SEPTEMBER 2022 **NL.PLANET-BUSINESS.BE**

mediaplanet
A CAYBON COMPANY

Future of IT

De visie van onze experten

Een open gesprek over de impact van AI en IoT, de mogelijkheden van 5G en de uitdagingen rond cyberveiligheid in een snel evoluerend landschap.

© FOTO: MAARTEN DE BOUW

Voorwoord

Vijf aandachtspunten bij IT-outsourcing

Jef Loos

HEAD SOURCING EUROPE
WHITELANE RESEARCH

Er moet een goede match zijn tussen de cultuur van jouw bedrijf en die van je vendor.

Steeds meer Belgische organisaties kiezen ervoor om hun IT te outsourcen. Door de schaarste op de arbeidsmarkt is vooral de toegang tot resources en talent daar vandaag een belangrijke driver voor, naast kostenreductie, innovatie, transformatie en flexibiliteit. Om een goede vendor-klantrelatie te bekomen, geeft Jef Loos van Whitelane Research alvast vijf aanbevelingen.

1. Bied je vendor een belangrijke deal

Zorg ervoor dat de deal belangrijk genoeg is voor de vendor of service provider. Een vendor is geïnteresseerd in de grootte van de deal, de groeimogelijkheden en de winstmarge. Het heeft geen zin om een kleine en onbelangrijke deal te geven aan een grote vendor. Je krijgt dan immers slechts het B- of C-team. Bij een kleine deal kies je dus ook beter voor een kleinere partner.

2. Tracht een referentieaccount te zijn van je vendor

Wanneer je regelmatig in contact staat met mogelijke prospecten van de vendor, zal die er alles aan doen om jou de beste service te geven en gelukkig te houden. Het geeft je bovendien een drukkingsmiddel om afspraken en deadlines te laten nakomen.

3. Zorg voor een goede culturele match

Er moet een goede match zijn tussen de cultuur van jouw bedrijf en die van je vendor. Zo heeft bijvoorbeeld Accenture een uitstekende en beproefde methodologie, maar houden zij niet van veel wijzigingen. Is je business zeer veranderlijk en wijzigen de vereisten haast iedere week, dan ben je dus beter af bij een bedrijf zoals Capgemini, waar er een minder strenge methodologie is en men dus vatbaarder is voor wijzigingen. Beide bedrijven zijn topspelers, maar ieder heeft zijn eigen DNA.

4. Kijk verder dan de prijs

Nog te veel aankoopafdelingen werken enkel op de prijs van een deal. Bij IT-outsourcing gaat het echter over grote strategische deals, waarbij er naast de prijs nog andere en belangrijkere factoren zijn. Zorg er dus zeker voor dat je vendor nog een winstmarge heeft. Hem uitpersen zal je op lange termijn zeker niet de beste deal opleveren, want je zal dan ook niet de beste service krijgen.

> Bij IT-outsourcing gaat het over grote strategische deals waarbij er naast de prijs nog andere en belangrijkere factoren zijn.

5. Zorg voor een sterke governance

Op vlak van transities hebben bedrijven vaak nog niet zoveel ervaring. Dat vereist een sterk transitieteam. Daarnaast moet ook het 'demand management' op punt staan. IT-outsourcingbedrijven moeten voldoende op voorhand worden ingelicht over de toekomstige noden. Hiervoor moet het IT-departement meer op lange termijn kunnen denken en eisen dat de rest van het bedrijf daar ook rekening mee houdt. Een sterke governance laat ook toe om het innovatieproces zelf deels in handen te nemen in plaats van dat volledig over te laten aan de vendor. ■

04

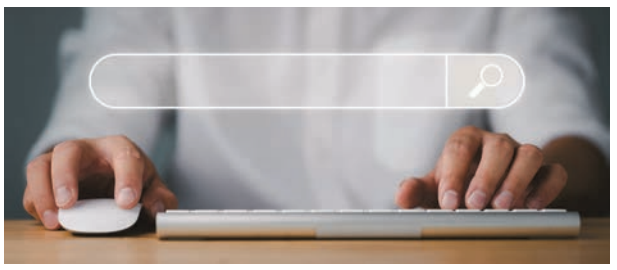
Duurzaamheid

Belgisch platform maakt het mogelijk om financiële en duurzame data te verbinden.

