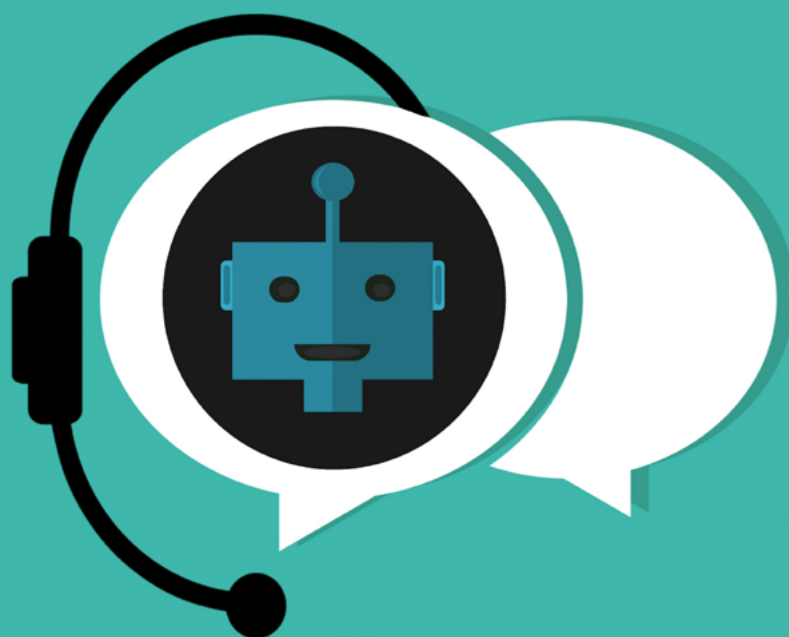


WELKOM IN HET TIJDPERK VAN AMBIENT COMPUTING

WAAROM CHATBOTS KOMEN OPZETTEN
EN HOE ZIT DAT TECHNOLOGISCH?

pag. 11



INTERVIEW
JACQUES VANDENBULCKE

pag. 8



ACHTERGROND
WIE WIL VANDAAG CISO ZIJN?

pag. 19



SAI QUIZ
DOE MEE EN WIN!

pag. 10

EDITO

Beste SAI lid en lezer,

Het is een groot genoegen u te mogen verwelkomen bij dit eerste eigen magazine in de geschiedenis van SAI.

Op basis van een grondige analyse van de inhoud en vormgeving van het vorige magazine én op basis van de commentaren van diverse leden, heeft de raad van bestuur van SAI eind vorig jaar beslist om het heft in eigen hand te nemen en een eigen kwaliteitsvol magazine te maken in lijn met de inhoud en de verwachtingen van SAI en SAI-leden. Uiteraard kijken we uit naar uw commentaar en suggesties om de volgende SAI-magazines nog beter te maken.

In dit magazine kan u een gesprek lezen met Prof. Dr. Jacques Vandebulcke die na 42 jaar de fakkel heeft doorgegeven aan een enthousiast team om SAI verder te ontwikkelen. Zijn energie, netwerk en focus voor SAI vanaf de oprichting heeft SAI gebracht waar het vandaag staat en dat is een meer dan uitzonderlijke prestatie die enorm gewaardeerd wordt in de Vlaamse en Brusselse IT wereld. Zijn bijdrage via SAI aan het opleiden en informeren van letterlijk duizenden mensen op het gebied van informatiewetenschap mag legendarisch genoemd worden. Prof. Dr. Vandebulcke mag terecht trots zijn dat hij SAI overdragen heeft in 2020, een organisatie met meer dan 1.600 leden en in goede financiële gezondheid. Ik ben dan ook zeer verheugd dat Prof. Dr. Vandebulcke aan boord blijft als ere-voorzitter en penningmeester om het SAI team met goede raad en daad bij te staan in de komende jaren.

Het SAI team heeft tijdens de afgelopen maanden ook naar de toekomst gekeken. Informatie is één van de meest kostbare bronnen geworden in de 21ste eeuw. Als IT professionals dragen wij allen een grote verantwoordelijkheid in de ontwikkeling van elke organisatie (ook in Vlaanderen en Brussel) waarbij het succes zeer sterk afhangt van het vermogen om huidige en nieuwe IT-ideeën, processen en technologieën met huidige en nieuwe IT professionals efficiënt en effectief in te zetten. Het is hartverwarmend om de constante groei te zien tijdens de afgelopen jaren van zowel jonge pas afgestudeerden als ervaren herschoolde mannen en vrouwen die de IT-markt betreden.

Het is een zeer goede evolutie, maar het kan altijd beter. SAI zal haar verantwoordelijkheid blijven opnemen om u en alle IT professionals te blijven stimuleren in het ontdekken, bespreken en beheersen van nieuwe relevante IT-ideeën, processen en technologieën op een objectieve en pragmatische manier.



Het SAI team is er klaar voor en rekt op uw suggesties en inbreng. Intussen geniet van dit eerste SAI magazine.

Marc Vael
Voorzitter van de Raad van Bestuur SAI

INHOUD

NIEUWS | SAI FLASH
pag. 3 – 6

HOLLYWOOD-FILMS
pag. 7

INTERVIEW |
JACQUES VANDENBULCKE
pag. 8 – 9

QUIZ
pag. 10

FOCUS | CHATBOTS
pag. 11 – 17

UPDATE | WINDOWS 7
pag. 18

ACHTERGROND | CISO
pag. 19 – 23

SERVICE
pag. 24



**TECHNOLOGIE IS
HET KAMPVUUR
WAARROND WE
ONZE VERHALEN
VERTELLEN.**

LAURIE ANDERSON

PYTHON IS POPULAIRSTE PROGRAMMEERTAAL

Python is de populairste programmeertaal, gevolgd door Java en Javascript. Dat blijkt uit de Computable Index, de lijst van meest gebruikte programmeertalen die het Belgisch/Nederlandse vakblad Computable jaarlijks opstelt. De lijst kreeg begin dit jaar een nieuwe versie.

Uiteraard zijn de verschillende programmeertalen op de lijst moeilijk te vergelijken. Maar de Computable Index geeft wel een goed idee van wat er beweegt en waar ontwikkelaars de komende jaren op kunnen inzetten. De index komt voort uit zes vooraanstaande rankings, waardoor het de globale trends weergeeft.

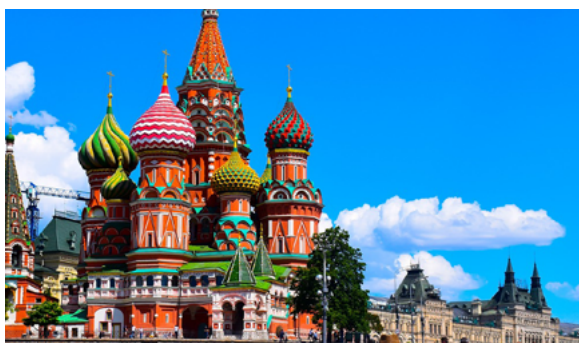
De grote vijf, samen met Python, zijn Java, Javascript, C++ en C#. Als we naar de grote groeiers kijken in de lijst, dan blijft Typescript terrein winnen. Al zijn Kotlin en Go in verhouding de grote stijgers. Bij de dalers in de Index valt Perl op, dat uit de top 20 valt. Ook PHP moet wat terrein prijsgeven.

#	Programmeertaal	Totaal	Vershil
1	Python	112	4
2	Java	111	-2
3	Javascript	107	1
4	C++	94	-4
5	C#	90	-5
6	C	89	1
7	PHP	82	-11
8	Swift	57	2
9	Ruby	50	-3
10	R	49	2
11	GO	47	12
12	Objective-C	39	-3
13	SQL	36	15
14	Shell	32	10
15	Typescript	31	10
16	Matlab	28	0
17	Assembly	21	-6
18	Scala	20	-9
19	Kotlin	20	18
20	VB.Net	15	-6

RUSLAND LEGT EIGEN SOFTWARE OP

De Russische president Vladimir Poetin verplicht vanaf 1 juli van dit jaar voorgeïnstalleerde Russische software op elke nieuwe pc, maar bijvoorbeeld ook op smart-phones en smart-tv.

Eigenlijk gaat het om een simpele verplichting die bedrijven in Rusland krijgen waardoor ze op hun toestellen



Russische software moeten installeren. Met deze beslissing moeten eigen IT-bedrijven een streepje voor krijgen in hun concurrentiestrijd met buitenlandse mogelijkheden en bedrijven. Vandaag bepalen niet-Russische leveranciers – van Apple tot Huawei – de Russische markt. En dat willen de Russische beleidsmakers graag anders zien.

BOETES

Helemaal verrassend is de actie van Poetin niet. Onlangs trad de Russische staat al op tegen Google. Van een plaatselijke rechter moest Google zijn besturingssysteem Android openstellen voor zoekmachines van zijn concurrenten zoals het Russische Yandex. De wet gaat in op 1 juli 2020. Verkopers die zich er niet aan houden, kunnen boetes tot 200.000 roebel krijgen voorgeschoteld, ongeveer 2.800 euro.

Privacy-activisten hebben echter hun twijfels bij de aankondiging. Zij benadrukken dat Poetin het toezicht en de censuur op het Russische web alleen maar verder opdrijft. Zo moesten eerder al bepaalde chat-apps zoals Telegram ook al hun encryptiesleutels ter beschikking stellen. Of moeten zoekmachines regelmatig bepaalde resultaten verwijderen.

