17:20	Keynote 5: IT regulations and compliance	**Prof. Konstantinos Sergakis** Knowledge and Research Director Guberna	
17:25 - 17:55	Keynote 6: The impact of quantum on infrastructure	**Ramses Gallego** Chief Technologist DXC Technology	
18:00 - 18:30	Panelgesprek		
18:35 - 18:45	SAI Personality Award 2025	**Special guest...**	
18:45 - 19:35	Keynote 7: Technovision 2026 en het Kuramoto Model	**Ron Tolido** CTO Capgemini	
19:35 - 19:50	Outro	**Marc Vael** President SAI	
19:50 - 20:00	Afsluiter	**Guido Thys** Master of Cermony	
20:00 - 21:15	Receptie		

LOCATIE
SQUARE Brussels, Mont des Arts,
1000 Brussels, Belgium

DATUM
4 december 2025
12:30 - 21:00

REGISTREREN

- Toegankelijk voor SAI.BE-leden en niet-leden
- Je krijgt **een exclusief SAI.BE-geschenk**
- Early bird (prijs tot oktober 2025):
  35 euro (incl. btw)
- Late ticket: 45 euro (incl. btw)
- Betalingen worden verwerkt via **Stripe.** Betalen kan met krediet-kaart of Bancontact. Na de betaling krijg je een factuur via e-mail.
- Opgelet: controleer goed je e-mailadres op de betalings-pagina!
- Dit evenement kan worden gebruikt voor het vervullen van interne opleidingsdoelen van jouw medewerkers.
- Wil je eerst een factuur ontvan-gen en dan betalen of meerdere werknemers tegelijk inschrijven? **Contacteer ons**.

*Meer info over de sprekers en het inhoudelijke programma, vind je **hier**.*

*Registreren voor RESET IT 2025 kan via **deze link**.*

Het panel van CISO's op Cybersec Europe, met in het midden (van links naar rechts): Tom Gilis (CISO UCB), Iwona Muchin (CISO & DPO Ageas) en Claudio Bolla (CISO INEOS).

UITDAGINGEN, INVESTERINGEN EN HET TEKORT AAN TALENT: 5 VRAGEN AAN CISO'S

DIT HOUDT SECURITY OFFICERS WAKKER

Tijdens het Secure Bites-event op Cybersec Europe werden een vijftigtal CISO's (Chief Information Security Officers) uitgenodigd voor een interactieve sessie. Zij gaven anoniem hun stem over een aantal stellingen. Het resultaat: een staalkaart van hoe CISO's denken.

1 WELKE OPKOMENDE TECHNOLOGIE ZAL DE GROOTSTE IMPACT HEBBEN OP HET DIGITALE DREIGINGSLANDSCHAP VOOR ORGANISATIES IN DE KOMENDE VIJF JAAR?

Generative Artificial Intelligence (Gen AI)	52%
Quantum Computing	33%
Low/no-code softwareontwikkeling	9%
Geavanceerde robotica (inclusief drones)	3%
Andere	3%

Gen AI is ook voor CISO's dé technologie om rekening mee te houden. Het CISO-panel was, zeker voor de lange termijn, gematigd positief over de voordelen van AI. Al zijn ze zich ook bewust van de uitdagingen. "Cybercriminelen zijn niet gebonden aan regels en regelgeving. Maar de verdedigers wel", zegt **Jan Paredis**, CISO van VUB.

2 WAT IS VANDAAG DE GROOTSTE UITDAGING VOOR JOUW ORGANISATIE BIJ HET AANPASSEN AAN OPKOMENDE TECHNOLOGIEEN?

Het snelle tempo van technologische veranderingen	29%
Gebrek aan gekwalificeerd personeel	21%
Complexe integratie met bestaande systemen	15%
Gebrek aan draagvlak bij het management	15%
Regelgeving en compliance	12%
Weerstand tegen verandering	6%
Hoge implementatiekosten	2%

De snelle veranderingen zien CISO's als de grootste uitdaging. **Dolores Seoane** (Director Innovation & Information Technology bij European Economic & Social Committee) ziet bestuurscycli vaak achterlopen op technologische veranderingen. "Het is moeilijk om je aan te passen, maar we zijn aan het verbeteren. Cyberveiligheid staat ook bovenaan de EU-agenda."

Ook het gebrek aan goede securityprofessionals speelt een rol. "Ik zie vaak twee soorten securityprofessionals", stelt **Rik Bobbaers**, technical CISO bij ING Global. "Je hebt de profielen die echt in de materie geïnteresseerd zijn. Maar je hebt ook zij die naar de sector trekken omdat ze daar goed geld kunnen verdienen. De uitdaging is om het verschil tussen deze twee types te onderscheiden."

Het panel tijdens het Secure Bites-event, met links Jan Paredis (VUB) en Rik Bobbaers (ING).

3 WELK DOMEIN BINNEN CYBERSECURITY VEREIST DE GROOTSTE INVESTERINGEN?

Security Architecture	49%
Incident- en crisisbeheer	22%
Cybersecuritytraining en bewustmaking	14%
Securityautomatisatie	11%
Cyber threat intelligence	5%

De belangrijkste investering om ervoor te zorgen dat de organisatie haar producten en diensten kan beschermen in overeenstemming met internationale normen, is architectuur. Toch lopen de meningen uiteen. “Zelf zou ik opteren voor securityautomatisatie, al is het maar om het personeelstekort en de snelheid in technologie te kunnen beantwoorden”, stelt Jan Paredis van VUB.

4 WAT BESCHOUW JE VANDAAG ALS DE GROOTSTE KWETSBAARHEID IN JE TOELEVERINGSKETEN?

Een geslaagde grote cyberaanval op een kritieke derde partij	41%
Overmatige toegang van derden tot onze systemen	29%
Gebrek aan zicht op de activiteiten van derden	21%
Digitale kwetsbaarheden bij derde partijen	6%
Onveilige gegevensverwerking bij derde partijen	3%

Het gaat hierbij om de grootste supply chain-kwetsbaarheid die de cyberweerbaarheid van jouw organisatie kan aantasten. De remedie hiertegen is volgens de CISO’s vooral een regelmatige audit van de leveranciers. “Al hangt dit af van je type leverancier. Bij een kleinere partij kun je een audit vragen, maar bij grotere spelers is dat moeilijker. Bij giganten keer je wat dat betreft zeker van een kale reis terug”, zegt Rik Bobbaers van ING Global. “Toch raad ik aan om bij gelijk welke leverancier hierover zo open mogelijk te converseren.”

5 WAT IS VANDAAG DE GROOTSTE UITDAGING BIJ HET AANTREKKEN EN BEHOUDEN VAN CYBER-TALENT?

Competitieve verloning en voordelen	32%
Jobtevredenheid	21%
Beschikbaarheid van gekwalificeerde kandidaten	18%
Waardering en erkenning voor geleverd werk	15%
Work-life balance	12%
Kansen voor professionele ontwikkeling en doorgroei	3%

Salaris blijkt een belangrijke factor te zijn bij het aantrekken van talent. Al heeft elke organisatie daarbij haar eigen uitdagingen. Publieke organisaties hebben het vaak moeilijker om mee te concurreren qua salaris. Bij andere organisaties spelen dan weer andere elementen. “Als je bij een bank aan de slag gaat, heb je sowieso te maken met flink wat regulering en niet iedereen kan zich daarin vinden”, zegt Rik Bobbaers.

CISO’s gaven in hun *war for talent* aan dat het verbeteren van de work-life balance de belangrijkste strategie is om talent aan te trekken. Al verschilt veel van functie tot functie. Bobbaers: “Ben je bijvoorbeeld een *incident responder,* dan kan ik me voorstellen dat dat voor je work-life balance een grotere uitdaging kan zijn in vergelijking met een resem andere functies in cybersecurity.”

» *Dit artikel verschijnt naar aanleiding van het evenement Secure Bites VIP CISO Luncheon op Cybersec Europe. Dit event werd georganiseerd in samenwerking met SAI vzw, European Cyber Security Organisation (ECSO), ISACA Belgium Chapter en het CCB.*

Brad Pitt in de rol van teamdirecteur Billy Beane in Moneyball, een Hollywoodklassieker inzake de kracht van data-analyse.

MONEYBALL OP ZIJN BELGISCH

HOE UNION DE VOETBALWERELD HACKTE MET LONDENSE ALGORITMES

Zeven jaar geleden speelde Union Saint-Gilloise nog in de Belgische tweede klasse. Afgelopen seizoen werd de Brusselse voetbalclub kampioen van België. Het geheim achter deze opmerkelijke transformatie? Een geavanceerd data-analyseplatform.

In de Hollywoodfilm *Moneyball* gooit honkbal-teamdirecteur Billy Beane (gespeeld door Brad Pitt) hoge ogen door voor Oakland Athletics – met ondergewaardeerde spelers en slimme data-analyse – een topseizoen neer te zetten. Het bekende softwarebedrijf SAS Institute, gespecialiseerd in data analytics, nodigde klanten en journalisten indertijd uit voor de première van de film in België.

242 DATATOPPERS

Intussen heeft ook het Belgische voetbal zijn eigen Moneyball. De Brusselse traditieclub Union Saint-Gilloise illustreert perfect hoe datagedreven besluitvorming het traditionele sportmanagement kan overtreffen. In 2018 namen de Britse investeerders Tony Bloom en Alex Muzio de club over. Ze deden dat niet zomaar. Ze waren gewapend met de expertise van Starlizard, een **databedrijf met 242 hoogopgeleide analisten, statistici en onderzoekers**. Hier werken enkele van de knapste koppen van Engeland, die een halfjaarlijkse bonus van meer dan 500.000 euro kunnen opstrijken.

Bloom is ook de eigenaar van Brighton & Hove Albion. De club werd afgelopen seizoen achtste in de Engelse Premier League, 's werelds grootste nationale voetbalcompetitie. Brighton viel vooral op door een neus voor goedkoop talent dat het later voor veel geld doorverkocht.

'BESTE DATABEDRIJF IN VOETBAL'

Starlizard, het moederbedrijf achter Unions dataoperaties, ontwikkelde oorspronkelijk algoritmes voor de gokmarkt. Het team analyseert **wekelijks miljoenen datapunten**. Het gaat daar maniakaal ver in – van blessurepatronen en teamsfeer tot veldcondities en supportersaantallen – en dat allemaal om nauwkeurige voorspellingen te maken.

Die schat aan kennis gebruiken ze om elk weekend voor miljoenen euro's aan weddenschappen in te dienen, het merendeel daarvan in het gokgekke Azië. Volgens Business Insider genereert het bedrijf hiermee jaarlijks 20 tot 100 miljoen euro winst.

Deze expertise wordt nu toegepast op voetbalrekrutering via Jamestown Analytics, de voetbaltak van de onderneming Starlizard. *Nobody does data better* is de **centrale slogan op de eerder sobere website van Jamestown Analytics**. Dat is geen valse bescheidenheid. De Britse kwaliteitskrant The Times noemt hen 'het beste databedrijf in het voetbal', al blijken ze niet bepaald goedkoop.

DE TECHNISCHE INFRASTRUCTUUR ACHTER HET SUCCES

Het platform van Jamestown Analytics combineert ruwe statistieken met eigen datacollectie en laat daar 'tal van gesofisticeerde algoritmes op los', zoals een waarnemer het omschrijft. Cruciale toevoeging: **ook persoonlijk-**

Het Joseph Mariën-stadion, waar Union kampioen werd, ruimt binnenkort plaats voor een moderner exemplaar, gefinancierd met datagedreven transferwinsten.

heidsprofielen worden meegenomen in de analyse. Ook dat doet denken aan de film Moneyball, waarin het sportieve team bij een speler een gebrek aan zelfvertrouwen detecteerde op basis van diens keuze voor een minder aantrekkelijke vriendin met wat overgewicht.