07

Cyber security

Volgens Koen Druyts blijft de mens de zwakste schakel in de veiligheidsketen.



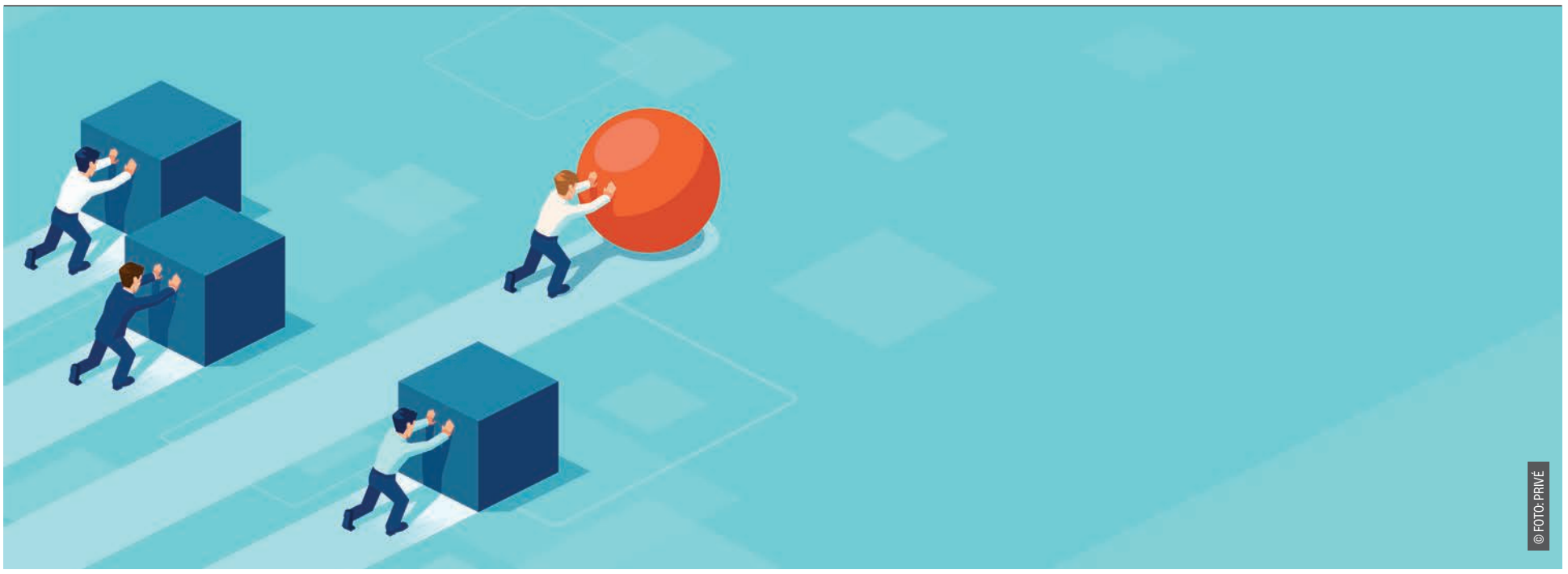
nl.planet-business.be

In de loop van 2023 lanceert het CCB een Safeonweb portal voor bedrijven, organisaties en overheidsdiensten. Lees er alles over op onze website.

VOLG ONS

Planet Business België
@MediaplanetBE
Mediaplanet Belgium
Mediaplanetbe
Mediaplanet Belgium

Managing Director: Leoni Smedts
Head of Production: Daan De Becker
Production Manager: Nicolas Mascia
Head of Digital: Stijn Rosiers
Digital Manager: Nicolas Michenaud
Business Developer: Laurens De Grave
Senior Project Manager: Jérémy Verkercke
E-mail: jeremy.verkercke@mediaplanet.com
Redactie: Joris Hendrickx, Valérie Deridder
Lay-out: i Graphic
E-mail: info@i-graphic.be
Print: Roularta
Distributie: Trends
Mediaplanet contactinformatie:
Tel: +32 2 421 18 20
redactie.be@mediaplanet.com
D/2022/12.996/43