HOE DIGITAAL IS JOUW MANAGEMENT?

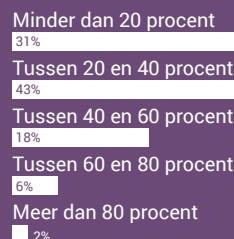
Digitale transformatie begint aan de top van een bedrijf. Maar hoe vertrouwd zijn zij zelf met technologie?

Op het event CIONext, een initiatief van CIONet, werd deze vraag gesteld aan de 1.200 deelnemers, voornamelijk CIO's en IT-managers afkomstig uit Europa (en dus ook uit ons land). En daaruit bleek

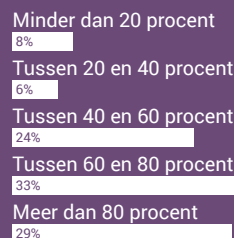
dat er nog best wel een weg is af te leggen wat betreft het 'digital savviness-gehalte' van het executive committee, zeg maar jouw directieleden, althans toch volgens de IT-mensen.



WELK PERCENTAGE VAN UW EXECUTIVE COMMITTEE IS 'DIGITALLY SAVVY'?



WAT IS VOLGENS U HET IDEALE PERCENTAGE?



WE ZOEKEN IT COLLEGA'S OM DE INNOVATIEVE BANK-VERZEKERAAR VAN MORGEN MEE VORM TE GEVEN!

100% Belgisch. Met een passie voortalent van hier. Daar maken we hier het verschil mee. Daarom investeren we niet alleen in de beste service en de meest performante producten voor onze klanten, maar ook in het welzijn van onze medewerkers. Met een open bedrijfscultuur en carrièremogelijkheden in een inspirerende werkomgeving en met opleidingen op maat. Want enthousiaste medewerkers die zich goed voelen, zijn de beste garantie voor de beste service. **Maak mee het verschil. Solliciteer vandaag nog bij Belfius.**

belfius.be/jobs

Belfius
Bank & Verzekeringen

Belfius Bank NV, Karel Rogierplein 11, 1210 Brussel - IBAN BE23 0529 0064 6991
BIC GKCCBEBB - RPR Brussel BTW BE 0403.201.185 - FSMA nr. 19649 A



TOP 10 CYBERSECURITY COMPANIES TO WATCH IN 2020

De wereldwijde uitgaven voor informatiebeveiliging en risk management zullen in 2022 goed zijn voor 174 miljard dollar, ongeveer een derde hoger dan dit jaar. Het zakenblad Forbes voorspelt tien opkomende securitybedrijven.

De cijfers over de securitymarkt komen van onderzoeksbureau Gartner. Dit jaar zal de markt, volgens het bureau, zowat 131 miljard dollar uitmaken. Van dat bedrag zal ongeveer 50 miljard dollar worden besteed aan endpoint protection.

De categorie 'application security' zal volgens Gartner 3,4 miljard uitmaken. Securitydiensten nemen evenwel de grootste hap uit het totale securitybudget. Die zijn dit jaar goed voor 66,9 miljard dollar. Het grootste groeipercen- tage vinden we in de verkoop van cloud securityplatformen en -applicaties. Die zal met meer dan 250% groeien van 636 miljoen dollar in 2020 tot 1,63 miljard in 2023.

Het zakenblad Forbes voorspelt welke tien opkomende securitybedrijven we in de gaten moeten houden (in alfabetische volgorde):

1. **Absolute** – Endpoint zichtbaarheid & controle
2. **Centrify** – Privileged Access Management (PAM)
3. **Deep Instinct** – Deep learning voor cybersecurity
4. **Kount** – Fraudepreventie op basis van artificial intelligence
5. **Infoblox** – Netwerktransformatie
6. **Mimecast** – Management van vertrouwelijke communicatie en data
7. **MobileIron** – Beheer van mobiele toestellen en applicaties
8. **One Identity** – Identity Management
9. **Securiti.ai** – Privacy compliance
10. **Transmit Security** – Identity management

» Op 23/4 organiseert SAI in Brussel een avondconferentie over 'the cyber operating model of the future'.

ZOGEZEGD

“Er zal nooit een quantum computer op uw bureau staan om teksten op te typen. Al ben ik wel voorzichtig met zo'n uitspraak. Want Thomas Watson van IBM vertelde ook ooit dat er een markt zou zijn voor hooguit vijf computers”

Koen Pellegrims
op de avondconferentie over
Quantum Computing (28/1)



VIER TRENDS DIE CLOUD-ADOPTIE IN 2020 BEÏNVLOEDEN

In alle sectoren blijft cloud computing een van de snelst groeiende segmenten van de IT-uitgaven. Maar hiermee groeit ook de verantwoordelijkheid voor CIO's en IT-afdelingen om verstandig te investeren in budgetten.

Onderzoeksbureau Gartner somt in een recent rapport vier trends op die dit jaar een impact zullen hebben op cloud-adoptie binnen dit en vier jaar.

1/ KOSTENOPTIMALISATIE ZAL CLOUD-ACCEPTATIE STIMULEREN

Tot 2024 zullen bijna alle legacy-applicaties die gemigreerd zijn als dienst (IaaS) naar de publieke cloud-infrastructuur, moeten worden geoptimaliseerd om kosteneffectiever te worden. Cloudaanbieders zullen met hun native optimalisatiemogelijkheden organisaties helpen om de meest kosteneffectieve architectuur te selecteren.

2/ MULTICLOUD ZAL VENDOR LOCK-IN VERMINDEREN

Multicloud-strategieën, het gebruik van meerdere cloud providers, zullen de afhankelijkheid van leveranciers voor twee derden van de organisaties verminderen. Dit zal echter vooral gebeuren door afspraken, en niet zozeer door application portability, de mogelijkheid om een applicatie te migreren over verschillende platformen zonder dat er veranderingen nodig zijn.

3/ GEBREK AAN CLOUD SKILLS ZORGT VOOR VERTRAGING

Onvoldoende IaaS-vaardigheden op het gebied van de cloud zullen migraties vertragen. Tot 2022 zal dit tekort de migratie van de helft van de IT-organisaties naar de cloud met twee jaar of meer vertragen. De huidige cloud-migratiestrategieën neigen meer naar 'lift-and-shift' dan naar modernisering of refactoring.

4/ DISTRIBUTED CLOUD EN MICRO-DATACENTERS KOMEN OPZETTEN

Tegen 2023 zullen de toonaangevende leveranciers van clouddiensten een gedistribueerde aanwezigheid hebben om een subset van hun diensten te bedienen. Veel aanbieders van clouddiensten investeren nu al in manieren om hun diensten dichterbij de gebruikers beschikbaar te stellen. Gartner denkt hierbij aan micro-datacenters of zelfs aan 'pop-up cloud-servicepunten', bijvoorbeeld voor sportevenementen en concerten. Of hoe de trend van edge computing zich zou doorzetten.

» Op 5/3 organiseert SAI twee avondconferenties in Antwerpen. Eentje over **cloud native architectures** en eentje over **'Hybrid Cloud: from strategy to realization'**.



CYBERSECURITY DUIDEN VIA HOLLYWOOD-FILMS

Hollywood en IT security zijn al jaren goede vrienden. In het boek 'Informatieveiligheid duiden via film' overloopt Marc Vael tien films die cybersecurity als hoofdthema hebben. "Er bestaan veel films die een goed beeld geven over de gevolgen van cybercriminaliteit."

Het boek, uitgegeven door Politeia, en met SAI, Isaca en V-ICT-OR als sponsors, schetst belangrijke security tips op basis van tien films. Die films komen uit de filmcatalogus van Marc Vael met meer dan 80 relevante films en documentaires.

Zelf ziet Vael in Hollywood twee types van cybercriminelen. "Er is enerzijds het crimineel meesterbrein, en anderzijds de meer Robin Hood-achtige figuur. Maar de meeste cybercriminelen hebben duidelijke motieven en

leggen hun plannen duidelijk uit", stelt hij. En bovendien, merkt hij op, gaat hacken in films vrij snel en eenvoudig. "Gelukkig maar, want niemand zit te wachten op een scène waarin een hacker weken bezig is om ergens binnen te raken zonder succes."

De tien films behandelen allemaal één specifiek thema rond informatiebeveiliging en cybersecurity, met telkens praktische tips en kernboodschappen voor it- en zakenmensen. Dit zijn de tien:



1. WAR GAMES
backdoor



5. OFFICE SPACE
IT-fraude door personeel



8. DUPLICITY
bedrijfsspionage



2. SNEAKERS
illegale penetratietesten



6. FIREWALL
CISO afpersing



9. SKYFALL
verlies van gevoelige data



3. THE NET
identiteitsdiefstal



7. DIE HARD 4
IoT Hacking



10. I.T.
onveilige IT outsourcing



4. ENEMY OF THE STATE
illegal surveillance



Meer info op: www.politeia.be/nl/publicaties/211755-informatieveiligheid+en+cybersecurity+duiden+via+film
Er wordt bij bij SAI later dit jaar ook nog een event met alle films ingepland

HOE SAI RUIM VIJFTIG JAAR GELEDEN BEGON ALS ELEVATOR PITCH
EN VANDAAG DUIZEND INFORMATICI VERENIGT

MILIEU EN IT-TEKORT WORDEN DÉ UITDAGINGEN VOOR DE TOEKOMST

Diepe buiging voor Jacques Vandenbulcke. De professor emeritus van de KU Leuven en de onderzoeksgroep beleidsinformatica gaf op 1 februari de fakkel door aan de nieuwe SAI-voorzitter Marc Vael. Ook al blijft hij (gelukkig) nog betrokken bij SAI, toch maakt hij tijd voor een afscheidsinterview dat er geen is. En hoe het allemaal begon met een ‘elevator pitch’.