In elk geval gaat de granulariteit van de data bij Union verder dan traditionele statistieken. Het systeem meet zelfs het aantal decibels dat supporters produceren wanneer specifieke spelers aan de bal zijn, om zo de impact van individuele spelers op de teamdynamiek te kwantificeren.

VAN DUITSE DERDEKLASSER TOT CHAMPIONS LEAGUE

Ook in data-land geldt het adagium: *vivons heureux, vivons cachés*. Tony Bloom en Starlizard hangen niets aan de grote klok. Ze proberen bewust onder de radar te blijven en zijn daarin best achterdochtig. Aanvragen voor een interview of bezoek aan hun kantoor worden afgewimpeld. **Werknemers mogen geen sociale media-accounts** beheren en moeten geheimhoudingsclausules tekenen. Als zou uitlekken waar Starlizard zijn geld op inzet, zouden massaal veel mensen op hetzelfde kunnen wedden. En dan zijn ze hun voorsprong kwijt.

De resultaten van de aanpak spreken voor zich. Union pikte spits Deniz Undav weg uit de Duitse derde klasse, vond Victor Boniface op de bank bij een Noors team, en haalde Mohammed Amoura als invaller uit Zwitserland. Huidig topschutter Promise David speelde in Estland. Deze **spelers werden voor minimale bedragen aangekocht en later doorverkocht met enorme winst** – Boniface bijvoorbeeld voor 20 miljoen euro na één jaar.

Union haalt spelers die voor anderen onhaalbaar zijn, letterlijk dan. “Voor clubs als Club Brugge of Anderlecht zou het heel moeilijk zijn een Undav of Burgess in de Duitse of Engelse derde klasse te vinden”, erkende Union-voorzitter Muzio onlangs aan *De Standaard.* “Maar Starlizard dekt met zijn gegevens bijna alle competities die je maar kunt bedenken.”

COMPLIANCE EN CONCURRENTIEVOORDEEL

Enige handigheid helpt ook. Toen UEFA verbood dat Brighton en Union dezelfde eigenaar zouden hebben, bedacht het team een elegante technische oplossing. Union werd klant van Jamestown Analytics, formeel een apart bedrijf met exclusieve rechten voor België. Deze constructie, gevestigd in hetzelfde kantoorcomplex als Starlizard aan Jamestown Road, behoudt het concurrentievoordeel terwijl het voldoet aan de regelgeving.

Het businessmodel schaalt intussen ook internationaal. Jamestown Analytics werkt inmiddels ook voor het Italiaanse Como, Spaanse Castellón, Schotse Hearts, Australische Melbourne Victory en Engelse Grimsby Town. Opvallend: alle klanten zijn ‘underdogs’ – teams die stuk voor stuk vanuit lagere divisies naar boven klimmen.

RENDEMENT EN TOEKOMSTVISIE

Niet alleen de sportieve resultaten maar ook de zakelijke cijfers bevestigen de effectiviteit van deze datagedreven benadering. Union realiseerde afgelopen seizoen 16 miljoen euro nettowinst en kwalificeerde zich voor de Champions League – een financiële jackpot van tientallen miljoenen. Deze cashflow wordt geherinvesteerd in infrastructuur, waaronder een nieuw stadion met 16.000 zitplaatsen en een ultramoderne jeugdacademie.

De Union-case toont aan dat data-analyse niet alleen de efficiëntie of werking verbetert, maar complete industrieën kan herdefiniëren. Door technologie strategisch in te zetten, kunnen kleinere organisaties systematisch concurreren met veel grotere partijen. Voor bedrijven en hun IT-professionals is dit een perfect voorbeeld van hoe algoritmes en big data concrete businessresultaten kunnen leveren op plekken waar je het misschien niet meteen zou verwachten.

EEN ZAK GELD SCOORT NIET

De oude voetbalgrootmeester Johan Cruijff vertelde ooit, naar aanleiding van de alsmaar groter wordende geldtoevloed in het betaald voetbal, dat hij ‘nog nooit een zak geld een goal had zien maken’. Maar dat was nog voor de tijd van big data en algoritmes. In voetbal wint niet altijd de club of voorzitter met de diepste zakken, maar wel die met het slimste datateam.

DATA ACHTER DATA

242
Zoveel hoogopgeleide analisten, statistici en onderzoekers werken bij Starlizard.

20 tot 100 miljoen euro
De gemiddelde jaarwinst van Starlizard.

500.000 euro of meer
De halfjaarlijkse bonus voor sommige data-analisten.

Enkele miljoenen
Zoveel datapunten verzamelt Starlizard wekelijks.

STEEDS MEER PARTNERS VOOR IT-OUTSOURCING: WELKE KIES JE?

Van softwareontwikkeling en infrastructuur tot security: bedrijven hebben steeds meer keuze in IT-outsourcingpartners. “Vaak zijn klanten meer tevreden over hun IT-dienstenleverancier dan omgekeerd.”

1/ MARKT VERZADIGD

35 IT-outsourcingbedrijven staan op de lijst van het bureau Whitelane Research, en dat aantal is de voorbije jaren alleen maar toegenomen. “De markt is eigenlijk verzadigd. In mijn onderzoek geeft 31 procent van de klanten aan meer van hun IT-budget aan externe providers te willen besteden. Dat is het laagste percentage in vijf jaar”, stelt Jef Loos van Whitelane Research. Bovendien is het niet zo dat er heel veel overnames zijn geweest in de markt. “Van een grootschalige **consolidatie in de markt van IT-dienstverleners is geen sprake**.”

In het onderzoek van Whitelane Research zijn meer dan 300 van de grootste bedrijven in België en Luxemburg betrokken, goed voor 800 contracten. Het zijn dus de grootste klanten van IT-dienstverleners die aan het onderzoek deelnamen. Whitelane Research doet elk jaar onderzoek naar sourcingdeals en hun klanten. Het polst hierbij naar de tevredenheid.

2/ DAAR ZIJN DE CONSULTANTS

De grote nieuwkomers van de laatste jaren komen uit de hoek van de grote consultancybedrijven. Partijen als Deloitte en PwC hebben zich de voorbije jaren gespecialiseerd in domeinen zoals digitale transformatie en security. Ze zijn hier ook erg bedreven in geworden. “Intussen zie je dat de meer **strategische consultants zoals McKinsey en Boston Consulting Group** zich ook meer en meer in de markt van IT-outsourcing begeven.”

3/ TEVREDENHEID OVER LEVERANCIERS IS HOOG

Computacenter, Stefanini, Hexaware, GTT, Cronos en Cegeka voeren de algemene rangschikking aan (zie afbeelding), over alle domeinen heen, allemaal met scores boven de 80 procent. Deze scoren traditioneel vrij hoog. Alleen

WIE IS WIE IN OUTSOURCING?

1. **De Belgen,** zoals Cegeka, Cronos, Proximus en Telenet
2. **De Indiërs,** zoals TCS, Wipro, Infosys en Tech Mahindra
3. **De Europeanen,** zoals Capgemini, Inetum, Atos/Eviden en Econocom
4. **De consultants,** zoals Deloitte en PwC
5. **De specialisten,** zoals Orange Cyberdefense (security), Computacenter (workplace) en GTT (network)

RANKSCHIKKING PER DOMEIN

Applicatie
1. Deloitte (83%)
2. Cognizant (83%)
3. Cegeka (83%)

Cloudinfrastructuur
1. Cegeka (83%)
2. Atos/Eviden (81%)
3. Kyndryl (80%)

Workplace
1. Computacenter (89%)
2. Stefanini (86%)
3. Econocom (78%)

Network & connectivity
1. GTT (84%)
2. Telenet (82%)
3. NTT Data (81%)

Security
1. Cegeka (87%)
2. Telenet (83%)
3. Proximus (81%)

Cloudinfrastructuurplatform
1. Microsoft Azure (77%)
2. AWS (77%)
3. Oracle Cloud (75%)

Cloudsoftwareplatform
1. Microsoft Dynamics 365 (76%)
2. Workday (75%)
3. ServiceNow (73%)

Bron: Whitelane Research, 2025.
Percentage staat voor klantentevredenheid.

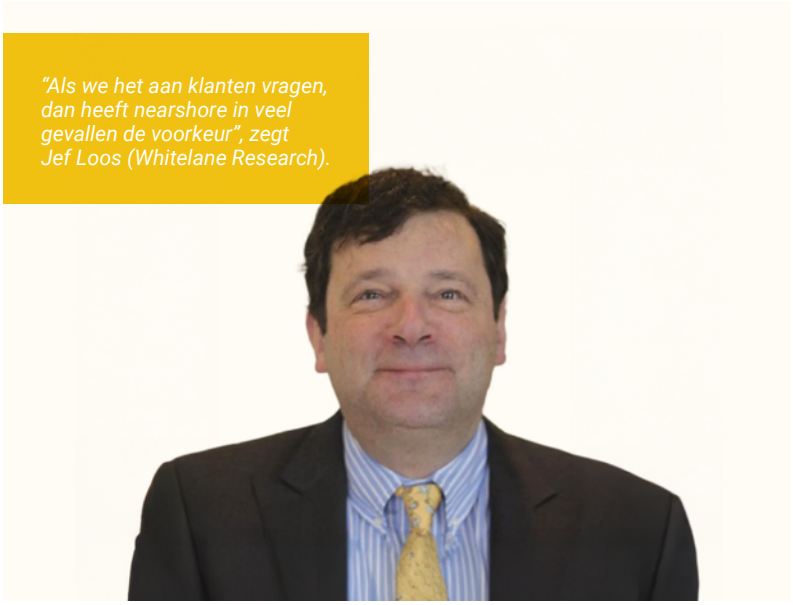
ALGEMENE RANKSCHIKKING

Leverancier	Tevredenheid
Computacenter	90%
Stefanini	87%
GTT	84%
Hexaware	84%
Cegeka	82%
Cronos	82%
Telenet	81%
TCS	81%
Deloitte	81%
PwC	80%
Kyndryl	80%
Infosys	80%
Cognizant	80%
Accenture	80%
Orange Cyberdefense	79%
Atos/Eviden	79%
Inetum-RealDolmen	79%
Verizon	78%
Econocom	78%
NTT DATA	78%
CGI	78%
Delaware	78%
Colt	78%
HCLTech	78%
Orange Business	77%
NRB	77%
Proximus	77%
Fujitsu	77%
Wipro	76%
DXC Technology	75%
Sopra Steria	75%
Capgemini	75%
BT	73%
IBM	69%
Tech Mahindra	68%

Stefanini, dat zich richt op workplacediensten, is wat dat betreft een relatieve nieuwkomer.

Tech Mahindra en IBM staan onderaan met (iets) minder dan 70 procent. De **gemiddelde score is best hoog** met 78 procent. “Er zijn geen slechte outsourcers in België”, benadrukt Jef Loos. “Maar door het grote aanbod is het voor outsourcers een kwestie om goed te scoren. Zo komen ze onder de aandacht van de klanten.” Bij Whitelane draait het om klantentevredenheid. Natuurlijk zijn er nog andere factoren die een rol spelen bij de keuze van een leverancier, zoals beschikbaarheid (van talent in de specifieke materie), ervaring in het betreffende domein en prijszetting.