© FOTO: PRIVÉ

IT-partner versterkt bedrijven in snel veranderend landschap

Computacenter scoort al jarenlang consistent goed in de Whitelane Survey. Dit jaar haalde het bedrijf zelfs een dubbele eerste plaats in de categorieën 'general satisfaction' en 'workplace & end-user compute'. Vanuit zijn goede band met de eindgebruikers op de werkvloer stelt het bedrijf enkele duidelijke trends vast waar het via technologie mee een antwoord op kan bieden. **Tekst:** Joris Hendrickx

Jurgen Strijkers

MANAGING DIRECTOR COMPUTACENTER

Sofie De Vos

DIRECTOR CONTRACTUAL SERVICES COMPUTACENTER

"Computacenter is actief in drie domeinen: workplace, network en data center. We verkopen technologie, implementeren deze en staan klanten bij in de transformatie die daarmee gepaard gaat", vertelt Managing Director Jurgen Strijkers. "Met onze managed services kunnen we klanten bovendien op een resultaatgedreven manier volledig ontlasten. In België hebben we een sterke focus op de eindgebruiker. Computacenter Group evolueert intussen richting een omzet van acht miljard euro en telt zo'n achttienduizend medewerkers. In België hebben we een tweehonderdtal medewerkers en nog eens honderd externe krachten, en realiseren we een omzet van rond de honderd miljoen euro. We richten ons vooral op grote internationale bedrijven die we vanuit België goed kunnen begrijpen én tegelijk vanuit de groep de gepaste service kunnen bieden."

Managed services als antwoord op war for talent

"Tegenover bedrijven waar IT geen deel uitmaakt van de kernactiviteiten is nieuw talent soms terughoudend. De laatste jaren zijn we immers geëvolueerd naar een kandidatenmarkt. Het is niet langer de werkgever die kan kiezen uit meerdere kandidaten, maar de kandidaten die een ruime keuze hebben aan potentiële werkgevers. Uiteraard is er binnen IT altijd een zekere schaarste geweest, maar het is nu toch meer uitgesproken geworden", aldus Strijkers. "Bij hun keuze is het voor kandidaten erg belangrijk geworden dat ze de strategie begrijpen en weten welke concrete groeimogelijkheden je bedrijf hen kan bieden. Tegelijk merken we dat onze klanten soms worstelen met die war for talent en daarom een beroep doen op ons om zichzelf te verzekeren van de toegang tot talent. Zo hoeven zij daar niet al hun tijd en middelen in te investeren, met het risico dat het talent binnen afzienbare tijd weer vertrekt."

Disruptieve markt vraagt om flexibiliteit en veerkracht

"Bedrijven willen zich goed laten omringen door partners zoals Computacenter om zichzelf continu in vraag te kunnen blijven stellen en uit te dagen. Zij weten immers dat het vandaag makkelijk is voor nieuwe spelers om de markt te betreden en met een vernieuwend idee het businessmodel van de bestaande spelers meteen onder druk te zetten. Meestal vragen ze daarom na een succesvolle samenwerking rond de werkplek om ook hun kernactiviteiten en -processen te digitaliseren en daarbij gebruik te maken van de beste nieuwe technologieën die beschikbaar zijn. Met de huidige politieke en economische onzekerheid is flexibiliteit erg belangrijk geworden. Bedrijven willen daarom een partner die schaalbaarheid kan aanbieden in plaats van een stug contract. Wanneer het nodig blijkt, kan dan men snel up- of downscalen. In dat kader volgen we onze managed services klanten ook echt. Net zoals in een huwelijk zijn we er in goede en in slechte tijden", klinkt het.