SAI is een ledenvereniging die al meer dan vijftig jaar bestaat. Maar eigenlijk begon het allemaal in een lift. “Het was wijlen Maurice Verhelst die in 1965 in Nederland een bezoek bracht aan de informatica-bibliotheek. Hij kwam in de lift Arie Duijvestijn tegen, de oprichter van het automatiseringsgenootschap in Nederland, en ze raakten aan de praat. Van daaruit is het idee ontstaan om ook in België iets gelijkaardigs op het getouw te zetten. Twee jaar later is dan SAI ontstaan als Studiecentrum voor Automatische Informatieverwerking.”

In al die jaren was u zelf ook het meest van de tijd betrokken, niet?
Jacques Vandenbulcke: “Dat klopt. Maurice Verhelst is zelf ruim tien jaar voorzitter geweest. In 1976 heeft men dan aan mij gevraagd om die functie op te nemen. Dat zou dan zozegegd voor enkele jaren zijn. Maar uiteindelijk heb ik het 44 jaar gedaan. En ik heb het altijd graag gedaan.”

Waar bent u het meest trots op?
“In de voorbije 42 jaar is SAI uitgegroeid tot een vaste waarde voor alle informatici in Vlaanderen en Brussel. En daar zijn wij best fier op. Onze organisatie telt duizend informatici als leden. Ik ben altijd trots als ik zie hoeveel informatici naar onze events komen. Er zijn conferenties waar veertig mensen op af komen, maar we hebben er ook waar er tweehonderd op aanwezig zijn.”

Wat zijn voor u in al die tijd de grootste veranderingen geweest in de wereld van ict?
“De komst en de doorbraak van het internet is zonder twijfel de grootste verandering geweest. Dat heeft eigenlijk ook mee voor een grote verandering aan onderwerpen gezorgd. Ging het bijvoorbeeld vroeger over specifieke topics en technologieën als bijvoorbeeld Cobol als programmeertaal, dan gaat het nu over een brede waaier aan onderwerpen.”

Het aanbod is vandaag veel breder, en dit in diverse dimensies?
“Ja, dat klopt. Breder in reikwijdte. We brengen alle mogelijke onderwerpen om IT'ers te ondersteunen. Van 5G en blockchain tot security en alles daartussen. Zo stellen wij vast dat bedrijven naargelang het onderwerp kiezen wie in aanmerking komt om naar het SAI-event te gaan. Soms sturen ze een ander profiel. Maar de breedte situeert zich ook nog op een ander vlak. We zijn in al die jaren namelijk veel meer de nadruk gaan leggen op de bedrijfseconomische impact van informatica, en niet alleen de technologische.”

Dat is een zeer mooi parcours. Maar wat kan er nog beter bij SAI, denkt u?
“Misschien dat wij vandaag nog niet zo erg actief zijn op sociale media. Onze marketing in het geheel kan mogelijk wel wat beter. Veel bedrijven kennen ons nog niet. Maar ik ben ervan overtuigd dat de nieuwe voorzitter Marc Vael en ook



Jacques Vandenbulcke (rechts): "Ik ben altijd trots als ik zie hoeveel informatici naar onze events komen."

onze operationeel manager Seppe vanden Broucke hier zeker stappen in zullen zetten. Daar zijn ze al volop mee bezig. Zo ben ik ook heel trots op ons nieuwe en eigen vakblad dat er zeer mooi uitziet. Ook op dat vlak gaan we flink vooruit."

Als we breder gaan: wat ziet u als de grote it-trends voor de komende tien jaar in IT? Wat wordt 'the gamechanger'?

Volgens mij gaat het niet om één bepaalde grote trend. Eigenlijk zie ik er verschillende die een rol van betekenis kunnen spelen. Ik denk dan aan artificial intelligence, maar dan wel artificial intelligence dat ook echt de problemen gaat oplossen en je kan uitleggen waarom een bepaalde redenering de goede is. Maar er zijn nog veel andere zaken

die van belang zullen zijn: Internet of Things en blockchain en natuurlijk cybersecurity, dat nog belangrijker zal worden. Ook veel zaken waar het nog moet beginnen. Denk bijvoorbeeld aan quantumcomputing dat echt nog toekomstmuziek is. Heel veel domeinen dus, en dat maakt onze sector ook zo boeiend."

Wat worden voor IT de grote uitdagingen?

"Ik zie er twee. Enerzijds is dat het milieu-aspect. Zo is de IT-sector vandaag goed voor 4 procent van alle CO2-uitstoot, en als we niet opletten zal dat de komende jaren naar 8 of 9 procent gaan. Dat is dus zeker een aandachtspunt, en concepten en technologieën zoals rond edge computing zullen op dat

vlak zeker in the picture komen. Een tweede uitdaging is de zoektocht naar talent en het tekort aan informatici op termijn. Als ik zie hoeveel studenten er in onze technische- en IT-richtingen zitten momenteel, dan stel ik vast dat dat onvoldoende zal zijn om aan de hoge vraag te voldoen. Ook dat wordt een aandachtspunt."

Laatste vraag: zal u het voorzitterschap missen?

"Ik heb het altijd graag gedaan, maar ga het niet missen. Bovendien blijf ik verbonden met de organisatie als lid van de raad van bestuur en ook als penningmeester. Ik plaats mezelf met veel plezier in een rol meer op de achtergrond en ben blij dat jonge mensen het overnemen."



DOE MEE EN WIN EEN MOOIE PRIJS MET DE SAI QUIZ

VRAAG 1

In welke actiefilm werd de codenaam T.H.O.R. gebruikt door samenzweervers om de privacy van burgers te schenden, politieke tegenstanders uit te schakelen en grootschalige publieke ongehoorzaamheid te creëren?

VRAAG 2

Wie presenteerde in december voor SAI de technotrends op een avondconferentie?

SCHIFTINGSVRAAG

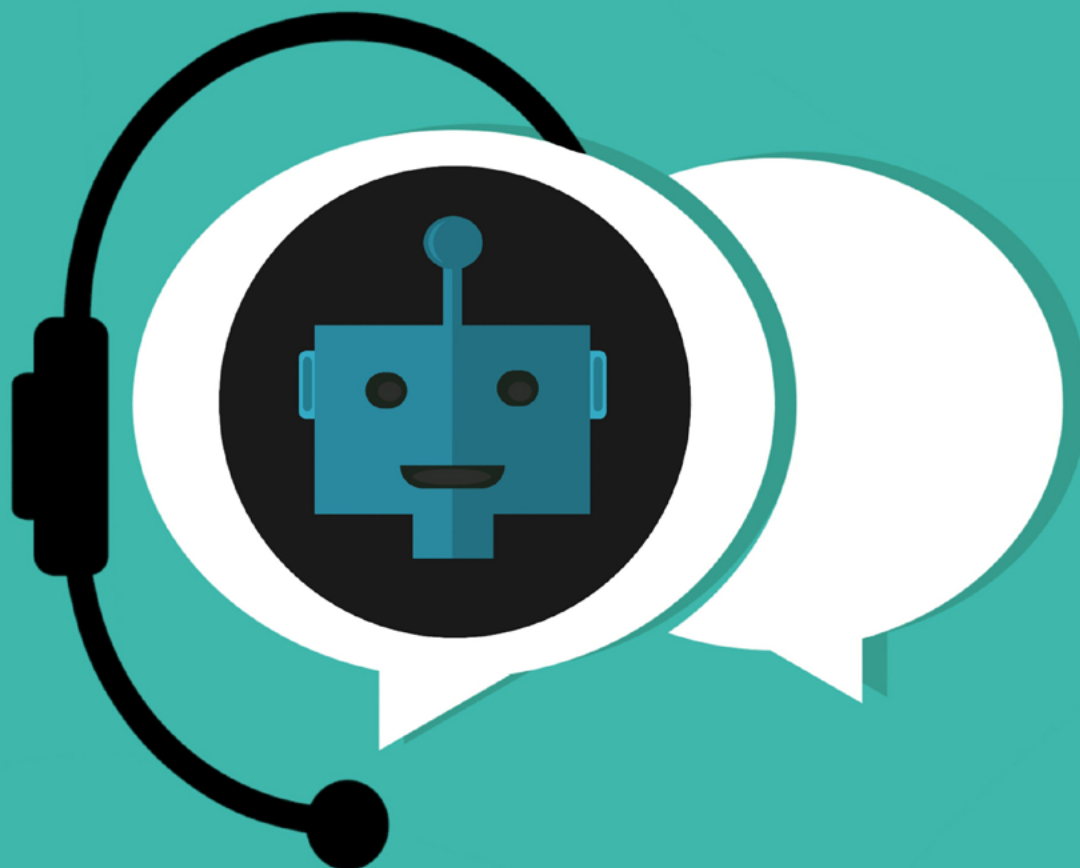
Hoeveel SAI-leden zullen het juiste antwoord gemaild hebben tegen vrijdag 1 mei 2020?