“Als we het aan klanten vragen, dan heeft nearshore in veel gevallen de voorkeur”, zegt Jef Loos (Whitelane Research).



4/ TEVREDENHEID OVER KLANTEN LIGT LAGER

Dat is een opvallende kloof, met name als het gaat om governance capabilities. “Als we vragen naar de capabiliteit in transitie en change management bij outsourcingprojecten, geeft een kwart van de klanten van zichzelf aan dat dit onderdeel vatbaar is voor verbetering. Maar als je het aan de leveranciers vraagt, geeft maar liefst 58 procent aan dat de capaciteiten van klanten in **transitie en change management beter kunnen**. Ik denk dat dit cijfer dichter bij de waarheid ligt.”

5/ NEARSHORE IN TREK

In de wereld van IT-outsourcing zijn er – als het om locatie gaat – drie modellen die voor Belgische en Europese organisaties vooropstaan: onshore (thuisland), nearshore (buurlanden of relatief dichtbij zoals Polen of Roemenië) of offshore (verre bestemmingen zoals India of de Filipijnen). Vaak is het schuiven en schakelen tussen onshore, nearshore en offshore.

“Als we aan klanten vragen in welke richting van deze drie ze willen bewegen, dan heeft nearshore in veel gevallen de voorkeur van klanten”, stelt Loos vast. Uit het onderzoek van Whitelane Research blijkt dat 12 procent van de organisaties onshore outsourcing wil uitbouwen. Voor offshore is dat 26 procent, maar voor nearshore 39 procent. “Klanten **verkiezen nearshore omwille van klassieke voordelen**”, weet Jef Loos van Whitelane Research. “Ze kunnen aan de slag in dezelfde of in een nabije tijdzone. De afstand is beperkt en ze voelen zich vaak comfortabeler in de talenkennis van de outsourcer daar”, stelt hij.

Al speelt de schaarste aan talent ook een rol in nearshore-locaties zoals Oost-Europa. Offshore, in landen als India, zijn er twintig keer zoveel *resources* als nearshore. Volgens Loos hangt er regelmatig een bordje met ‘uitverkocht’ op de nearshore-bestemmingen. “Er zijn dikwijls gewoon onvoldoende resources beschikbaar en we zagen als gevolg ook de prijzen flink toenemen.”

6/ OFFSHORE IN VRAAG

Niet alleen bedrijven bouwen eerder nearshore-activiteiten op en die in offshore-locaties af, er speelt nog iets anders. Volgens onderzoek van Whitelane Research heeft 28 procent van de grote organisaties een eigen delivery center voor IT-diensten in het buitenland, en ongeveer de helft daarvan is van plan dit uit te breiden. Dit wordt vaak aangeduid als een captive center. Veel organisaties, zoals Johnson & Johnson, BNP Paribas en AXA, hebben inmiddels zo’n center opgezet.

In India is **het idee van een captive center momenteel zeer actueel**. Een aantal bedrijven wil er een uit de grond stampen. “Bij de oprichting van een captive center moeten schaalvoordelen zeker een rol spelen. Je spreekt al snel over een center met 300 tot 500 medewerkers.”

Deze plannen hebben ongetwijfeld impact op grote outsourcingpartijen zoals Accenture en Capgemini. De meeste mondiale IT-serviceproviders hebben momenteel meer dan de helft van hun wereldwijde personeel in India. “Globale outsourcingpartijen werken volgens hun *global delivery network*, waarbij Indiërs onderdeel uitmaken van dat netwerk”, stelt Loos. “Alleen al in België realiseren Indiase outsourcingpartijen zoals Tata Consulting Services en Infosys jaarlijks een omzet van 1 miljard euro.”

HR EN IT VERSMELTEN ONDER DRUK VAN AI-AUTOMATISERING

De traditionele scheiding tussen HR en IT vervaagt nu AI-agents steeds meer werkzaamheden overnemen. Twee recente ontwikkelingen illustreren deze verschuiving: IBM vervangt honderden HR-medewerkers door AI, terwijl Moderna zijn HR- en IT-afdelingen zelfs samenvoegt.

IBM CEO Arvind Krishna onthulde enkele weken geleden dat het techbedrijf AI-agents heeft ingezet om het werk van 'een paar honderd HR-medewerkers' over te nemen, zo meldde *The Wall Street Journal*. De vrijgekomen middelen worden volgens de CEO herinvesteerd in andere functies zoals softwareontwikkeling, verkoop en marketing.

Met de opmars van AI wordt de HR-afdeling nog meer geautomatiseerd. "Wat AI doet, is dat het je meer inves-

teringsruimte geeft om in andere gebieden te steken", aldus Krishna. Hij benadrukt dat deze domeinen gericht zijn op 'kritisch denken' en werk waarbij mensen 'tegenover andere mensen staan, in plaats van alleen routineus proceswerk te doen'.

TAAKGERICHTE ARCHITECTUUR

Waar functies voorheen vaak werden gedefinieerd door afdelingen en hiërarchieën, ontstaat nu steeds vaker een taakgerichte architectuur. Organisaties analyseren welke onderdelen van een functie routinematig zijn en geschikt voor automatisering met bijvoorbeeld AI-agents, en welke juist menselijke creativiteit, empathie of complexe besluitvorming vereisen. "Generatieve **AI heeft het potentieel om menselijke capaciteit te ontsluiten en menselijk kapitaal te behouden**", stelde Alicia Pittman, managing director & partner bij Boston Consulting Group (BCG) onlangs op *Business Insider.*

Deze fragmentatie van werk vereist een fundamenteel andere benadering van organisatiestructuren. Medewerkers moeten ook leren samenwerken met AI-systemen als digitale collega's. "Tegelijkertijd moeten organisaties investeren in rollen die deze hybride workflows kunnen ontwerpen en beheren", aldus Pittman.

MODERNA INTRODUCEERT HYBRIDE LEIDERSCHAPSROL

Biotechbedrijf Moderna gaat nog een stap verder door zijn HR- en technologieafdelingen volledig samen te voegen. Het bedrijf creëert een nieuwe functie, die van de *Chief People & Digital Technology Officer*. Deze hybride rol moet **talent- en technologiestrategieën op structureel niveau afstemmen**.

De nieuwe functie keert de traditionele aanname om dat mensen dé standaard productieve eenheid zijn. In plaats daarvan wordt taakarchitectuur de bepalende factor voor kosten, snelheid en naleving. De centrale vraag luidt dan ook: welke workflows kunnen al door AI worden uitgevoerd en welke menselijke vaardigheden blijven schaars? Deze visie sluit aan bij het advies van Ethan Mollick, professor aan de Wharton School aan de University of Pennsylvania en hoofd van het GenAI Lab: *"Treat AI like a person, but always remember it isn't."*

GEVOLGEN VOOR IT-ORGANISATIES

De verschuivingen bij IBM en Moderna tonen aan dat de integratie van AI-agents geen toekomstmuziek meer is, maar stilaan werkelijkheid wordt. Voor IT-afdelingen betekent deze ontwikkeling een uitbreiding van hun verantwoordelijkheden. IT-professionals zullen zich ook moeten voorbereiden op een rol waarin technische expertise gecombineerd wordt met begrip van organisatiedynamiek en menselijke workflows. Waar IT traditioneel systemen en infrastructuur beheerde, wordt nu ook de **orchestratie van mens-machineworkflows** onderdeel van hun domein, benadrukte Ethan Mollick in een recente TED-talk. Dit vereist nieuwe competenties op het snijvlak van technologie en organisatieontwerp.

Bedrijven die deze hybride expertise niet ontwikkelen, lopen het risico hun AI-investeringen niet duurzaam te kunnen verzilveren, zo klinkt het ook bij Boston Consulting Group. "De uitdaging ligt niet alleen in het gebruiken van de technologie", aldus Ethan Mollick. "Maar ook in het behouden van de bedrijfscultuur, en menselijkheid, in de organisatie, terwijl automatisering versnelt."

Ethan Mollick (University of Pennsylvania): "Treat AI like a person, but always remember it isn't."

CASE

KINEPOLIS INTEGREERT HR EN IT VOOR INTERNATIONALE GROEI

De Europese bioscoopketen Kinepolis hanteert een geïntegreerde aanpak tussen HR en IT om zijn groeistrategie te ondersteunen. Het bedrijf, dat bioscopen exploiteert in zeven landen, zet technologie in als strategische factor voor zowel operationele efficiëntie als werknemerservaring. "IT is de ruggengraat van onze dagelijkse operaties en toekomstige groei", zo vertelde Kurt Pede, hoofd IT-productie bij Kinepolis, recent aan *HR Magazine*. Deze benadering krijgt vorm bij overnames, waar snelle technische integratie bepalend is voor het succes van nieuwe vestigingen.

Bij een recente overname in Frankrijk werkte Kinepolis met vooraf geconfigureerde hardware via HP's Device Provisioning-dienst en Microsoft Intune. "We hadden slechts een beperkte tijd om een overgenomen bioscoop volledig operationeel te krijgen", verklaart Pede. Deze aanpak stelde het bedrijf in staat om binnen de gestelde deadline een werkende vestiging op te leveren.

De technische infrastructuur heeft directe gevolgen voor personeelsprocessen. Nieuwe medewerkers kunnen zonder technische vertragingen beginnen, wat onboarding-procedures versnelt. Het bedrijf migreert momenteel van legacy-systemen naar moderne tools zoals Microsoft Intune, wat meer flexibiliteit moet bieden voor verschillende werkmodellen.

Kinepolis hanteert een hybride IT-architectuur met eigen datacenters naast cloudoplossingen via Azure en AWS. Deze complexiteit vereist nauwe afstemming tussen IT- en HR-afdelingen om systemen operationeel te houden zonder werknemers te hinderen.

De samenwerking tussen beide afdelingen gaat verder dan louter de technische kant. HR-managers bij Kinepolis zijn actief betrokken bij de keuze van tools en het ontwerp van workflows, terwijl IT-teams rekening houden met gebruikerservaring en opleidingsnoden bij systeemupgrades. Een illustratie van hoe technologische beslissingen rechtstreeks inspelen op organisatorische doelen – en hoe structurele samenwerking tussen HR en IT daarbij cruciaal is.

"Door de verschillende overnames hadden we een zeer complex IT-landschap met systemen die niet goed met elkaar communiceerden", aldus Koen Crabbe van Mediahuis.

TENANT-TO-TENANTMIGRATIE BIJ MEDIAHUIS VERENIGT EUROPESE TEAMS OP ÉÉN MICROSOFT 365-OMGEVING

48 TERABYTE, 1.500 GEBRUIKERS EN 1 WEEKEND

48 terabyte aan kritieke bedrijfsdata migreren zonder downtime, terwijl de redacties van internationale nieuwsmerken gewoon blijven doorwerken aan hun content: de uitdaging voor mediagroep Mediahuis was groot, de IT-migratie complex. "Dit vormt de basis voor verdere digitalisering."

DE UITDAGING: CONSOLIDATIE VAN EEN COMPLEX IT-LANDSCHAP

Voor Mediahuis, de Europese mediagroep achter nieuwsmerken zoals De Telegraaf, De Standaard en Irish Independent, vormde de **gefragmenteerde IT-infrastructuur een rem op de groeiambities**. “Door de verschillende overnames hadden we een zeer complex IT-landschap met systemen die niet goed met elkaar communiceerden”, aldus Koen Crabbe, delivery manager ICT Infrastructure bij TPS, de technologie- en productafdeling van Mediahuis. “Dit belemmerde niet alleen de interne samenwerking, maar maakte ook gegevensbeheer en beveiliging complex.”