Langetermijnpartner versterkt klantgerichtheid en weerbaarheid

"Binnen de managed services hebben we de mogelijkheid om zwaar in te zetten op een customer en services mindset", vult collega Sofie De Vos, Director Contractual Services, aan. "Anderzijds bieden we ook de technologie en een leerpad voor nieuwe talenten aan. We vormen een sterk partnership met onze klanten en besteden veel aandacht aan de governance en de onderlinge relatie. Veel dingen die nu gebeuren bij klanten hebben wij bovendien zelf intern ook al ervaren. Zo kunnen we hen vanuit onze eigen ervaring helpen om te evolueren naar een 'as-a-service'-model. In de IT-wereld is deze evolutie immers al langer aan de gang. Maar ook op vlak van resilience zijn we fier dat we vaak langetermijnrelaties met onze klanten aangaan en dus samen al heel wat watertjes doorzwommen hebben. We kijken steeds naar wat de uitdagingen zijn waar zij mee te maken krijgen en hoe wij daar vanuit onze dienstverlening en technologie in kunnen helpen en de weerbaarheid kunnen verhogen. Digitalisering zorgt er bijvoorbeeld voor dat men kostenefficiënter kan gaan werken, wat uiteraard een enorme troef is in crisistijden. Dat vereist dan uiteraard wel een goede strategie."

"Een onderwerp dat bij veel bedrijven momenteel hoog op de agenda staat, is de ervaring van de eindgebruiker. Een bedrijf dat werknemers een goed uitgeruste en functionele digitale werkplek kan bieden, is beter gewapend op de arbeidsmarkt en kan optimaal inzetten op hybride en remote werken. Als workplace service provider die een impact heeft op zowel de werkplek als de IT-omgeving, is het onze core business om hiervoor te zorgen. Zo kunnen werknemers van onze klanten zich concentreren op de businessuitdagingen die op hen af komen, zodat zij hun bedrijf meer resilient kunnen maken", besluit De Vos. ■

Computacenter

Meer weten?
computacenter.com/en-be/who-we-are

Met de huidige politieke en economische onzekerheid is flexibiliteit erg belangrijk geworden. Bedrijven willen daarom een partner die schaalbaarheid kan aanbieden in plaats van een stug contract.

Een bedrijf dat werknemers een goed uitgeruste en functionele digitale werkplek kan bieden, is beter gewapend op de arbeidsmarkt en kan optimaal inzetten op hybride en remote werken.

© FOTO: PRIVÉ

Belgisch platform maakt duurzame vooruitgang meetbaar

Een innovatief Belgisch SaaS-platform maakt het mogelijk om alle data binnen bedrijven en organisaties met elkaar te verbinden, diepgaande ESG-inzichten te bieden én erover te rapporteren. Zo reikt het hen alle tools aan die nodig zijn om échte, meetbare vooruitgang te boeken op het vlak van duurzaamheid. Meer uitleg door Carl Seys en Pieter Feys, oprichters van Canary. **Tekst:** Joris Hendrickx

Carl Seys

OPRICHTER CANARY

Pieter Feys

OPRICHTER CANARY

Bedrijven hebben vaak een grote hoeveelheid data die verspreid zit over verschillende systemen en processen. Hierdoor moeten elk jaar alle data van de verschillende processen handmatig worden verzameld en verwerkt om vervolgens een jaarrapport te kunnen opstellen. Dat vraagt gigantisch veel inspanningen en brengt onzekerheid met zich mee dat alle data wel aanwezig en correct is. Bovendien is het meest actuele rapport per definitie al verouderd. Financiele en ESG-data zijn sterk met elkaar gelinkt, het zijn als het ware communicerende vaten. Zo kunnen milieu- of klimaat-technische problemen een directe impact hebben op de cijfers van de onderneming, maar omgekeerd kunnen de ondernemingsactiviteiten ook een bepaalde impact hebben waar men sneller op zou willen anticiperen."

All-in-one datagedreven platform voor duurzaamheid

"Wij brengen daarom via ons Canary platform al die data op een eenvoudige manier samen zodat we ze op dezelfde manier kunnen behandelen zoals gewoonlijk met financiële data. Met dit krachtige en flexibele dataplatform wordt het mogelijk om de data in realtime binnen te halen, automatisch verbanden te leggen en dit alles ter beschikking te stellen aan interne en externe stakeholders dankzij op maat gemaakte dashboards. Bovendien laat dit toe om inzichten te genereren, actieplannen op te maken, tijdig bij te sturen en de duurzame transitie echt mogelijk te maken. Afhankelijk van waar de data zich bevinden, kunnen we deze op verschillende manieren naar ons platform halen. Zo hebben we 'Catch' hardware om facilitaire data van bestaande systemen in het gebouw te koppelen, maar kunnen we evenzeer connecteren met de loondienst, het financiële departement en de productieprocessen. Zijn bepaalde data niet voorhanden, dan verkrijgen we die via een bevragingsmodule. Daarnaast kunnen we diverse types van gegevensbestanden importeren en zelfs koppelen met de database van een andere partij."