» Stuur het antwoord op deze vragen voor 1 mei 2020 naar communicatie@sai.be.
De winnaar wordt bekendgemaakt op 15 mei 2020 en wordt persoonlijk verwittigd.

WAAROM CHATBOTS KOMEN OPZETTEN
EN HOE ZIT DAT TECHNOLOGISCH?

WELKOM IN HET TIJDPERK VAN AMBIENT COMPUTING

Wat voor velen misschien eerst een gimmick leek, breekt door in bedrijven en op IT-afdelingen. Chatbots komen opzetten bij het online shoppen of bij schadeverzekeringen. Of ze reserveren voor jou een restaurant. De stand van zaken en toekomst van de chatbot in zeven vragen en antwoorden.



1/ WAAROM ZIJN CHATBOTS DEEL VAN EEN GROTERE IT-EVOLUTIE?

Chatbots of geautomatiseerde gesprekspartners (in zowel spraak als tekst) zijn de exponent van enkele vooraanstaande it-trends. Om te beginnen is er het Internet of Things (IoT) waarbij bedrijven en gezinnen allerlei toepassingen (van hun thermostaat, bewakingscamera's tot hun muziekinstallatie) aan een netwerk koppelen. En tegelijk – en dat is dan weer de trend rond artificial intelligence - worden al deze toepassingen en de achterliggende technologie ook alsmaar slimmer.

Vandaag zijn we aanbeland in het tijdperk van ambient computing. "Eerst was er hardware en software, dan apps die op mobiele toestellen terecht kwamen. Daarna verscheen zo'n app als feature in een andere app, bijvoorbeeld om iets te vertalen. En tenslotte werden die apps acties, die op verschillende manieren (zoals met de stem) kunnen worden aangesproken. Denk aan opdrachten die we geven aan Alexa of Google Home", vertelt Gil Nimmegeers, mede-oprichter van

Bothrs, dat zich als bedrijf specialiseert in chatbots.

Volgens Nimmegeers zijn we vandaag aanbeland in de derde it-golf. Eerst was er de mainframe, waar computerkracht centraal werd beheerd. Daarna ging men over naar de tweede golf: die van de personal computer. Met dank aan evoluties als cloud, Web, mobiel en IoT, zijn we aanbeland in de derde golf van ambient computing. "Hierbij is die zogenaamde computer een integraal deel van de omgeving", stelt Nimmegeers. Chatbots spelen naast onder meer digitale assistenten en zogenaamde 'ephemeral apps' of 'progressive web apps' een belangrijke rol in deze evolutie. "The next big thing will be a lot of small things."

2/ WAT ZIJN DE PLUSPUNTEN VAN CHATBOTS?

Bij chatbots verloopt de interactie op basis van conversaties in natuurlijke taal, zowel geschreven als gesproken. Ze voelen voor een gebruiker alvast persoonlijker en na-

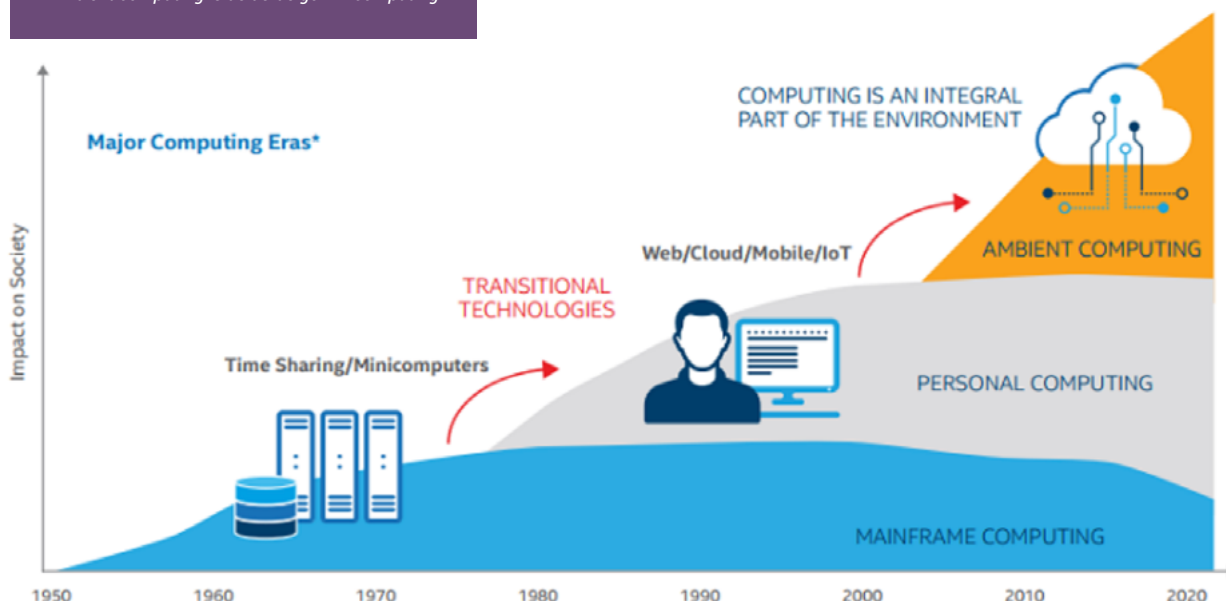
tuurlijker aan dan apps of websites, en dit via een gepersonaliseerde flow. Terwijl, bijvoorbeeld op een klantendienst, het traditionele team van menselijke operatoren wordt ontlast. Intussen zijn ze, volgens Nimmegeers, ook vrij makkelijk te gebruiken. En vormen ze een extra kanaal met 'virtuele experts' dat de gebruiker kan aanwenden.

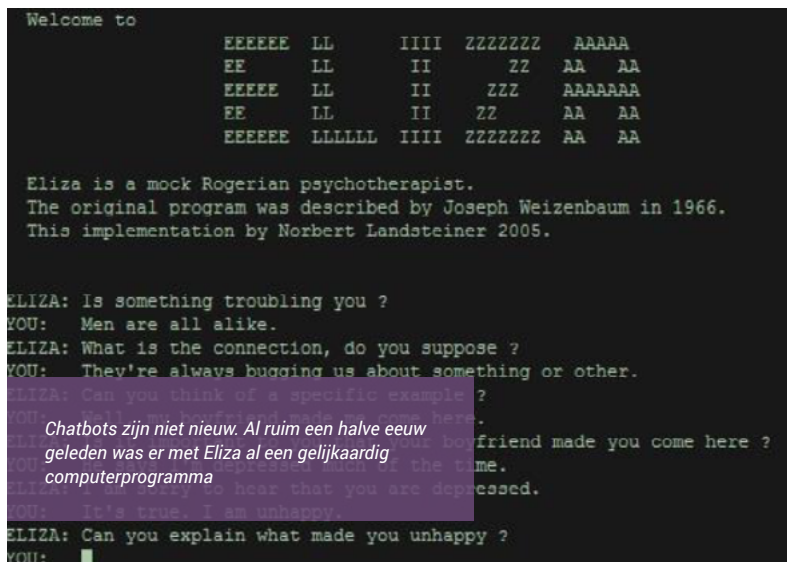
Bovendien hoeft de gebruiker hier ook niet meteen iets extra voor te downloaden of installeren, want chatbots zitten ingebed in apps of op een website, de klassieke kanalen dus. Ook bieden ze de mogelijkheid om zogenaamde push-notificaties te sturen. "Het is vandaag waardevol om te overwegen om een conversatie, in al zijn vormen, als onderdeel van de product toolkit te beschouwen", vat Nimmegeers samen.

3/ WAAROM MISLUKKEN CHATBOTS?

Chatbots zijn niet nieuw. Al ruim een halve eeuw geleden was er met Eliza al een gelijkaardig computerprogramma. Al lijken chatbots nu

Ambient computing is de derde golf in computing





pas echt door te breken. Wat ging er aanvankelijk fout? Heel veel zaken vaak, erkent Stef Nimmegeers, mede-oprichter van Bothrs. “Want het heeft toch enkele jaren geduurd om te staan waar we nu staan. In het begin werden chatbots aanzien als een gimmick, een hype of erger nog: een oplossing voor een probleem dat niet bestond.”

Maar dat kwam ook doordat de eerste use cases van chatbots niet zo goed waren en ze trachtten om diverse zaken tegelijk aan te pakken. Ook waren veel chatbots van het eerste uur niet goed ontworpen en communiceerden ze niet met de bestaande computersystemen in een organisatie. Of ze misten de noodzakelijke menselijke escalatie-protocollen waardoor de gebruikers zich al snel aan hun lot overgelaten voelden. “Vergeet ook niet dat iets als een conversatie super tricky is”, benadrukt Stef Nimmegeers.

Aan al die voorwaarden wordt nu meer en meer voldaan. “Daarnaast speelt ook de recente vooruitgang in Natural Language Processing / Understanding (NLP/NLU) om de intentie van een gebruiker via natuurlijke taal te begrijpen”, zo stelde Joachim Ganseman, researcher bij Smals, onlangs bij een presentatie. En dan is er ook nog de opkomst

van cloud-based AI services van de grote partijen als IBM, Microsoft, Amazon en Google.

4/ WAAR ZITTEN DE USE CASES (BINNENKORT)?