De cijfers benadrukken de omvang van de uitdaging: 136 domeinnamen, meer dan 1.500 gebruikersaccounts, 930 gedeelde mailboxen, 1.351 Teams-kanalen, 14,6 TB maildata en 33,5 TB OneDrive-data moesten worden gemigreerd. Bovendien stelde Mediahuis als voorwaarde dat de migratie binnen één weekend moest plaatsvinden om operationele continuïteit te waarborgen.

Het risicoprofiel was aanzienlijk. **Dataverlies was geen optie** voor een mediabedrijf dat afhankelijk is van continue nieuwsproductie. Ook de vertrouwelijkheid van gevoelige journalistieke informatie moest gewaarborgd blijven tijdens het migratieproces. De uitdaging werd verder gecompliceerd door de noodzaak om gebruikers uit verschillende omgevingen en werkculturen te integreren op één platform.

DE OPLOSSING: GEAUTOMATISEERD MIGRATIEFRAMEWORK

Mediahuis-partner Inetum zette een geautomatiseerd Master Framework in voor de complexe migratie. Dit framework vormde de ruggengraat van een gestructureerde aanpak die risico’s minimaliseerde en transparantie maximaliseerde.

Het migratieproces bestond uit **verschillende geautomatiseerde componenten**. De Teams-chatmigratie zorgde ervoor dat alle conversaties, inclusief groepschats en deelrechten op documenten, behouden bleven. Voor Mediahuis was dit cruciaal omdat veel redactionele samenwerking via Teams verloopt.

Een migratiedashboard bood real-time inzicht in de voortgang per gebruiker, wat Koen Crabbe en zijn team in staat stelde om de hele migratie nauwkeurig te monitoren. “Zo konden we precies zien welke onderdelen van de migratie waren voltooid en waar eventuele problemen opdoken. Deze transparantie gaf ons het vertrouwen dat we de strakke planning zouden halen.”

Een ander kritiek onderdeel was de clientconversie, die alle clienttoepassingen die naar de oude tenant verwezen, **automatisch omleidde naar de nieuwe omgeving**. Dit voorkwam dat gebruikers na de migratie handmatig instellingen moesten aanpassen.

De planning werd uitgewerkt met gedetailleerde tijdschema's en contingency-procedures. Testmigraties werden uitgevoerd om potentiële knelpunten te identificeren voordat de daadwerkelijke migratie plaatsvond.

HET RESULTAAT: SUCCESVOLLE CONSOLIDATIE ZONDER DOWNTIME

De weekendmigratie werd succesvol uitgevoerd zonder dataverlies of significante onderbrekingen. Alle 48 TB aan data werd veilig overgezet, en maandagochtend konden alle meer dan 1.500 gebruikers gewoon doorwerken op het nieuwe platform.

Voor Mediahuis betekent dit meer dan alleen een technische upgrade. De geconsolideerde tenant maakt **echte samenwerking mogelijk in verschillende landen** tussen redacties, terwijl het management beter zicht heeft gekregen op resources en workflows. “We zien nu al dat de

Koen Crabbe, delivery manager ICT Infrastructure bij TPS.

samenwerking tussen onze teams intensiever is geworden”, zegt Crabbe. “Collega's uit Nederland kunnen gemakkelijker samenwerken met collega's uit België of Ierland. Dit opent nieuwe mogelijkheden voor crossmediale content en efficientere nieuwsproductie.”

De migratie heeft ook de digitale transformatie van Mediahuis versneld. Het bedrijf beschikt nu naar eigen zeggen over een solide, schaalbare basis voor toekomstige groei en acquisities. Nieuwe overnames kunnen eenvoudiger worden geïntegreerd omdat er nu één gestandaardiseerd platform is.

En dan is er natuurlijk nog het beveiligingsperspectief. In plaats van meerdere systemen te moeten beveiligen en beheren, kan Mediahuis zich nu concentreren op één robuuste omgeving met consistente security policies en compliance-procedures.

De succesvolle migratie benadrukt het belang van zorgvuldige planning, gedegen projectmanagement, geautomatiseerde tools en ervaren partners bij complexe IT-transformaties. Het IT-project veroverde een plek op de shortlist van de Computable Awards in de categorie *project of the year enterprise market*. Voor Mediahuis vormt deze migratie, volgens de delivery manager ICT infrastructure, alvast **de basis voor verdere digitalisering** en groei in de competitieve mediamarkt.

EXCLUSIEF ONDERZOEK

DE GROTE SOFTWARE DEVELOPMENT UPDATE

We nemen een diepe duik in de manier waarop organisaties en hun IT-professionals vandaag software ontwikkelen. Hoe organiseren ze hun teams? Welke uitdagingen ervaren ze? Welke methodologieën, programmeertalen en tools gebruiken ze? En uiteraard: wat gebeurt er met AI?

We vroegen bij de SAI.BE-leden en hun softwareverantwoordelijken via een uitgebreide vragenlijst wat er speelt in software development. Hier ontdek je de resultaten en bevindingen.

1 UITDAGINGEN: LEGACY EN BUDGETDRUK

Uit het onderzoek blijkt dat budgettaire beperkingen (21 procent) nog altijd de grootste uitdaging vormen bij softwareprojecten, op de voet gevolgd door het onderhouden en moderniseren van legacysystemen (18 procent). De blijvende impact van verouderde IT-landschappen blijft gevolgen hebben voor de digitalisering.

Projectvereisten (16 procent) – een klassieker bij IT-projecten – en compliance (14 procent) zijn eveneens grote zorgen, wat wijst op de toegenomen complexiteit van regelgeving en klanteisen. “Onze compliance-vereisten zijn vandaag belangrijk en dringend”, zegt een deelnemer aan het onderzoek uit de financiële sector, waar de compliancevereisten hoog zijn.

Opvallend: slechts 9 procent noemt ontwikkelaars-schaarste als topuitdaging, wat een indicatie kan zijn van meer stabiele IT-teams, effectiever resource management of een minder forse war for talent. Vaak gaat het om een combinatie van uitdagingen. “Wij merken bijvoorbeeld veel meer gelijktijdige lopende projecten met kortere opleveringsdata”, oppert Geert Debruyne van softwarebedrijf Qastan. “Hierdoor kan kwaliteitsbewaking in het gedrang komen.”

Wat zijn momenteel de grootste uitdagingen in uw interne softwareprojecten?

Budgetherzieningen en -beperkingen)	21%
Businessbetrokkenheid	7%
Projectvereisten (scope, deadlines, requirements)	16%
Compliancevereisten (security, privacy, wetgeving, intern)	14%
Legacysystemen onderhouden of moderniseren	18%
Beschikbaarheid ontwikkelaars	9%
Projectleiding	2%
Kwaliteit (opgeleverde code of documentatie)	6%
Snel wijzigende technologie	5%
Snelle marktevoluties met impact op businessprocessen	3%

N = 54, max. 3 antwoorden

2 TEAM: DEVOPS DOMINANT, LOW-CODE KOMT OPZETTEN

Een multidisciplinair teammodel met DevOps en QA (Quality Assurance) in één team is bij 38 procent van de bedrijven het dominante organisatiemodel. De traditionele scheiding tussen development, testing en operations wordt duidelijk verlaten.

Tegelijk werkt een kwart van de organisaties met een mix van interne en externe partners. 5 procent besteedt ontwikkeling volledig uit. Opvallend is de opkomst van low-code/no-codeplatformen (19 procent), wat kan wijzen op een focus op snelle applicatieontwikkeling. “Low-code met leveranciers als OutSystems is een duidelijke trend”, zegt Ronny Ruyters van IT-dienstverlener ACA Group.

Hoe is het IT-personeel en de ontwikkelingsaanpak binnen uw organisatie momenteel georganiseerd?

We hebben multidisciplinaire productteams (devops, qa)	38%
Er zijn aparte afdelingen voor development, testing en operations	13%
We werken met interne teams en met externe partners	25%
De ontwikkeling is uitbesteed aan externe partners	5%
We gebruiken low-code/no-codeplatformen	19%

N = 54, max. 3 antwoorden

3 METHODOLOGIE: AGILE IS DE NORM

"Onze methodologie is een mix van de 'pure' Agiles. We gaan vooral voor zo weinig mogelijk overhead bij de developers", stelt Geert Debruyne van Qastan.

Agile-methodologieën zijn dominant, met een score van acht op tien voor front-end en zeven op tien voor back-end. Waterfall is dus eerder uitzondering dan regel. Dit bevestigt de volwassenheid van agile in België. Agile werkt niet alleen sneller, het sluit ook beter aan bij de snel veranderende eisen van business en klant. De iets lagere score voor back-end kan wijzen op complexere integraties of afhankelijkheden die agile moeilijker maken.

Wat is de verhouding tussen volgende ontwikkelmethodologieën die u gebruikt voor front-end en back-end development?
(5 geeft een fifty-fifty verdeling tussen beiden weer)

Front-end
agile versus **waterfall**

Back-end
agile versus **waterfall**

4a PROGRAMMEERTALEN FRONT-END: JAVASCRIPT BLIJFT KONING, TYPESCRIPT GROEIT

JavaScript (28 procent) blijft veruit de populairste taal voor nieuwe frontendprojecten, met TypeScript (18 procent) als snelgroeiende opvolger. TypeScript wordt vaak gekozen boven JavaScript voor grotere, complexere projecten vanwege de statische typering. Dit helpt bij het vroegtijdig opsporen van fouten, wat leidt tot betere codekwaliteit en onderhoudbaarheid.

De rol van Java en C# in front-end blijft verrassend groot, zeker bij bestaande projecten, wat kan wijzen op (web)applicaties met oudere technologie of op toepassingen waar front-end en back-end in dezelfde taal geschreven zijn.

Welke programmeertalen worden vooral gebruikt in uw organisatie voor front-end development?

Front-end	Bestaande projecten	Nieuwe projecten
Java	20%	18%
Python	6%	11%
JavaScript	24%	28%
TypeScript	15%	18%
C#	8%	9%
C	2%	0%
C++	4%	1%
Rust	1%	1%
PHP	8%	4%
Cobol	0%	0%
Kotlin	1%	2%
Swift	0%	0%
Ruby	2%	0%
VB(.NET)	2%	2%
Zig	0%	1%
Andere	8%	7%

N = 54, max. 3 antwoorden

4b PROGRAMMEERTALEN BACK-END: JAVA STEVIG AAN KOP, PYTHON IN OPMARS

Voor back-endontwikkeling blijft Java met 33 procent de dominante kracht, zowel in bestaande als nieuwe projecten. De groei van Python (van 8 procent naar 13 procent) duidt op de bredere inzetbaarheid van deze taal in data- en AI-toepassingen. C# groeit naar 16 procent, waarschijnlijk door de populariteit van Microsoft-platformen en Azure. Cobol zakt van 12 procent (bestaande projecten) naar 4 procent (nieuwe projecten), maar blijft toch aanwezig – andermaal een signaal dat kritieke legacy (en dus ook Cobol) nog niet verdwenen is.

Welke programmeertalen worden vooral gebruikt in uw organisatie voor back-end development?