Transparantie leidt tot versterking op meerdere niveaus

"Heel wat bedrijven maken zich grote zorgen omdat bepaalde financiële indicatoren de pan uit swingen. Via ons platform kunnen zij echter inzicht krijgen vanwaar dat komt. Andere bedrijven willen bewust duurzamer worden en zo hun voortbestaan op lange termijn garanderen: een duurzaam bedrijf is immers veerkrachtiger en kan anticiperen op externe factoren. Bedrijven kunnen daarnaast ook gedreven worden door hun supply chain. Dat kan gaan over leveranciers of klanten die bepaalde verwachtingen hebben over een wederzijdse uitwisseling van data, die dan moeten verwerkt worden in ieders duurzaamheidsverslag. Of het kan gaan over investeerders of banken die de ESG-doelen hoog in het vaandel dragen. Daarnaast hechten steeds meer jonge talenten belang aan hoe duurzaam een bedrijf is, welke aandacht het heeft voor haar maatschappelijke rol en welke rol zij daar persoonlijk in kunnen opnemen."

> Financiële en ESG-data zijn sterk met elkaar gelinkt, het zijn als het ware twee communicerende vaten.

> Een duurzaam bedrijf is veerkrachtiger en kan anticiperen op externe factoren.

Kwaliteitsvolle, inzichtelijke en auditeerbare data

"Canary maakt je data kwaliteitsvol, inzichtelijk en auditeerbaar. We kunnen zelfs tot op het niveau van de ruwe data gaan. Op welke momenten is er wat gebeurd met de databehandeling? Welke conversiefactoren zijn toegepast? Een auditeur krijgt hiermee zeer concrete, duidelijke en bruikbare info die aan alle internationale rapportagenormen voldoet en zal deze dus sneller en makkelijker als echt kunnen valideren. Door in alle openheid de échte resultaten te tonen bewijs je dat je niets te verbergen hebt. Met zo'n transparantie minimaliseer je meteen ook proactief het risico dat een kritische of ontevreden stakeholder een onderzoek start en je in een verdedigingsmodus dwingt. Tegelijk weet je zo snel waar en hoe je moet ingrijpen. Ons platform kan zelfs real time data aan tot op het niveau van een specifieke asset, zoals een energievreter. In zoverre uiteraard dat deze info relevant is om snel negatieve impacten te kunnen herkennen en aanpakken."

Europese regelgeving pusht bedrijven richting volledige transparantie

"De Europese Green Deal zorgt voor heel wat nieuwe regels en standaardisatie. Daarenboven zal GHG reporting geïntegreerd worden in de Corporate Sustainability Reporting Directive (CSRD). Vanaf januari 2024 zullen de eerste organisaties in dat kader hun data moeten beginnen capteren. Uiteindelijk zullen in Europa meer dan 50.000 bedrijven en organisaties moeten voldoen aan de nieuwe duurzaamheidsregelgeving. Maar eigenlijk is het zelfs een veelvoud, want die bedrijven zullen vervolgens ook hun partners door de supply chain heen aanzetten om op een gestandaardiseerde manier data te verzamelen. Bedrijven beseffen dat er nog veel te gebeuren valt om te voldoen aan de nood van een snelle bijsturing van processen, en zo hun duurzaamheid veilig te stellen. Zij blijven echter worstelen vanaf de captatie van grote hoeveelheden data over inzichten tot aan de noodzakelijke hoogfrequente reporting. Canary lost dat tijds- en kostenefficiënt op." ■

“Inzetten op retentie is minstens even belangrijk als rekruteren”

De war for talent naar ICT-profielen stelt bedrijven meer dan ooit voor enorme uitdagingen, maar is die vaak agressieve zoektocht naar nieuw technisch talent wel de juiste aanpak? Thomas Vleugels (founder) en Piet Leemans (marketing strategist) van het Antwerps rekruteringskantoor Madison Recruitment, leggen uit hoe je het verschil kan maken. **Tekst:** Joris Hendrickx