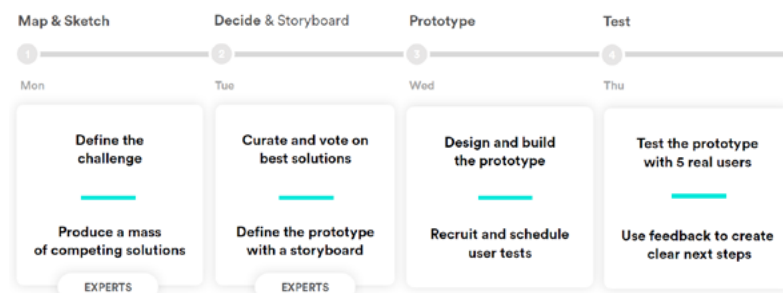
Die zijn divers. Van interne medewerkers tot burgers en klanten. Van het beantwoorden van algemene vragen tot het opvragen van de status van een dossier. Veel chatbots zitten in de sfeer van (e-)commerce. Van het kopen van een zonnebril bij Ray Ban, het aanpassen van je boodschappenlijstje bij Colruyt tot het boeken van een reisexcursie. Of, zoals bij Belfius (zie volgende artikel), tot het ingeven van een schadegeval door klanten. “Het gaat niet over gebrui-

kers die met bots chatten, maar over zaken die ze op een eenvoudige manier gedaan moeten krijgen”, aldus Gil Nimmegeers.

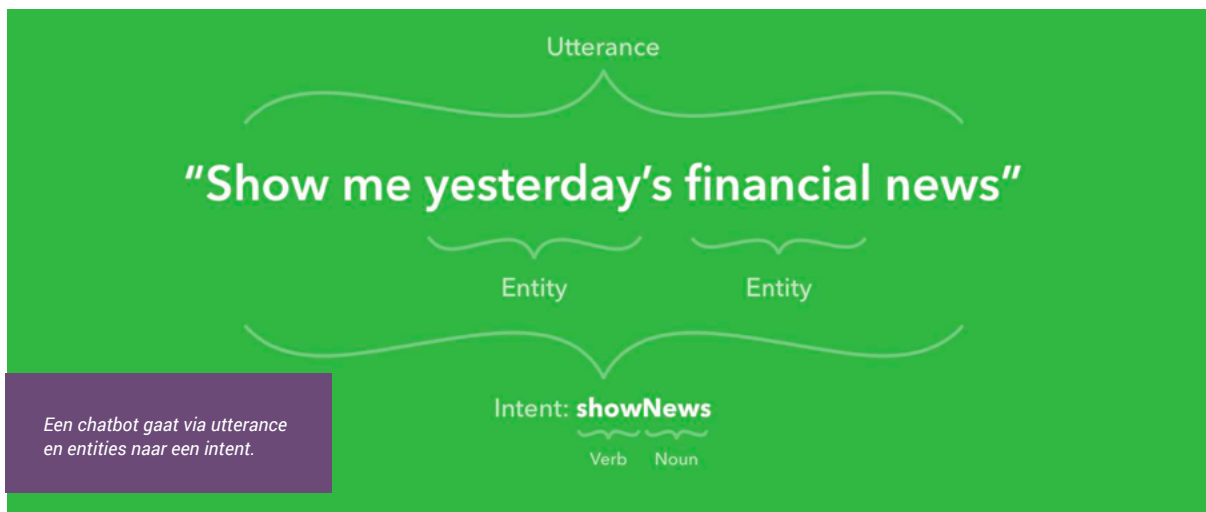
Er zijn chatbots die praten of die chatten. Of soms een combinatie van beide: zoals Google dat je een tijdstip laat ingeven waarna de bot zelf naar het restaurant belt om de afspraak vast te leggen. Dergelijke use cases geven een beeld van wat er in de toekomst mogelijk is want hoeveel telefonistes – van artspraktijken tot autogarages – doen de hele dag niets anders dan het opnemen en inboeken van afspraken?

5/ HOE BEGIN JE IN JE BEDRIJF MET EEN CHATBOT?

Een chatbot vertrekt vanuit het idee, waarna het ontwerp en de toepassing wordt gebouwd. Dat vergt enige tijd, maar de bedoeling is om dit proces niet al te lang te doen rekken en binnen afzienbare tijd te lanceren. Want door middel van die lancering worden data gecreëerd die het systeem enerzijds verbeteren en anderzijds ook voor nieuwe ideeën zorgen waarna het hele proces van nul begint. Zo’n bot leert namelijk uit voorbeeldzinnen, dus hoe meer zinnen, hoe beter het antwoord. “Tracht je doelpubliek te gebruiken en let hierbij ook op de interface die ze gebruiken om met jou in contact te komen”, raadt Gil Nimmegeers aan.



De conversational Design Sprint in vier etappes



Bij de uiteindelijke design sprint draait het vooral om de wisselwerking tussen het idee en de data. Zo'n 'conversation sprint' is een proces voor het beantwoorden van cruciale vragen door middel van interessante ideeën met klanten (prototyping). Hierbij doorloopt dit proces vier fasen: van het definiëren van een uitdaging over het creëren van oplossingen en het definiëren, ontwerpen en bouwen van een prototype tot het testen van dat prototype.

6/ HOE WERKT EEN CHATBOT?

Eenzijds werken chatbots op hun eigen manier met specifieke termen

als intent en entity. Het systeem leidt de intent af uit een zin, bijvoorbeeld dat de gebruiker een vlucht wil boeken. Uit die zin (of utterance) herkent hij bepaalde 'entities', in dit geval zijn dat steden zoals New York of Londen, of aantallen of tijdstippen. Termen die je wilt herkennen als entiteit moet je dus in het systeem voorzien. En hierbij is het meestal: hoe minder intents, hoe makkelijker te classificeren. Ook al is machine learning in staat om een vraag die niet letterlijk voorkomt in de voorbeeldzinnen te koppelen aan de juiste intentie.

Vervolgens vult het systeem de parameters van de intent aan en onderneemt het actie zodra de in-

tent volledig is (het zogezegde fulfillment). Dit kan dan een tekstueel of gesproken antwoord zijn of het bestellen en opsturen van tickets.

7/ WAT IS DE ACHTERLIGGENDE TECHNOLOGIE?

Anderzijds is er de klassieke technologische stack. Front-end van een chatbot (het luik dat de klant ziet) is de app, het messaging platform (zoals Messenger of WhatsApp) of een smart object (zoals Google Home). Platforms of toepassingen aan de back-end zijn bijvoorbeeld Chatlayer, Rasa NLU, Dialogflow (van Google) of Flow.ai. Sommige daarvan zijn cloud-based, andere ook on-premise. Tussen deze twee zit vaak ook een middleware-app, zoals Botkit, die front-end met back-end verbindt. Deze vangt berichten op van front-end en stuurt die door naar back-end en ontvangt antwoord.

Bedrijven opteren best voor een toolset die hun case ondersteunt. "Kies tools die uw infrastructuur ondersteunen en u helpen om het product en de gebruikersbeleving te bouwen", stelt Gil Nimmegeers. Al zal die beleving ook evolueren. "Bij chatbots is het een kwestie om te starten met experimenteren, en ook binnen afzienbare tijd effectief in productie te gaan", benadrukt hij.

DRIE VOORBEELDEN CHATBOTS & ASSISTENTEN @ WORK



1/ **BOL.COM**
Bol.com, voor klantenondersteuning



2/ **STUDENT@WORK**
Nora, de virtuele assistent van Student@Work



3/ **GOOGLE BOOKING ASSISTENT**
De Google booking assistent is beschikbaar in de VS. Je wilt een reservatie in een restaurant en Google assistent gaat het telefoontje zelf doen voor jou.



Het myBo mission team bestaande uit medewerkers van Insurance, Bank, IT en Business, stond in voor de ontwikkeling en werd ondersteund door een aantal strategische partners (zie inzet).
Op de foto: Boven: Glenn, Cynthia, Simon, Karishma, Gianni en Bala. Onder: Dorien, Bruno, Jana, Marjoléin en Laura.

SCHADECLAIMS VIA CHATBOT

Het moment waarbij de verzekeringsklant zijn schadegeval doorgeeft, is voor een verzekeraar het spreekwoordelijke moment van de waarheid. Het is dus niet evident om daar, zoals bij Belfius Insurance, een chatbot voor in te schakelen. SAI Update bekijkt zowel de strategie als technologie achter deze case rond MyBo, de chatbot bij Belfius Insurance.

Net als de hele financiële sector zit de verzekeringswereld volop in een digitale transformatie, met als doel om relevant en efficiënt te blijven voor de klant. “Het aanbieden van een optimale customer experience staat hierbij centraal. We willen onze processen zo eenvoudig mogelijk houden, en zo transparant

mogelijk zijn naar de klant toe. Dit door die processen uit te denken vanuit een zero-based design”, vertelt Gert Vanhaecht, CIO, Belfius Insurance. Belfius Insurance omvat de merken Belfius, DVV en Corona Direct. De IT-afdeling van Belfius Insurance ondersteunt hoofdzakelijk de 2 eerste merken.

ONTWORPEN VANUIT BUSINESS EN KLANTEN

De oplossing die Belfius Insurance uitwerkte, na heel wat directe interactie met klanten, was het aanbieden van een chatbot. Deze moest de klantenervaring bij het aangeven van een schadegeval helpen optimaliseren.