Back-end	Bestaande projecten	Nieuwe projecten
Java	32%	33%
Python	8%	13%
JavaScript	8%	6%
TypeScript	3%	2%
C#	10%	16%
C	3%	0%
C++	7%	8%
Rust	1%	2%
PHP	4%	3%
Cobol	12%	4%
Kotlin	2%	3%
Swift	0%	0%
Ruby	0%	0%
VB(.NET)	4%	3%
Zig	0%	0%
Andere	8%	8%

N = 54, max. 3 antwoorden

5 TOOLS: GIT EN JIRA ZIJN HOEKSTENEN, AI-TOOLS IN OPMARS

Git-platformen (20 procent), Jira (16 procent), en Docker (14 procent) domineren het toolgebruik. Deze combinatie wijst op een sterke DevOps- en CI/CD-cultuur. GitHub Copilot (8 procent) wordt in dit domein al relatief veel gebruikt, wat wijst op een snelle adoptie van AI-assistenten. Jenkins is met 10 procent nog altijd relevant ondanks de opkomst van nieuwere CI/CD-tools zoals GitHub Actions (4 procent).

Welke tools gebruikt uw team momenteel hoofdzakelijk in de ontwikkelingscyclus?

Git (GitHub, GitLab)	20%
Jenkins	10%
GitHub Actions, GitLab CI	4%
Jira	16%
Azure DevOps	9%
Trello	1%
Docker (containers)	14%
Visual Studio Code	9%
JetBrains IDEs	7%
Cursor	0%
Windsurf	0%
GitHub Copilot	8%
Cline	1%
Andere	2%

N = 54, max. 3 antwoorden

6 KWALITEITSCONTROLE: AUTOMATISERING IS STANDAARD

Kwaliteitscontrole is bij bijna alle bedrijven ingebed in het ontwikkelproces. Geautomatiseerde tests (27 procent), manuele codereviews (26 procent) en CI/CD kwaliteitschecks (25 procent) vormen de top. Slechts 1 procent heeft geen formele kwaliteitscontrole, of erkent dat. Statische analyse (15 procent) blijft relatief beperkt, wat ruimte laat voor groei, zeker in grotere codebasissen. AI-ondersteunde kwaliteitsbewaking (6 procent) staat nog in de kinderschoenen, maar dat aandeel zal waarschijnlijk groeien.

Hoe wordt de kwaliteit van uw code bewaakt in uw organisatie?

Codereviews (manueel)	26%
Geautomatiseerde tests (unit tests, integration tests)	27%
CI/CD pipelines met kwaliteitschecks	25%
Statische codeanalyse	16%
AI	6%
Geen formele kwaliteitscontrole	1%

N = 54, max. 3 antwoorden

7 ARTIFICIAL INTELLIGENCE IN SOFTWARE DEVELOPMENT

Bijna 90 procent van de bedrijven gebruikt AI in de ontwikkeling, al is dat vooral in ondersteunende vorm. AI-tools voor codeassistentie (47 procent) zijn het populairst, gevolgd door AI voor testgeneratie en debugging (16 procent).

Ook het gebruik van AI voor requirements en documentatie (10 procent) groeit. 16 procent gebruikt AI in het product zelf, wat aantoont dat hoewel AI-tools in de developer-ervaring doordringen, AI-productfunctionaliteit nog minder courant is.

Hoe wordt AI momenteel ingezet in uw ontwikkelproces?

AI wordt (nog) niet gebruikt	10%
AI-tools voor codeassistentie	47%
AI voor testgeneratie of foutopsporing	16%
AI voor requirementsanalyse en/of documentatie	10%
AI in het product zelf (zoals ML-modellen in applicaties)	16%

N = 54, max. 3 antwoorden

CONCLUSIE: GROEIENDE MATURITEIT MET AI AAN DE POORT

Belgische bedrijven, en de SAI.BE-leden in het onderzoek, tonen een best professionele en gestructureerde aanpak in softwareontwikkeling. **Agile is de norm, DevOps groeit** en de kwaliteit wordt stevig bewaakt met geautomatiseerde processen. **Legacy blijft een remmende factor en ook de budgetdruk blijft voelbaar.**

Tegelijk zien we de eerste echte golf van AI-adoptie, vooral in tooling, maar nog beperkt in autonome of productmatige toepassingen. AI is AI een potentiële gamechanger aan de horizon.

In het volgende nummer van SAI Update lees je het tweede deel van het Software Development Update-onderzoek: trends, cloud, infrastructure, architecture en security in software development.

» *Bekijk of herbekijk **hier** de SAI Shorts over softwareontwikkeling.*

AI IN SOFTWAREONTWIKKELING

WANNEER WEL EN WANNEER (NOG) NIET?

AI is vandaag al een vast onderdeel van het ontwikkelproces. Uit het Software Development Update-onderzoek van SAI.BE blijkt dat 47 procent van de ontwikkelaars tools voor code-assistentie gebruikt. De vraag is dan ook niet langer óf je AI inzet, maar: waar maakt het echt een verschil en waar dreigt het meer schade dan voordeel te veroorzaken?

Volgens Gunnar Grosch, principal developer advocate bij AWS, zit het probleem niet in een gebrek aan technologie, maar in een verkeerd evenwicht. “Ontwikkelaars besteden vandaag 73 procent van hun tijd aan het draaien en onderhouden van bestaande toepassingen, en slechts 27 procent aan innovatie en transformatie”, zegt Grosch, waarmee hij citeert uit het ***Global code time report*** **van software.com**. “AI kan helpen die verhouding om te keren.”

Grosch ziet AI dan ook als een manier om ontwikkelaars productiever te maken, zonder dat hun vaardigheden zelf veranderen. “Mijn niveau als ontwikkelaar blijft met AI hetzelfde, maar je krijgt meer gedaan.”

WANNEER AI WÉL LOONT

Volgens Grosch ligt de sterkte van AI in bepaalde taken. Een klassiek voorbeeld is het genereren van code: je beschrijft wat je wilt, en de AI doet een eerste voorstel. “In plaats van alles te schrijven, wordt het een kwestie van begrijpen en bijsturen”, zegt hij. Ook bij het analyseren van bestaande systemen – bijvoorbeeld code die je niet zelf geschreven hebt – kan AI assisteren: het helpt begrijpen wat de code doet, optimaliseert waar nodig en voegt zelfs automatisch commentaar toe.

Een andere concrete toepassing is het bouwen van API’s. Daar ziet Grosch een nieuwe generatie AI ontstaan: development agents die niet alleen code genereren, maar een heel plan voorstellen. “Je vraagt om een API, en de agent komt met suggesties, bouwt het op, integreert het met een interface en kan zelfs helpen om er een hele applicatie van te maken.” Hetzelfde principe geldt voor websites: op basis van ingevoerde informatie stelt de AI de structuur samen, voegt een API-koppeling toe en genereert een werkend geheel.

Documentatie, berucht als het minst populaire onderdeel van het ontwikkelwerk, is nog zo’n domein waar AI volgens Grosch uitblinkt. “Agentic features kunnen automatisch een structuur of skeleton aanmaken voor documentatie, of bestaande stukken bijwerken wanneer de code verandert.” Daarmee neemt AI net dat deel van de job over waar veel developers tijd verliezen of werk laten liggen.

Bovendien sluit dit naadloos aan bij de **vier belangrijkste toepassingsgebieden** die Grosch vandaag ziet **voor AI in softwareontwikkeling**: het verhogen van productiviteit, maar ook het afbouwen van technical debt via code-modernisering, het verbeteren van beveiliging en codekwaliteit én ondersteuning bij het testen.

“Mijn niveau als ontwikkelaar blijft met AI hetzelfde, maar je krijgt meer gedaan”, zegt Gunnar Grosch, principal developer advocate bij AWS.

WANNEER JE AI BETER NIET INZET

Toch zijn de grenzen van AI in softwareontwikkeling duidelijk voelbaar. Waar het model geen toegang heeft tot context, of wanneer taken complex of langdurig zijn, lopen de resultaten al snel mank. “Je kunt veel tijd verliezen – of zelfs code kwijtraken – als je AI zonder supervisie zijn gang laat gaan”, zegt Kevin Swiber, API-strateeg bij Layered System, in *InfoWorld*. Die waarschuwing geldt des te meer bij grote codebases, legacy-systemen of refactoring op schaal.

Ook Charity Majors, CTO van Honeycomb, is duidelijk: “**AI presteert vaak beter in het schrijven van nieuwe code dan in het aanpassen van bestaande codebases**.” De modellen zijn getraind op vaak voorkomende patronen en functioneren goed binnen beperkte, goed gedefinieerde taken. Maar zodra er domeinspecifieke kennis nodig is, of architecturale keuzes gemaakt moeten worden, volstaat generatieve AI vaak (nog) niet.

De risico’s zijn bovendien reëel: syntactisch correcte, maar logisch foute code, beveiligingsproblemen en een verhoogde *technical debt* als je AI-output ongezien integreert. In omgevingen waar betrouwbaarheid en governance essentieel zijn, blijft menselijke supervisie per definitie onmisbaar.

“Je moet begrijpen wat je vraagt en wat je terugkrijgt”, vat Grosch samen. “AI is geen magische oplossing. Maar wanneer je het juist inzet, werkt het als een versneller voor alles wat je als ontwikkelaar al kon.”

WANNEER AI ZEKER WÉL WERKT

Bij het genereren van standaardcode, het bouwen van eenvoudige API’s, het opzetten van prototypes, het aanvullen van documentatie, het analyseren van externe code en bij taken met snelle feedbackcycli, zoals frontendontwikkeling en unit testing.

WANNEER AI (VAAK NOG) NIET WERKT

Bij complexe of volwassen codebases, architecturen met veel afhankelijkheden, grootschalige refactorings, domeinspecifieke logica, beveiligingskritische software en lange buildcycli waarbij foutdetectie traag verloopt.

GENERATIEVE AI EN LEGACYSOFTWARE

NIEUWE MOGELIJKHEDEN VOOR SOFTWARE-ONDERHOUD

Legacy en AI zijn de twee termen die prominent opduiken in het onderzoek van SAI.BE over softwareontwikkeling. Waar legacycode lange tijd werd gezien als een noodzakelijk kwaad – de digitale erfenis die bedrijven draaiende houdt maar ontwikkelaars doet zuchten – krijgt het nu onverwacht gezelschap van generatieve AI. Deze ogenschijnlijk tegenstrijdige werelden blijken een krachtige combinatie te vormen.

Legacysoftware vormt de ruggengraat van kritieke systemen in sectoren van gezondheidszorg tot financiën. Het onderhoud van deze systemen groeit echter uit tot een complexe uitdaging die veel middelen opslokt.

Softwareonderhoud neemt momenteel het grootste deel van de ontwikkelingscycli in beslag. Gartner voorspelt dat **technical debt in 2025 verder zal oplopen en IT-budgetten onder druk zet**. In bepaalde domeinen, zoals de productie van medische apparatuur, is legacysoftware cruciaal voor functionaliteit en veiligheid, maar tegelijkertijd moeilijk te onderhouden. “Het is niet alleen een technisch probleem, maar heeft een directe invloed op de innovatie en het concurrentievermogen van bedrijven”, aldus Joe Reynolds, data scientist bij Capgemini Engineering.

HYBRIDE AANPAK MET AI

Een **veelbelovende ontwikkeling is de combinatie van LLM’s met traditionele analysetools**. Deze hybride aanpak koppelt modellen zoals GPT-4 en Code-Llama aan graph databases en Abstract Syntax Trees (AST). Hierdoor wordt het mogelijk architectuurdiagrammen te genereren uit broncode, UML-diagrammen te creëren en codepatronen in natuurlijke taal te interpreteren.