Thomas Vleugels

FOUNDER
MADISON RECRUITMENT

MADISON RECRUITMENT

Meer weten?
madison.be

De voorbije twaalf maanden bedroeg de spanningsratio voor ICT-jobs bij VDAB maar liefst 0,30. Als rekruteringskantoor gespecialiseerd in ICT, Engineering en Supply Chain, zit Madison middenin het getouwtrek. Het kantoor heeft die markt voor, tijdens en na COVID stevig zien fluctueren, met als piekmoment de herfst en winter van 2021.

Welke evoluties hebben jullie vastgesteld de voorbije jaren?

Vleugels: “De vergrijzing, de digitalisatie en uiteraard COVID hebben de strijd om ICT-talent de laatste jaren fel geïntensifieerd. Het gedrag van Belgische bedrijven nam voor januari extreme vormen aan om toch hun slag te kunnen slaan: absurde tegenvoorstellen met excessieve loons- en pakketverhogingen, freelancetarieven ver boven het aanbod van bedrijven, enz. In de VS is die exuberante opbodcultuur een halfjaar geleden wel wat gaan liggen. We weten dat wat daar op de arbeidsmarkten ontstaat, hier meestal een halfjaar later gebeurt. En dat blijkt te kloppen: de gekte in België heeft zich stilaan weer hersteld naar het ‘normale’ niveau, waar de strijd nog wel steeds erg groot is.”

Wat maakt een job interessant voor potentiële kandidaten?

Vleugels: “De meeste bedrijven focussen nog steeds erg op verloning. Uiteraard is dat een cruciale factor, maar voor de schaarse ICT’er gewoonweg voor de hand liggend. Een belangrijke kanttekening is wel dat dankzij de recente/toekomstige indexsprongen en de inflatie het nog meer aangewezen zal zijn als bedrijf om je verloningspakket fiscaal te optimaliseren. IP-rechten, cafetariaplan, maaltijdcheques,... Al deze aspecten moeten juist zitten, en dat is nog altijd bij erg veel bedrijven niet het geval.”

Leemans: “Begrijp ons niet verkeerd. Loon is bij ICT’ers natuurlijk nog steeds één van de belangrijkste criteria tijdens hun zoektocht naar een nieuwe job. Het zijn echter de werkgevers die een goed loonpakket combineren met een duidelijke technologische strategie die de strijd veel vaker winnen. We zien dat trouwens niet alleen in onze eigen data. Veel studies tonen aan dat ‘het bereiken van een technologisch plafond’ dé belangrijkste factor is voor een ICT’er om van werkgever te switchen. Of ze worden freelancer, om zo zelf technologische invulling te geven aan hun job. De jaarlijkse survey van Stack Overflow leert ons zelfs dat meer dan 60% van de Belgische softwareontwikkelaars openstaat voor nieuwe opportuniteiten. Concreter startte bijna 60% de voorbije twee jaar bij een nieuwe werkgever. Waarom? Omdat ze technologisch niet genoeg geprikkeld werden. Het antwoord op de ‘war for talent’-vraagstuk is dus zeker niet alleen ‘het optimaal aantrekken van nieuw talent’.”

Wat is dan jullie belangrijkste boodschap naar bedrijven toe?

Vleugels: “We spreken misschien tegen onze eigen winkel, maar investeer in een goed retentiebeleid! Bied naast een goede verloning ook technologische uitdaging en perspectief. Die investering is beduidend lager dan het aanwerven van nieuw personeel. De totale kost om een vertrekkende, ingeburgerde ICT’er op te vangen, is immers veel hoger dan louter de prijs voor zijn of haar vervanger. Je moet ze eerst vinden, opleiden, vertrouwd maken met de omgeving, producten, enz. Bovendien trekken gelukkige, bekwame ICT’ers andere getalenteerde mensen aan.”