“Bij de uitwerking deden we niet alleen een uitvoerig beroep op onze klanten maar ook op onze businessmensen. Denk hierbij aan de klantenbeheerders die dagelijks intensief contact hebben met klanten. Mensen van het terrein dus”, vertelt Marc Purnal, head of claims non-life bij Belfius Insurance. Zo werd MyBo geboren als chatbot voor Belfius Bank.

WAT DOET DE CHATBOT?

De chatbot, die gebruikmaakt van artificiële intelligentie, begeleidt de klanten stap voor stap in een eenvoudige en verstaanbare taal en helpt ze om hun aangifte in alle kalmte vanaf hun pc of hun smartphone online in te dienen. myBo staat de klanten in real time bij en stelt ze de nodige vragen om hun dossier te behandelen.

Aan de hand van de informatie die tijdens de ‘chat’ werd verstrekt, identificeert myBo de waarborg van het contract met betrekking tot het schadegeval en gaat na of de klant voor deze waarborg gedekt is. myBo stuurt de klant onmiddellijk het nummer van zijn dossier en de documenten die hij nog moet uploaden om het te vervolledigen. De klant weet precies wat de volgende stappen zullen zijn in de afhandeling van zijn schadegeval. Vaak kan hij ook kiezen voor een ‘direct payout’ of onmiddellijk het type van herstelling kiezen (Belfius Home Repair, eigen hersteller, zelf herstellen ...). Na afloop van de ‘chat’ ontvangt hij via e-mail een samenvatting van zijn conversatie met myBo. Uiterlijk één werkdag later wordt het dossier dan door een schadebeheerder behandeld als dit toch nog nodig zou blijken. Als de klant op gelijk welk moment hulp nodig heeft, verschijnt er in de chatsessie een telefoonnummer om naar een beheerder te kunnen bellen.

Zijn de klassieke klantenmedewerkers dan overbodig? Toch niet. “We

zien een sterke groei in onze business, die we enkel zullen kunnen ondersteunen als we de jobs laten evolueren naar een behandeling van cases waar menselijke tussenkomst echt een toegevoegde waarde heeft voor de klant”, stelt Marc Purnal.

VAARWEL VEROUDERDE ARCHITECTUUR

Ook de IT-aanpak bij Belfius moest het succes mee bepalen. “We vervangen, via ons interne programma

Core Insurance Renewal, al onze insurance non-life toepassingen (in eerste instantie auto en home) en dit voor de diverse merken Belfius en DVV”, aldus Vanhaecht. Concreet betekent dat ook dat ze de oude mainframetoepassingen bij Belfius Insurance systematisch aan het vervangen zijn. “We bouwden een toekomstgerichte integratie-architectuur uit, die ons in staat stelt ons met alle nodige systemen van bank en verzekeringen te connecteren. Een architectuur die ons vlot integreert met externe platformen



Gert Vanhaecht,
CIO, Belfius Insurance.

DE TRANSFORMATIE VAN IT-ARCHITECTUUR BIJ BELFIUS

De voorbije jaren werd de IT-architectuur van Belfius Insurance grondig vernieuwd en klaargemaakt voor het (volgende) digitale tijdperk. “Zonder dit programma zou de ‘app normale autoverzekering’, waarbij we verkoop en dienstverlening van autoverzekeringen via de mobiele app van de bank aanbieden op een uitermate innovatieve manier, nooit mogelijk geweest zijn” oppert Gert Vanhaecht.

De transformatie situeert zich in hoofdzakelijk drie domeinen:

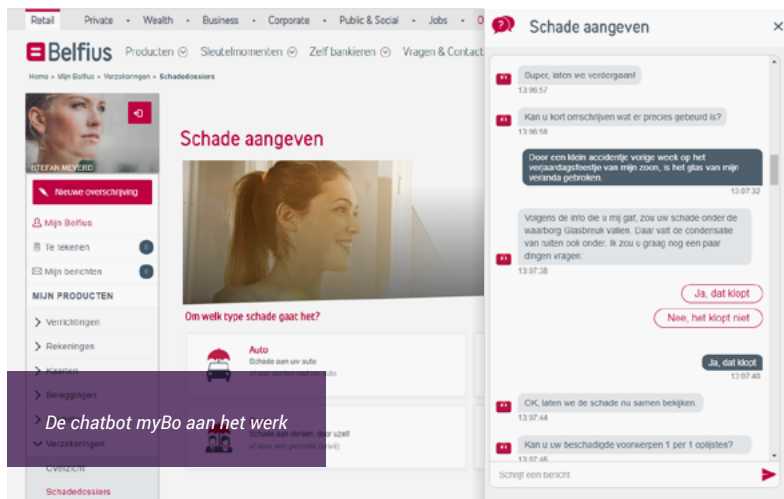
- 1/ Oude mainframe-systemen voor non-life vervangen door het AXON pakket van Keylane
- 2/ Integratie van het platform voor de hele lifecycle, met onder meer externe partners en alle distributiekanaalen van de ondersteunde merken
- 3/ Het geïntegreerd digitaal communicatieplatform

zodat we deel gaan uitmaken van ecosystemen.”

Ook de organisatie evolueerde mee. “We installeerden een Target Operating Model binnen IT waarmee we dergelijke programma’s mee kunnen realiseren én mee kunnen bijdragen aan innovatie”, vertelt Vanhaecht. “Hierbij introduceerden we - daar waar relevant en waar de organisatie er klaar voor was - een agile werking die we pragmatisch benaderden. Eentje waarbij we de business & IT teams, samen met externe partners, in virtuele ‘mission teams’ laten samenwerken om op een iteratieve manier naar een product te kunnen evolueren.”

DE RESULTATEN

Chatbots bij schadeclaims lijken niet evident. Maar volgens Gert Vanhaecht is de klantenfeedback uitermate positief, mede en vooral



omdat er is vertrokken vanuit de échte fricties die de klant ervaart. “Het proces dat de klant doorloopt, wordt als zeer natuurlijk aanvoeld. Ze appreciëren ook enorm de snelheid van afhandelen van een groot aantal dossiers”, vertelt hij. “Ook uit

het agentennetwerk krijgen we een gelijkaardige positieve feedback.”

» *MyBo YouTube video:*
https://www.youtube.com/embed/jq0NztBh_c0



Marc Purnal,
 Head of Claims Non-Life, Belfius Insurance

TEAMWORK VOOR DE BOT

Het chatbot-systeem bij Belfius Insurance met de uitbouw van de myBo chatbot en voor de vertaalslag naar de core systemen komt er alleen door nauwe en hechte samenwerking met diverse externe partijen:

- **Bothrs:** ‘design thinking’-oefeningen en ondersteuning in opzetten van de dialogen
- **Chatlayer:** voor implementatie van de intelligente dialogen en het aanbieden van het conversationele platform
- **ML6:** voor het NLP & Machine Learning gedeelte. Het begrijpen van de context van de klant en deze vertalen naar een dekking.

BIJNA ÉÉN OP ACHT PC'S NOG OP WINDOWS 7

WIE GEBRUIKT WINDOWS 7 NOG?

Vanaf midden januari levert Microsoft geen veiligheidsupdates meer voor zijn besturingssysteem Windows 7. Al werkt in België nog zowat 12 procent van de pc's op Windows 7.

Het is intussen dus meer dan tien jaar geleden dat Microsoft Windows 7 lanceerde. Het werd voor Microsoft een populair besturingssysteem in hun reeks van Windows-versies. Maar sinds dinsdag 14 januari is de officiële dienst dus voorbij. Het softwarebedrijf stopte vanaf dan met de veiligheidsupdates voor Windows 7.

ALBERT HEIJN

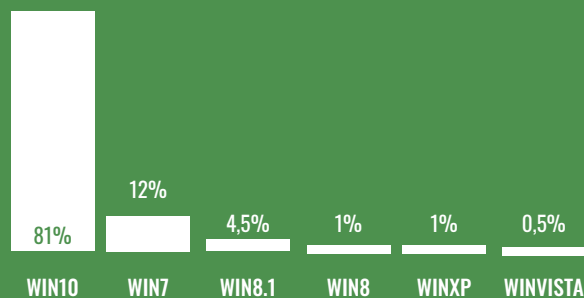
Dat betekent zeker niet dat bedrijven of organisaties het niet meer zouden gebruiken. Bijna twaalf procent van de Windows-gebruikers heeft nog een computer met Windows 7, dat is bijna één pc op acht. Dat blijkt uit cijfers van StatCounter. Windows 7 is dus nog erg ingeburgerd. Ook bij retailketen Albert Heijn (zie foto) is Windows 7 nog danig in omloop.

Al kan het nog altijd ouder. Zo werken nog wel wat gebruikers met Vista of XP. Vooral het gebruik (toch nog altijd bijna 1 procent) van XP is opvallend. Want Windows XP werd maar liefst achttien jaar geleden geïntroduceerd.

13 PROCENT VEROUDERD

In totaal gebruikt dus ruim 13 procent van de Belgische gebruikers zo'n verouderde versie van Windows. Al die verouderde Windows-versies vormen volgens het Centrum voor Cybersecurity België (CCB) een uitgelezen doelwit voor cybercriminaliteit, vermits de grote meerderheid van alle malware-infecties op oudere Windows-systemen zou plaatsvinden. Het CCB raadt gebruikers en bedrijven met een verouderde versie van Windows aan om te upgraden.