Deze technologie kan de dagelijkse werkzaamheden van software engineers veranderen. In plaats van uren door code te zoeken, kunnen engineers specifieke vragen stellen over de relaties tussen componenten. Het systeem interpreteert de vraag, doorzoekt relevante informatie en presenteert resultaten in een leesbaar formaat.

PRAKTISCHE IMPACT

- Reductie van kosten en tijd voor het onderhoud van legacysoftware
- Verlenging van de levensduur van kritieke softwaresystemen
- Overbrugging tussen oude codebases en moderne innovaties
- Toegankelijker maken van complexe code

TECHNISCHE ONTWIKKELINGEN

- Natural language querying van codebases
- Automatische generatie van architectuurdiagrammen
- Realtime code-analyse met LLM’s en graph databases
- Hybride systemen die AI combineren met traditionele tools

Joe Reynolds, data scientist bij Capgemini Engineering.

RISICO'S EN VEILIGHEIDSOVERWEGINGEN

De statistische aard van LLM's brengt risico’s met zich mee, vooral in kritieke sectoren zoals de zorg. AI-modellen kunnen soms ‘hallucineren’ of onjuiste informatie genereren. Daarom zijn veiligheidsmaatregelen en menselijke controle essentieel. **Organisaties die deze technologie gebruiken, moeten rekening houden met gegevensbeveiliging, mogelijke AI-bias en de impact op werknemers.**

De combinatie van gen AI met traditionele software-engineeringtools kan de manier waarop organisaties omgaan met legacysystemen fundamenteel veranderen.

Een voorbeeld van een praktische toepassing is het Renaissance-project van Capgemini Engineering, TNO-ESI en Philips. Dit project werkt aan uitbreiding voor meerdere programmeertalen, AI-ondersteunde code-refactoringtools en geautomatiseerd testen. “We vervangen ingenieurs niet, maar vergroten hun capaciteiten en nemen hen routinematig werk uit handen, zodat zij zich kunnen concentreren op meer creatieve taken”, benadrukt Reynolds.

Kortom, de combinatie van generatieve AI met traditionele software-engineeringtools kan de manier waarop organisaties omgaan met legacysystemen fundamenteel veranderen. Deze ontwikkeling maakt decennia aan software-intelligentie toegankelijker via natuurlijke taal en kan complexe codebases begrijpelijker maken voor een bredere groep professionals.

VAN COBOL TOT CHATBOT

SD WORX MODERNISEERT KENNISMANAGEMENT ZONDER SYSTEMEN TE VERVANGEN

SD Worx, Europa's grootste aanbieder van payroll- en HR-diensten, heeft na tachtig jaar van softwareontwikkeling een bibliotheek van meer dan 100.000 documenten opgebouwd. Van complexe enterprisesystemen van twintig jaar of ouder, tot recente .NET-applicaties: elk systeem komt met zijn eigen documentatie, juridische notities en technische specificaties.

Door veranderende wetgeving in meerdere landen werd het vinden van relevante informatie een tijdrovende puzzel. "De vraag was: hoe kunnen we onze oplossingen begrijpelijk en gemakkelijk onderhoudbaar maken voor huidige en toekomstige ontwikkelteams?", verklaart Patrick Maes, program manager bij SD Worx.

INTELLIGENT VIRTUAL ASSISTANT

In samenwerking met technologiepartner AE ontwikkelde SD Worx een **meertalige Intelligent Virtual Assistant genaamd ASKME, die gegevens uit meerdere bronnen kan scannen en indexeren**. Medewerkers kunnen vragen stellen in natuurlijke taal en ontvangen beknopte antwoorden met verwijzingen naar de onderliggende documenten. De virtuele assistent houdt rekening met de juridische context en regelgevingsupdates, cruciaal voor een nauwkeurige compliance. ASKME bevindt zich in een gevorderde testfase waarbij verschillende teams geleidelijk toegang krijgen.

De resultaten zijn meetbaar: minder tijd besteed aan zoeken naar documentatie, verkort inwerken van nieuwe medewerkers en verbeterde compliance. De case toont hoe legacymodernisering niet altijd betekent dat oude systemen volledig vervangen moeten worden. Soms volstaat het om de toegang tot bestaande kennis te verbeteren.

Patrick Maes, program manager bij SD Worx: "We willen onze oplossingen begrijpelijk en gemakkelijk onderhoudbaar maken voor huidige en toekomstige ontwikkelteams."

Aikido is een Europese speler die bedrijven van bij de ontwikkeling helpt hun software en cloudinfrastructuur veilig te maken. Het bedrijf won op Cybersec Europe de Cybersec Award voor Best Cybersec Innovation Europe. Recent, op VivaTech in Parijs, selecteerde de Franse president Emmanuel Macron Aikido als een van de zes Europese start-ups die hij persoonlijk wilde ontmoeten. De markt voor code- en cloudbeveiliging wordt wereldwijd beheerst door Amerikaanse en Israëlische spelers.

SECURITY VOOR ONTWIKKELAARS

“HET CRYWOLF-EFFECT IS VAAK NEFAST”

In de wereld van softwareontwikkeling is security niet langer het sluitstuk van het traject, maar een cruciaal onderdeel van het ontwikkelproces zelf. Dat is precies waar het Belgische Aikido Security zich positioneert.

De jonge scale-up kent een duizelingwekkende groei. “We zijn van 20 naar bijna 100 medewerkers gegaan op ongeveer een jaar tijd”, zegt Johan De Keulenaer, head of partnerships. “We hebben mensen in Brazilië, Singapore en Roemenië. We zijn dus echt een internationaal team geworden.”

Aikido mikt op een fundamenteel andere aanpak van security tooling: *developer first*. “**Traditionele securitytools richten zich op de CISO of het securityteam**”, vertelt De Keulenaer. “Die kiezen een oplossing en die arme developer moet die dan maar gebruiken. Wij keren dat om: de developer is voor ons zowel de gebruiker als de koper.” Dat uitgangspunt vertaalt zich in tooling die integreert in de dagelijkse workflow van de programmeur – denk aan integraties met editors als Visual Studio Code of PyCharm, waar kwetsbaarheden tijdens het coderen zichtbaar worden.

VALSE MELDINGEN

Security moet een bondgenoot zijn voor ontwikkelaars, vult Berg Severens, AI-engineer bij Aikido, aan. “Zeker voor kmo’s, onze oorspronkelijke doelgroep, die vaak geen dedicated securityteam hebben.” In plaats van losstaande tools voor dependency scanning, license compliance of static code analysis, biedt Aikido een geïntegreerd platform met een brede scope – van third-party package monitoring tot AI-ondersteunde code-analyse.

Het doel: ontwikkelaars niet alleen waarschuwen, maar ook ondersteunen. “Als een fout zich voordoet, bieden we een autofix aan waar dat mogelijk is”, aldus De Keulenaer. “Maar minstens even belangrijk is dat we proberen het aantal **false positives** drastisch te reduceren.” Want dat leidt tot wat Severens het *crywolf-effect* noemt: “Als een developer te vaak valse meldingen krijgt, gaat hij echte problemen ook negeren. Dat is niet alleen vervelend, maar ronduit gevaarlijk.”

Berg Severens (links) en Johan De Keulenaer van Aikido.

WANNEER ÉÉN VALLENDE IT-PARTNER ALLES OMVERWERPT

DIGITALE DOMINO'S IN JE SUPPLY CHAIN

Supplychainaanvallen zijn een klassieke, maar steeds vaker voorkomende tactiek, waarbij cybercriminelen de zwakste schakel in je vertrouwensketen uitbuiten. Terwijl IT-teams hun eigen infrastructuur steeds beter beveiligen, verschuift het aanvalsoppervlak naar de zwakste schakels in de digitale keten. Vier vragen en drie praktijkcases.

1/ WAAROM KOMT SUPPLYCHAINBEVEILIGING OPZETTEN?

In het verleden lag de focus vooral op het uitbuiten van vertrouwensrelaties, waarbij aanvallers minder beveiligde leveranciers gebruikten als opstapje naar grotere, waardevollere doelen.

"Vandaag brengt vooral de softwaretoeleveringsketen grote risico's met zich mee", argumenteert Nathalie Claes, externe CISO en DPO en auteur van het boek *Gehackt, wat nu?*. "In onze digitale economie bouwen we software niet meer vanaf de basis; we leunen sterk op kant-en-klare componenten zoals API's van derden, open-sourcecode en producten van softwareleveranciers. Elk van deze bouwstenen kan een achterdeur voor aanvallers bevatten."

Een slimme hacker kan deze toegangspunten gebruiken om schadelijke code in jouw systemen te sluizen, die niet alleen jouw infrastructuur kan infiltreren, maar ook die van jouw klanten – met mogelijk verwoestende gevolgen. "Terwijl digitale aanvallen al zorgwekkend genoeg zijn, moeten we ook alert zijn voor aanvallen die fysieke hardware betreffen. Zelfs de apparatuur die we dagelijks gebruiken kan een Trojaans paard worden."

2/ WAT IS DE STRATEGIE ACHTER SUPPLYCHAINAANVALLEN?

De basisstrategie achter een supplychainaanval is om een zwak punt binnen de keten te identificeren – zoals een klein bedrijf met minder strenge beveiligingsprotocollen – en dat als springplank te gebruiken om dieper in de netwerken van andere en grotere organisaties te infiltreren. Eens binnen is het kwaad geschied. “Dan kunnen de aanvallers schadelijke software verspreiden, gevoelige informatie stelen, of andere destructieve acties ondernemen die de betrouwbaarheid en de veiligheid van de hele keten in gevaar brengen.”

Twee elementen spelen mee. Enerzijds zijn hedendaagse toeleveringsketens best complex, anderzijds is er het vertrouwen dat eraan verbonden is. “Dat maakt ze kwetsbaar voor dit soort aanvallen. En net omdat de gevolgen enorm kunnen zijn, wordt de beveiliging van de supply chain een prioriteit voor organisaties wereldwijd.”

3/ WAT ZIJN VAAK VOORKOMENDE DOELWITTEN?

Een veelvoorkomend doelwit binnen de toeleveringsketen zijn volgens Nathalie Claes de Managed Service Providers (MSP’s), de partijen die we vertrouwen voor essentiële netwerk- en onderhoudsdiensten. “Zij hebben diepgaande toegang tot onze systemen, wat geweldig is voor de efficiëntie, maar ook een gouden kans biedt voor aanvallers. Als een MSP-beveiliging tekortschiet, kan een hacker zich gemakkelijk door de digitale achterdeur van je bedrijf wurmen.”

Nog een verontrustende methode is, volgens haar, de aanval op de softwareontwikkelingsprocessen, specifiek de CI/CD-pijplijn, die staat voor continue integratie en continue levering. “Deze pijplijnen helpen om software snel en efficiënt te ontwikkelen en uit te rollen. Maar als cybercriminelen deze processen infiltreren, kunnen ze stiekem schadelijke code insluiten. Wanneer de aangetaste software dan jouw systemen bereikt, ben je onbewust al gecompromitteerd.”

4/ EN… WAT KUN JE ERTEGEN DOEN?

Binnen je organisatie is het alvast van groot belang om per afdeling in kaart te brengen welke software en leveranciers gebruikt worden. “Vervolgens moet je voor deze leveranciers een goede supplier assessment doen en peilen naar de manier waarop ze met informatieveiligheid en GDPR omgaan.”