WINDOWS-VERSIES MARKTAANDEEL IN BELGIË



StatCounter, februari 2020



Ook bij retailketen Albert Heijn is Windows 7 nog danig in omloop.



WIE WIL ER VANDAAG CISO ZIJN?

DE TIEN VAKDOMEINEN VAN DE CISO

De Chief Information Security Officer (CISO) heeft de touwtjes in handen als het gaat om alle aspecten van de IT-veiligheid van een organisatie. Maar de rol gaat tegenwoordig verder dan het alleen maar definiëren van principes en procedures binnen het veiligheidsbeleid van een organisatie. Hoe ziet de functieomschrijving van een CISO anno 2019 er uit? Een beroep dat nog volop in ontwikkeling is.

De rol van de CISO gaat terug tot 1994, toen Citigroup het slachtoffer werd van een reeks cyberaanvallen van Russische hacker Vladimir Levin. De bank creëerde 's werelds eerste formele uitvoerende cyberveiligheidsteam met Steve Katz als leider. Toen was de CISO-functie een zeer technische job. De CISO

rapporteerde aan de CIO en had een achtergrond als systeem- of netwerkbeheerder, of als beveiligingsanalist in een security operations center of SOC.

OOK PSYCHOLOGEN

Bijna alle CISO's waren mannen,

met ruime ervaring in de informatica. Deze traditionele kijk is de laatste jaren grondig verschoven, niet alleen dankzij de diversificatie van het personeelsbestand, maar ook dankzij een groeiende wens om de veiligheid beter af te stemmen op de zakelijke belangen. Als gevolg hiervan zijn er vandaag

mannelijke en vrouwelijke CISO's van alle achtergronden met een verscheidenheid aan vaardigheden en ervaringen. Ze zijn misschien niet allemaal CISSP- of CISM-gecertificeerd maar ze weten wel hoe ze veiligheidsprojecten moeten beheren, communiceren en een business case voor informatieveiligheid moeten opbouwen.

Sommigen van de huidige generatie CISO's zijn afkomstig uit gebieden zoals psychologie, sociologie en rechten of uit domeinen die al zijn afgestemd op de typische veiligheidsrisico's, met een uitgesproken technische, consulting- of

advies-achtergrond. Minder CISO's hebben een audit- of compliance-achtergrond, ondanks het feit dat de kennis van governance, risicobeheer en wetgeving belangrijke vaardigheden zijn.

660 CYBERAANVALLEN PER DAG

Een CISO moet constant steeds meer en steeds geraffineerdere cyberaanvallen afslaan, ongeacht in welke organisatie of sector hij of zij vandaag actief is. Een organisatie met 10.000 eindpunten (pc's, laptops, smartphones, servers, firewalls, enz.) ondergaat naar schatting gemiddeld 660 cyberaan-

val pogingen per dag - wat leidt tot een immense druk op een CISO. Daarnaast is er de versnelde ontwikkeling en gebruik van allerlei nieuwe technologie in organisaties, wat zich vertaalt in grote digitale transformatieprojecten, voortdurend veranderende juridische en regelgevende omgevingen (zoals de EU AVG en de California Consumer Privacy Act), en het misverstand dat informatieveiligheid de exclusieve verantwoordelijkheid is van de CISO. Verder spelen ook interne en externe veiligheidsincidenten, financiële verliezen als gevolg van veiligheidsincidenten, naleving van wet- en regelgevingen, bescherming van de reputatie van de organisatie,... Kortom, de verantwoordelijkheden worden steeds groter en de mislukking bij om het even welk ernstig veiligheidsincident resulteert bijna altijd in direct ontslag.

BELANGRIJKSTE DOMEINEN VAN EEN CISO

De CISO-functie en -verantwoordelijkheden zijn in constante beweging omdat digitale veiligheid veel aspecten van transacties doorkruist, wat een uitdaging is om duidelijk afgebakende grenzen te stellen aan de verantwoordelijkheden van de CISO. Verwachten organisaties dat de CISO een technologietovenaar is, een zakelijk intelligente goeroe of beide? Verwachten organisaties dat de CISO de verantwoordelijkheid en aansprakelijkheid draagt voor het beveiligen van de IT-omgeving en de informatiemiddelen van de organisatie? Moet de CISO deel uitmaken van de directie, of moet de rol worden beperkt tot binnen de IT-afdeling?

Op basis van eigen ervaring, zijn alle taken van een goede CISO anno 2020 samen te brengen in deze zes basisdomeinen (zie links).

Merk op dat vijf van de zes domeinen proactief zijn, terwijl incidentbeheer zowel proactieve als reactieve taken heeft.

DE ZES BASISDOMEINEN VAN EEN CISO

SECURITY GOVERNANCE & RISICOBEBEER	Implementeer & verbeter beleid en processen voor een degelijk IT security governance & risicobeheer
SECURITY KLANTEN ONDERSTEUNING	Creëer & verbeter standaard security processen ter ondersteuning van departementen met een klantenfocus
SECURITY OPERATIONEEL BEHEER	Implementeer & verbeter principes voor de beveiliging van de IT-infrastructuur en operationele werking
SECURITY COMPLIANCE	Integreer IT compliance door 'security by design' toe te passen
SECURITY INNOVATIE	Integreer IT security in nieuwe innovatieve (IT) oplossingen van de organisatie
SECURITY INCIDENTENBEHEER	Identificeer, bescherm, detecteer, reageer op en herstel van IT security incidenten

10 BELANGRIJKE EIGENSCHAPPEN VAN EEN GOEDE CISO ANNO 2019?

Een goede CISO is een veelgevraagd en moeilijk te vinden persoon, omdat de rol een grote technische kennis combineert met veel ervaring, leiderschap, financiële kennis, zakelijk inzicht, visie en persoonlijkheid. Bovendien is er wereldwijd een enorm tekort aan veiligheidsexperten. Hierna volgt een lijst van de belangrijkste kenmerken van een goede CISO vandaag.

1

BEZIT EEN GROOT MOREEL EN ETHISCH BESEF

Goede CISO's hebben essentieel een groot moreel en ethisch kompas. Immers, hoe meer vertrouwen er is in de persoon/afdeling die de IT-veiligheid bewaakt, hoe meer invloed de CISO krijgt. Dit zal goed uitkomen als de CISO een drastische, onpopulaire beslissing moet nemen.

2

HEEFT EEN RUIME KENNIS VAN DIGITALE (VEILIGHEIDS)OPLOSSINGEN

Kennis van techniek is altijd al een belangrijk onderdeel geweest van de bagage van een goede CISO en zal ook in de toekomst een van de basisfundamenten van de functie blijven. Kennis van digitale oplossingen zorgt ervoor dat de CISO vertrouwen krijgt van de andere

departementen die zich bezighouden met zaken als softwareontwikkeling, ontwerp en beheer, uitbesteding aan derden ...

In plaats van enthousiasme voor de nieuwste veiligheids-tool/hype, dient de vraag gesteld "Wat is de impact van deze technologie op onze organisatie?" Waar de organisatie de mogelijkheden van nieuwe digitale oplossingen beoordeelt, is het de rol van de CISO om zeer inzichtelijk te maken welke risico's verbonden zijn aan het gebruik van nieuwe digitale technieken en toepassingen, hoe ze veilig in gebruik te nemen in overeenstemming met het beleid en met wet- en regelgeving. Een goede CISO stopt met het kopen van enkel maar veelbelovend klinkende veiligheidstechnologieën, maar zet eerder volop in op het begrijpen waar de echte veiligheidsproblemen liggen binnen de organisatie en werkt van daaruit eventueel samen met een leverancier om de juiste veiligheidsoplossingen te implementeren.



3

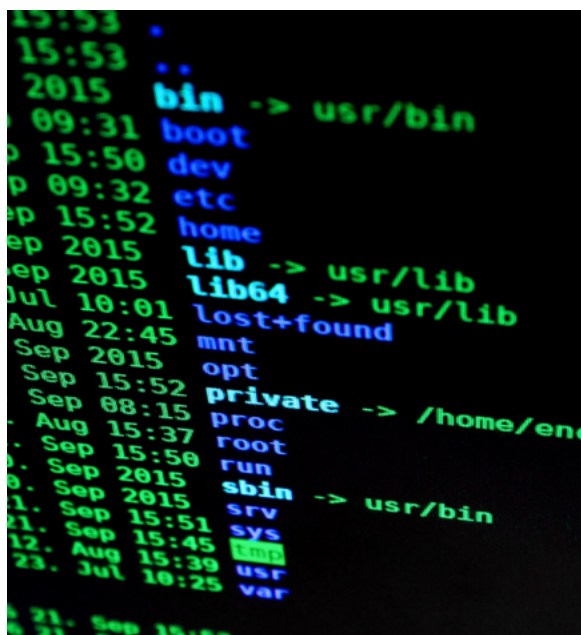
ONTDEKT EN VERDIEPT ZICH IN HET ECOSYSTEEM EN DE CULTUUR VAN DE ORGANISATIE

Een goede CISO is op de hoogte in wat voor soort organisatie hij zich bevindt. Hij of zij begrijpt net als een goede CIO of een goede CFO hoe de organisatie functioneert en wat de interne en externe factoren zijn waar de organisatie mee te maken krijgt. Met andere woorden: een goede CISO kent het digitale ecosysteem waarin de organisatie opereert.