Een proactieve aanpak is essentieel om de fundamenten van jouw bedrijf te beschermen. “Robuuste beveiligingsmaatregelen opzetten binnen je toeleveringsketen is geen eenmalige taak, maar een doorlopend proces van monitoring, aanpassing en samenwerking met je leveranciers.”

“Supplychainbeveiliging is een doorlopend proces van monitoring, aanpassing en samenwerking met je leveranciers.”
Nathalie Claes, CEO van cybersecurityadviseur Dadir, externe CISO en DPO en auteur van het boek *Gehackt, wat nu?*

CASE 1
ATLASSIAN SUPPLYCHAINAANVAL: INBRAAK VIA SSO

In 2021 werd Atlassian, een groot softwarebedrijf bekend om zijn samenwerkingstools zoals Jira en Confluence, getroffen door een geraffineerde supplychainaanval. Deze aanval richtte zich specifiek op de Single Sign-On-functionaliteit (SSO), die gebruikers met één enkele login toegang geeft tot meerdere diensten en applicaties.

Hackers richtten hun aandacht niet direct op Atlassian zelf, maar op een kleiner bedrijf dat onderdelen of diensten leverde aan Atlassian. Dit bedrijf was een schakel in de zogenaamde supply chain van Atlassian.

Door zwakheden uit te buiten in de beveiliging van dit kleinere bedrijf, **slaagden de hackers erin om hun eigen kwaadaardige code in te voegen in de software** die uiteindelijk bij Atlassian terechtkwam. Deze code was ontworpen om zich te vermommen als normale, veilige software. Toen Atlassian de besmette software ontving en installeerde, was de kwaadaardige code actief zonder dat iemand dat doorhad. De code was specifiek ontworpen om de SSO-functionaliteit te misbruiken.

Met controle over de SSO-functionaliteit konden de hackers potentieel toegang krijgen tot de inloggegevens van gebruikers die zich aanmeldden bij Atlassians diensten. Dat betekent dat als **een gebruiker inlogde, de hackers de mogelijkheid hadden om die inloggegevens te onderscheppen** en te gebruiken voor verdere aanvallen of om gevoelige informatie te stelen.

Toen de inbreuk werd ontdekt, reageerde Atlassian snel: het beveiligingslek werd gedicht, getroffen systemen werden hersteld en klanten werden geïnformeerd over de potentiële risico's.

CASE 2
OKTA: PERSOONLIJKE ACCOUNT EN HAR-BESTANDEN

Op donderdag 19 oktober 2023 rapporteerde Okta, een toonaangevende leverancier van diensten voor identiteits- en authenticatiebeheer, een beveiligingsincident. Digitale inbrekers hadden weken ervoor stiekem **toegang gekregen tot gevoelige bestanden in het klantondersteuningssysteem van Okta**. Hoewel minder dan 1% van alle klanten getroffen werd, was de impact aanzienlijk.

Deze gehackte bestanden bevatten zogenaamde HAR-bestanden, speciale logbestanden waarin sessietokens kunnen zitten. "Denk aan sessietokens als de tijdelijke sleutels die je toegang geven tot je account zonder dat je opnieuw je wachtwoord moet invoeren", stelt Nathalie Claes. "Slimme hackers hebben deze sessietokens gebruikt om zich voor te doen als legitieme gebruikers van vijf Okta-klanten, waardoor ze konden binnendringen in hun sessies en mogelijk gevoelige acties konden uitvoeren."

De oorzaak? Een Okta-medewerker had zijn inloggegevens voor het klantondersteuningssysteem opgeslagen in zijn persoonlijke Google-account. Toen dat **persoonlijke account gecompromitteerd werd**, lagen ook de sleutels van het klantensysteem van Okta voor het grijpen. Dit incident toont, volgens Nathalie Claes, de beveiligingsimpact van een kleine fout, zoals het opslaan van werkgerelateerde inloggegevens in een persoonlijke account. "Het is een scherpe herinnering aan het belang van het scheiden van werk en privé, vooral als het gaat om de bescherming van gevoelige informatie."

CASE 3
POSTMAN: CLOUDAPPLICATIE ZET DEUR OPEN

Geen voorbeeld van een aanval, maar wel van een risico dat te vaak over het hoofd wordt gezien. “Ik merk, ook bij mijn klanten, dat er **nog te los wordt omgesprongen met verschillende leveranciers**”, oppert Nathalie Claes.

In online tijden kun je allerlei tooltjes, al dan niet gratis installeren. Maar dat maakt het moeilijk om je volledige supply chain in kaart te brengen en te houden. “Een goed voorbeeld dat ik bij een klant tegenkwam, was het gebruik van Postman. Postman is een tool voor het testen en ontwikkelen van API’s. Het biedt ontwikkelaars een eenvoudige manier om HTTP-verzoeken te versturen, antwoorden te ontvangen, en API’s te debuggen en te documenteren.”

In mei 2024 veranderde Postman zijn werking: voor veel functies schakelde het over naar een cloud-only model. . “Daardoor geven de zelfbeheerde Postman-accountgegevens van een gebruiker nu **toegang tot alle productiegeheimen die ze hebben gebruikt**. Dat ondermijnt de scheiding van identiteit bij het beheren van productiebronnen in je organisatie”, vertelt ze. “Daarom hebben we bij de klant het gebruik van Postman verboden, maar dat konden we alleen doen omdat we wisten dat het werd gebruikt.”

CONCRETE STAPPEN VOOR BETERE SUPPLYCHAINBESCHERMING

In haar boek *Gehackt, wat nu?* somt Nathalie Claes enkele concrete stappen en tips op die je kunt gebruiken om de beveiliging van je toeleveringsketen te versterken:

1. **Prioriteer belangrijke assets.** Identificeer en beveilig essentiële gegevens, systemen en activa.
2. **Ken je netwerk.** Houd een actuele lijst van leveranciers bij en evalueer hun beveiligingsmaatregelen regelmatig.
3. **Monitor en evalueer.** Voer regelmatig beveiligingsaudits en controles uit.
4. **Versterk partnerschappen.** Bouw sterke relaties met leveranciers om samenwerking en vertrouwen te bevorderen.
5. **Eis compliance.** Zorg dat beveiligingsvereisten contractueel worden afgedwongen, ook bij onderaannemers.
6. **Communiceer effectief.** Maak je beveiligingseisen duidelijk aan alle leveranciers en zorg voor regelmatige updates.
7. **Onderwijs en train.** Verhoog het veiligheidsbewustzijn door regelmatige trainingen.
8. **Zorg voor een responsplan.** Ontwikkel en test een effectief incidentresponsplan.

Gehackt, wat nu? - Bescherm je bedrijf tegen cybercriminelen, Nathalie Claes, 2025, 160 pagina's, 9789463838351

» *Beluister **hier** ook de aflevering van SAI.NT, de podcast van SAI, met Nathalie Claes.*

"Microsoft wordt strenger in gebruik van protocollen als SPF, DKIM en DMARC. Met als gevolg dat mails vaak sneller in de spamfilter terechtkomen. Of soms zelfs vroeger worden afgeblokt."

E-MAILPROTOCOLLEN ALS EERSTE VERDEDIGINGSLINIE TEGEN PHISHING

De drempel voor het ontvangen en versturen van e-mail verhoogt. Dit komt omdat Microsoft vanuit zijn mailservers bestaande protocollen zoals SPF en DKIM gaat opleggen. Gebruiken we die protocollen al? En hoe zit dat technisch in elkaar?

Simple Mail Transfer Protocol (SMTP) is de facto de standaard voor het versturen van e-mail over het internet. "Het voordeel van SMTP is dat het, zoals de naam doet uitschijnen, eenvoudig is. Het nadeel is dat je je perfect kunt voordoen als een andere afzender", zegt security-specialist Jan Guldentops.

Dit is waar DMARC, DKIM en SPF in beeld komen. Deze technologieën spelen een belangrijke rol in het verbeteren van de betrouwbaarheid en het vertrouwen van e-mailcommunicatie.

1/ WAT DOEN DMARC, DKIM EN SPF?

SPF (Sender Policy Framework) is een e-mailauthenticatietechnologie die controleert of e-mails worden verzonden vanaf geautoriseerde servers die zijn geassocieerd met het domein van de afzender. "Domeineigenaren kunnen SPF-records toevoegen aan hun DNS-instellingen om een lijst met geautoriseerde servers te specificeren die gemachtigd zijn om e-mails namens hun domein te verzenden", vertelt Jan Guldentops. "Een soort van white listing voor e-mail dus."

DKIM (DomainKeys Identified Mail) is een mechanisme waarmee de ontvanger van een e-mail kan verifiëren dat de e-mail is verzonden en geautoriseerd door de eigenaar van het verzendende domein. Dit wordt gedaan door een soort van digitale handtekening toe te voegen aan de header van de e-mail. “Het is een uitbreiding van SPF, maar bij veel organisaties en hun mailserver is het niet correct ingesteld. Hier zal Microsoft dus strenger op worden.”

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is ten slotte protocol dat ontworpen is om e-mailauthenticatie en rapportage toe te passen op berichten die worden verzonden vanuit een bepaald domein. Met DMARC kan een domeineigenaar aangeven welke actie moet worden ondernomen als een ontvangen e-mail niet voldoet aan de authenticatievereisten. “Het dient voor rapportering”, aldus Jan Guldentops.

Doordat Microsoft strenger wordt in gebruik van protocollen als SPF, DKIM en DMARC zal dit voor velen een impact hebben. “Met als gevolg dat mails vaak sneller in de spamfilter terechtkomen. Of soms zelfs vroeger worden afgeblokt.”

2/ FUNDAMENTELE E-MAILSECURITY KORT UITGELEGD

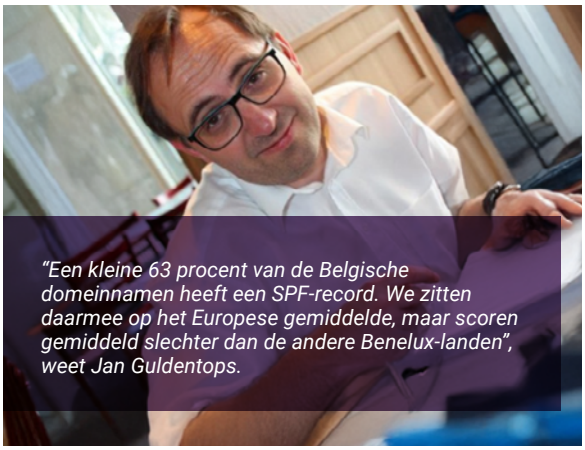
De sterkte en de zwakte van e-mailverkeer is het protocol dat er onder de motorkap zit. “Simple Mail Transfer Protocol (SMTP) is zo eenvoudig dat ik het uit mijn hoofd kan schrijven”, weet Guldentops.

```
nc ASPMX.L.GOOGLE.COM 25
HELO sai.be
MAIL FROM: <j@ba.be>
RCPT-TO: <william@sai.be >
DATA  mijn boodschap
From: Jan Guldentops
Subject: Dag William

Boodschap
.
```

Daardoor wordt het een succes en vervangt het stap voor stap alle andere protocollen en systemen, waardoor er een wereldwijd bruikbaar e-mailsysteem ontstaat. “Maar elk voordeel heeft zijn nadeel: in het protocol zit eigenlijk geen enkele beveiliging tegen vervalsingen en misbruik: als ik als `MAIL FROM: president@whitehouse.gov` invoer dan denkt onze hoofdredacteur dat hij mail krijgt van de man in het Witte Huis. Het resultaat? De problemen die we vandaag kennen: realistische phishing en vooral spam. Heel veel spam.”