4

LEIDT MENSEN

Een goede CISO gedraagt zich tegenover zijn mensen net alsof hij aan het hoofd zou staan van de volledige organisatie. Hij voert het veiligheidsprogramma consequent, kordaat en zorgvuldig uit. De gewenste verandering binnen een organisatie komt ook voor een belangrijk deel bij de CISO terecht, die dan een duidelijke boodschap en visie moet kunnen vertolken. Niet alleen naar de mensen die het al weten, maar juist naar diegenen die er hun schouders voor ophaalden. Daar is een gezonde dosis mensenkennis en leiderschap voor nodig. Een goede CISO is een sterke persoonlijkheid die blijft met de evoluties, want als de leider van de verandering het opgeeft, zal de rest zeker volgen. Een goede CISO kiest de juiste medewerkers om het hoogste niveau van bescherming te garanderen en om op een veilige manier in projecten te werken. Veiligheid is hun eerste prioriteit. Vertrouwen en delegatie aan een team is belangrijk. Een goede CISO neemt meer technisch getalenteerde mensen in dienst dan men zou kunnen hopen en vult



het team met grote denkers die resultaatgericht zijn. Getalenteerde mensen zijn moeilijk te vinden en hebben altijd opties. Een goede CISO geeft hen een werkplek die ze niet willen verlaten en die ze aanraden aan anderen als er een vacature is.

5

GEbruikt een taal die iedereen begrijpt

Wie een veiligheidsmaatregel goed geïmplementeerd wil krijgen, moet in staat zijn om op elk niveau van de organisatie duidelijk en via het juiste kanaal te communiceren. Zonder begrip van mensen en culturen, de verschillende onderdelen en de soms verschillende belangen is de implementatie gedoemd te mislukken.

Een goede CISO communiceert regelmatig rechtstreeks met de directie en zelfs de raad van bestuur “zonder suiker-laag”. Dat houdt in dat er over de voortgang wordt gerapporteerd, dat er wordt gezocht naar budgetten om nog meer voortgang te boeken, dat de doelstellingen van de organisatie op het vlak van informatieveiligheid worden gehaald en dat er kan worden uitgelegd waarom, als dat niet het geval is.

Helaas voor CISO's spreken directies en raden van bestuur meestal geen “infosecurity vakjargon”. De grootste uitdaging is het aantonen van de waarde van informatieveiligheid en goed risicobeheer in financiële termen voor de organisatie. De CISO is verantwoordelijk voor het vertalen van het digitale veiligheidsrisico naar de directie door het identificeren van wat er mis kan gaan, de omvang van de bedreigingen, de risicobereidheid van de organisatie, het aanvaardbare risiconiveau voor het bedrijf en de kosten om het risico te beperken. Deze verantwoordelijkheden maken het noodzakelijk dat CISO de zakelijke taal even vloeiend spreekt als de technische taal. Idealiter heeft de CISO minstens elk kwartaal een rechtstreekse vergadering met de directie.

6

HELPT BIJ DE VEILIGHEIDSVEREISTEN VAN KLANTEN VAN DE ORGANISATIE

Een goede CISO begrijpt dat zijn of haar rol niet is om de organisatie te controleren, maar om iedereen in de organisatie in staat te stellen op een redelijk veilige manier te doen wat ze moeten doen. Een goede CISO stemt zijn programma's af op de missie, de waarden en het doel van de organisatie en begrijpt hoe te communiceren op een manier die cultureel bewust is en die mensen in staat stelt om effectieve beslissingen te nemen.

Een CISO kan, als hij/zij echt wil, een superkluis creëren, onbreekbaar en onkraakbaar, waaruit informatie niet kan ontsnappen. Maar deze kluis zal de organisatie belemmeren om geld te verdienen omdat er geen infor-

matie meer stroomt. Een goede CISO speelt altijd een evenwichtsspel tussen wat goed is voor de informatie-veiligheid en wat goed is voor de organisatie.

7

VERZAMELT EN GEBRUIKT (VEILIGHEIDS)DATA

Constant een juiste inschatting maken van de veiligheid van de organisatie is zeer moeilijk. Omdat een goede CISO zoveel data moet verwerken, is het moeilijk om ook op gedetailleerd niveau altijd bij de les te blijven. De CISO verzamelt en gebruikt data om het risico in te schatten, niet enkel van de organisatie maar ook over de sector en het ecosysteem waarin de organisatie opereert.

Als de VP Marketing een nieuwe tool wil implementeren die duizenden euro's gaat besparen en de efficiëntie gaat verbeteren, dan maakt een goede CISO een risicoanalyse van de tool om te zien hoe deze in de huidige infrastructuur zal passen. Heeft deze datastroom zin? Is de tool veilig genoeg? Is de leverancier veilig genoeg? Zijn de datapraktijken in overeenstemming met de voorschriften? Een goede CISO denkt altijd na: waar zijn de grootste risico's voor datalekken, verlies of diefstal in de organisatie?

8

LEIDT VERANDERINGEN

Een goede CISO weet dat "Rome niet op één dag is gebouwd" en is voorbereid op een lange tocht, waarin hij/zij veel mensen zal tegenkomen die het niet eens zijn om de nodige veranderingen te realiseren. Het is geen taak voor stressgevoelige mensen. Vandaar dat goede CISO's ook veel aandacht besteden aan het samenwerken en beïnvloeden van alle geledingen in de organisatie. Alles in een organisatie veranderen, van de risicotolerantie en veiligheidscultuur tot en met de processen en code, kost heel veel geduld. Cultuur speelt een grote rol als processen moeten worden veranderd. Mensen moeten deel uitmaken van dit besluitvormingsproces en dat vereist toegankelijkheid en medewerking. Het creëren van een cultuur van verandering is niet eenvoudig en vereist veel kwaliteiten. Een goede CISO weet hoe alle stukjes van de puzzel passen en bedenkt nieuwe manieren die de minste impact hebben op ieders werk. Maar goede CISO's weten dat het vele jaren duurt om veranderingen in een cultuur van een organisatie te realiseren.

9

IS VRIENDELIJK EN TOEGANKELIJK

Een goede CISO is een uitstekend luisteraar en kan met iedereen in de organisatie op een vriendelijke en toegankelijke manier spreken. Het vermogen om op risico's gebaseerde, organisatiegerichte beslissingen te nemen



en deze uit te voeren is ook belangrijk. CISO is een stressvolle baan, maar het kan veel stressvoller zijn als er geen feedback of communicatie van collega's komt. Vriendelijk en aanspreekbaar zijn betekent dat een CISO domme vragen krijgt, maar het betekent ook dat als er iets groots gebeurt, mensen niet bang zullen zijn om de CISO snel te benaderen.

10

VERZAMELT "VEILIGHEIDSSUPPORTERS" IN DE ORGANISATIE

Een goede CISO zoekt hulp bij andere leiders en functies in de organisatie op het gebied van financiën, marketing, klantenservice en HR, die vaak prioriteit hebben bij het toewijzen van budgetten. Die hulp betreft niet alleen financiële ondersteuning maar ook advies op basis van wat zij in de hele organisatie zien. Een goede CISO staat erom bekend dat hij elke afdeling ondersteunt, maar zorgt er ook voor dat die ondersteuning terugkomt. Als medewerkers enthousiast zijn over hun functie en regelmatig correct gewaardeerd worden, dan krijgt een goede CISO vanzelf waardering en vertrouwen van de personen die hij of zij geholpen heeft. Immers, in de realiteit is iedereen, van de CEO tot de receptioniste, verantwoordelijk voor de bescherming van informatie.

Tot slot weet een goede CISO dat het onmogelijk is om "perfect" te zijn. Het is OK om fouten te maken, nieuwe manieren te proberen om veiligheidsproblemen op te lossen en andere opties te verkennen. Maar het is vooral een leerrijke functie om te mogen uitvoeren binnen een organisatie, mits de juiste ingesteldheid, ondersteuning en waardering.



VOLGENDE EVENTS VOOR SAI

Cloud Native Architecturen

Avondconferentie

05-03-2020

Antwerpen

Hybrid Cloud: from strategy to realization

Avondconferentie

05-03-2020

Antwerpen

Agile Business Analyse: waarde-creatie voor de organisatie van de toekomst (NIEUWE HERHALING)

Workshop

09-03-2020

Brussel

Kubernetes

Workshop

09-03-2020

Brussel

Hybride Integratie Platformen (HERHALING)

Workshop

16-03-2020

Brussel

Interpretable Machine Learning

Workshop

16-03-2020

Brussel

Supply Chain Digitalization: blockchain, IoT and AI help to solve hard issues

Avondconferentie

19-03-2020

Brussel

Trends in Databases, Datawarehousing en Analytics (HERHALING)

Workshop

23-03-2020

Brussel

API Management: aanpak, tools & beveiliging (NIEUWE HERHALING)

Workshop

23-03-2020

Brussel

De valkuilen van Artificial Intelligence

Avondconferentie

02-04-2020

Antwerpen

The Cyber Operating Model of the Future

Avondconferentie

23-04-2020

Brussel

» [Meer info op SAI.be](#)

ADVERTEREN IN SAI UPDATE?

Stuur een mail naar
communicatie@sai.be

INTERESSE IN ONS PRIJSVOORDELIJG LIDMAATSCHAP?

Kijk op www.sai.be

COLOFON

Werkten mee aan dit nummer: William Visterin (hoofdredacteur) / Teun Van Dongen (art director) / Stef Gyssels en Marc Vael.