Monty Python, zo oppert Guldentops, mag er dol op zijn maar het maakte op een bepaald moment e-mail onbruikbaar. Men moest een gemakkelijk, open en haalbaar



“Een kleine 63 procent van de Belgische domeinnamen heeft een SPF-record. We zitten daarmee op het Europese gemiddelde, maar scoren gemiddeld slechter dan de andere Benelux-landen”, weet Jan Guldentops.

mechanische verzinnen om ervoor te zorgen dat niet iedereen als om het even wie kon mailen. “Dit is gedeeltelijk opgelost door het Sender Policy Framework (SPF) uit te werken. Aan het domein (bijvoorbeeld sai.be) wordt een tekst-record meegegeven van welke IP’s mail mogen sturen voor een bepaald domein.” De ontvangende mailserver kan dit dan snel en goedkoop controleren door dit record op te zoeken:

```
sai.be descriptive text "v=spf1 include:spf.mailjet.com include:_spf.google.com include:eu.mailgun.org include:sendgrid.net ip4:191.233.94.144 ~all"
```

Dit toont de IP-adressen, de mailservers en alles van google.com (lees Google Workspace) mag mail sturen. “De `~all` leert ons dat het niet strikt moet toegepast worden. SAI.BE gebruikt ook mailgun.com om mails (vermoedelijke mailinglists) te sturen. Beter is -all te gebruiken: dan worden e-mails die niet aan het SPF-record voldoen, expliciet geweigerd door de ontvangende mailservers.”, aldus Guldentops. “Een opvallend IP is `191.233.94.144`. Dat blijkt van Microsoft Brasil te zijn… Een interessant IP om verder te onderzoeken. Met SPF-records kun je een aanvaller heel veel vertellen over waar je infrastructuur zit. Het SPF-record van roularta.be geeft ons alle IP’s die ze gebruiken, een handig lijstje voor wie een DDOS-aanval plant.”

```
roularta.be descriptive text "v=spf1 a mx ip4:78.29.236.95 ip4:91.212.185.178 ip4:91.212.185.176 ip4:37.58.40.58 ip4:37.58.40.61 ip4:91.233.206.11 ip4:85.17.220.128/27  include:servers.mcsv.net include:spf.protection.outlook.com include:e.my-crm.io include:spf.icontroller.eu -all"
```

DKIM (DomainKeys Identified Mail) voegt public/private key-authenticatie toe aan SPF. “Je mailserver heeft een public/private key aangemaakt. Elke uitgaande e-mail heeft een digitale handtekening in de header van dezelf-

de mail", legt hij uit. "De ontvanger of zijn mailserver kan dan via een DNS-record de publieke key opvragen en met deze publieke key checken of de digitale handtekening klopt. Op die manier weet je ook zeker dat er *en cours de route* niks veranderd is aan de boodschap zelf." Dit is niet alleen een belangrijke stap tegen spam, maar ook voor de authenticiteit van de boodschap. Het voorkomt later wijzigen of *on the fly* aanpassen van e-mails.

In DNS worden selectors toegevoegd:

```
host selector2._domainkey.vlaanderen.be
selector2._domainkey.vlaanderen.be is an
alias for selector2-vlaanderen-be._domain-
key.vlaamseoverheid.onmicrosoft.com.

host -t txt selector2-vlaanderen-be._
domainkey.vlaamseoverheid.onmicrosoft.com

selector2-vlaanderen-be._domainkey.vlaam-
seoverheid.onmicrosoft.com descriptive text
"v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBA-
QUAA4GNADCBiQKBgQDVFhcpZq8RoXSqEL5aYPUHE-
vP6LdHsFwLnld2zSBtQUasJ6dPg2dxlfHK6uAIyN-
DvidfvycrFAEwYpMPZjvnSrvg+U2OtaDpknyY3iE-
hkKC6/94oeeB+5Uf20TsNoMmxs/FVGpPbbO5DGsh/
eeA23umrNgZ82qdPT140GMpfmkvQIDAQAB;"
```

Deze bevatten dan de public key waarmee je in de header de integriteit kunt checken.

```
DKIM-Signature: v=1; a=rsa-sha256; c=re-
laxed/relaxed; d=vlaanderen.be;
 s=selector2;
 h=From:Date:Subject:Message-ID:Con-
tent-Type:MIME-Version:X-MS-Exchange-Sen-
derADCheck;
 bh=IA1YotnjqjTLUop2j5TkkL7G9j5rwAAl-
S3I9ckvvBtk=;
 b=xjd91St36JXlVm9CiK6GOmFWkuVyOF6RFbgbO-
FifvPeu5YWfhaOAjgjYZ4j3RXc2jJGmHtCz2SCkP-
qCQMELMw9aXTuO9IUMqlI5s1O4GD5o7ELSeCpoR-
38PuUNOF3Yc20+5gns7cm23NckDtQmM3zBN6f-
G78mctLkQZPkI63pfc=
```

Last but not least hebben we nog een DMARC-record (Domain-based Message Authentication, Reporting, and Conformance) dat uitlegt aan wie geweigerde e-mails van je domein moeten gerapporteerd worden.

```
host -t txt _dmarc.sai.be
_dmarc.sai.be descriptive text "v=DMARC1;
p=none; rua=mailto:operationeel@sai.be;
ruf=mailto:operationeel@sai.be"
```

Zo kun je als beheerder weten wie je domein aan het misbruiken is.

Take-away: zorg dat deze drie elementen perfect in orde zijn voor je domeinen of sommige correspondenten zullen je e-mail niet meer te zien krijgen, raadt Guldentops aan. "Doe het zelf of zoek hulp."

3/ GEBRUIK VAN DMARC EN SPF IN BELGIË

Via het CYSSME-consortium, met de steun van Europa, kunnen we statistieken opbouwen van hoeveel deze veiligheidsmechanismes worden gebruikt. "We hebben een lijst van domeinnamen per land samengesteld en testen structureel of ze een SPF en DMARC-record hebben en of die correct ingesteld is", stelt Guldentops.

Belgische cijfers tonen aan dat 62,67 procent van de Belgische domeinnamen een SPF-record hebben. We zitten daarmee op het Europese gemiddelde van 62,65 procent maar scoren gemiddeld slechter dan de andere Benelux-landen waar gemiddeld 70 procent van de domeinen een SPF-record heeft.

Als we beter gaan kijken hoe goed dit record is opgesteld, zien we dat maar 23 procent strikte instructies geeft voor zijn of haar domein (-all), waar we boven het Europees gemiddelde van 17 procent zitten.

Met DMARC is het slechter gesteld: maar 26,59 procent van de Belgen heeft een DMARC-record ingesteld. Slechts een kwart van de bedrijven is dan ook op de hoogte dat zijn domein misbruikt wordt voor bijvoorbeeld phishing of spam. Ook hier halen we het Europees gemiddelde, maar scoren we slechter dan Luxemburg en vooral Nederland.

ADOPTIEPERCENTAGES PER BEVEILIGINGSSTANDAARD (GESELECTEERDE REGIO'S EN LANDEN)

Regio/land	DMARC (%)	SPF (%)	Strikte SPF (%)
België (be)	26,59	62,67	23,02
Nederland (nl)	47,65	72,77	22,25
Luxemburg (lu)	27,62	69,79	28,84
Benelux	43,28	70,75	22,47
Europa (totaal)	25,93	62,65	18,21
Best scorende landen	Andorra (42,17)	Griekenland (78,09)	Oostenrijk (36,38)
Slechtst scorende landen	Zweden (10,49)	Zweden (37,99)	Hongarije (10,12)

Data mei 2025 (DMARC, SPF, IPv6).

OPVALLENDE QUOTES

“De Europese Unie zorgt ervoor dat wij een druk bestaan hebben.”

Jeremy Rollison, Head of EU Policy bij Microsoft, tijdens zijn presentatie op de Main Stage van Cybersec Europe in Brussel.

“We hebben het geluk dat we zeer slechte concurrenten hebben. SAP, Microsoft Dynamics, Oracle: allemaal grote bedrijven, maar ze zijn traag en leveren echt shit af.”

Fabien Pinckaers, CEO Odoo, in De Tijd.

“My kids will never be smarter than AI.”

Sam Altman, CEO OpenAI, in Business Insider.

“We zijn hier niet op kamp, hè.”

Reactie van werkgever toen Geert Van Steyvoort (intussen Infrastructure Project Leader) in zijn vorige job – een IT-functie zonder klantcontact – op een warme zomerdag in korte broek kwam werken (via LinkedIn).

“Cybersecurity needs a clearly defined leader that has the power to lead. Anything less is doomed to failure.”

Thom Langford, CTO EMEA van Rapid7, op Help Net Security.

“AI is geen spaghetti. Je gooit het niet tegen de koelkast om te zien of het werkt.”

Lynn Martin, voorzitter NYSE Group, adviseert bedrijven om voor AI vast te houden aan hun kernprincipes (op de Snowflake Summit).

“Als Donald Trump boos op je is, kan Microsoft je zonder problemen uit zijn clouddiensten kicken.”

Arjen Lubach in een aflevering van zijn satirisch programma Lubachs Diep Duik Donderdag.

VOLGENDE EVENTS VOOR SAI.BE

30 JUN 2025
Online – 13.00 – 13.30
SAI SHORTS - SECURITY
*Meer info vind je **hier***

1 JUL 2025
Online – 13.00 – 13.30
SAI SHORTS - LEGAL & COMPLIANCE
*Meer info vind je **hier***

2 JUL 2025
Online – 13.00 – 13.30
SAI SHORTS - CLOUD & INFRA
*Meer info vind je **hier***

3 JUL 2025
Online – 13.00 – 13.30
SAI SHORTS - SOFTWARE DEV
*Meer info vind je **hier***

4 JUL 2025
Online – 13.00 – 13.30
SAI SHORTS - EMERGING TECH
*Meer info vind je **hier***

7 JUL 2025
Online – 13.00 – 13.30
SAI SHORTS - DATA & AI
*Meer info vind je **hier***

8 JUL 2025
Online – 13.00 – 13.30
SAI SHORTS - ARCHITECTURE
*Meer info vind je **hier***

6 10 OKT 2025
Partner event
DEVOXX
*Meer info vind je **hier***

22 OKT 2025
Partner event
ANNACON
*Meer info vind je **hier***

4 DEC 2025
12.30 – 21.00 uur
SAI RESET IT 2025
SQUARE Brussels
*Meer info vind je **hier***

VOOR NIEUWE EVENTS:
NEEM ZEKER EEN KIJKJE
OP **WWW.SAI.BE**

Beluister ***hier*** ook de extra edities van **SAI.NT, de podcast van SAI.BE.** De SAI.NT-podcast bespreekt de laatste thema's en actualiteit binnen het IT- en technologielandschap.

ADVERTEREN IN SAI UPDATE?

Stuur een mail naar
communicatie@sai.be

INTERESSE IN ONS PRIJSVOORDELIG LIDMAATSCHAP?

Kijk op **www.sai.be/pagina/lidmaatschap/**

Voor de bestaande leden: de meldingen voor het vernieuwen van het SAI.BE-lidmaatschap zijn begin november uitgestuurd. **Aarzel niet om uw lidmaatschap te verlengen en ook nieuwe SAI.BE-leden zijn uiteraard altijd welkom.**

COLOFON

Werkten mee aan dit nummer: William Visterin (coördinatie), Robin Van den Bogaert, Jan Guldentops, Stef Gyssels 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