Leemans: “We zien hier trouwens al grote verschillen tussen pure, vaak kleinere ICT-bedrijven en grote, logge spelers die een ICT-afdeling hebben. De zuivere ICT-huizen zijn veel beter in staat om in te spelen op het dynamische karakter van dat wereldje. Technologieën of methoden die gisteren relevant waren, kunnen vandaag volledig voorbijgestreefd zijn. Je moet snel kunnen draaien met die technologische winden.”

Vleugels: “Een ICT’er voelt dat ook meteen aan. Wij spreken maandelijks honderden softwareontwikkelaars, data-analisten, leidinggevenden en freelancers. Dat zijn stuk voor stuk gepassioneerde mensen die permanent bezig zijn met de ontwikkeling van hun technologisch traject. Als je hen wil houden, moet je hen dus absoluut dat perspectief bieden. We zien het laatste jaar ook vaker dat bedrijven hun eigen ICT’ers mee betrekken bij hogere technologisch beslissingsprocessen. Combineer dat met technische interne opleidingen en je kan veel sneller inspelen op technologische ontwikkelingen. Bovendien wordt je eigen personeel geprikkeld en betrokken, waardoor het verloop afneemt.” ■

Het zijn de werkgevers die een goed loonpakket combineren met een duidelijke technologische strategie die de strijd om talent winnen.

Maar liefst 60% van de software-ontwikkelaars startte de voorbije twee jaar bij een nieuwe werkgever.

pathlock

The New Leader in Application Security and Controls Automation

GRC	Data Security	Application Security
Role design and Re-design	Transaction Monitoring	Vulnerability Management
Compliant Provisioning	Data Masking	Code Scanning
Separation of Duties and Risk Analysis	Control Enforcement and Transaction Blocking	Continuous Control Monitoring
User Access Certification and Review	Dynamic Authorization	Detection and Response
Privileged and Temporary Access Management	Adaptive Policy	Logging and SIEM Integration

Please contact **johan.hermans@pathlock.com** for more information.

NOW PART OF PATHLOCK

CSI tools · APPSIAN SECURITY · Q Software · SECURITY WEAVER · SAST

i Druyts: “Mensen moeten leren dat ‘1234’ geen veilig paswoord is, dat enkel websites met ‘https’ in de url veilig zijn en dat je in e-mails van onbekende zenders niet zomaar op links mag klikken.”

“Ieder bedrijf moet zich gedragen als een goede huisvader”

Geen enkel bedrijf is immuun voor cyberrisico’s. Het is daarom cruciaal om je hiertegen te wapenen met een combinatie van preventieve maatregelen en de juiste bijstand in geval van een incident. Koen Druyts, mede-oprichter van CyberContract, legt uit hoe je de risico’s kan beperken. **Tekst:** Joris Hendrickx

Koen Druyts

MEDE-OPRICHTER CYBERCONTRACT

CyberContract

Meer weten?
cybercontract.eu

Welke uitdagingen stellen zich vandaag op het vlak van cyberveiligheid?

“Dé belangrijkste uitdaging met een enorme impact is ransomware. Verzekeraar AIG zag de uitgekeerde schade toenemen van 325 miljoen USD in 2018 naar twintig miljard in 2021. Ze verwachten dat dit bij ongewijzigde preventie tegen 2025 zelfs zal stijgen naar tien triljard USD. Maar meer nog dan een verhoogde preventie is vooral meer bewustzijn nodig bij bedrijfsleiders en directieleden. Vandaag kan je op het darkweb immers ransomware ‘as-a-service’ bestellen tegen een erg lage prijs. Daarnaast kan je je laten uitbetalen in niet-traceerbare cryptomunten. Bovendien bestaan er safe havens voor hackers. De impact van cyberincidenten – crimineel of niet – wordt ook alsmaar groter. Bedrijven in eender welke sector worden immers steeds afhankelijker van IT. Vooral de impact van bedrijfsonderbrekingen is enorm.”

Waarom is het zo belangrijk om hier proactief mee bezig te zijn?

“Ieder bedrijf moet zich gedragen als een goede huisvader. Net zoals je je woning steeds op slot doet en het alarm activeert wanneer je weggaat, dient ieder bedrijf zich proactief te beschermen tegen cyberrisico’s. Mensen moeten leren dat ‘1234’ geen veilig paswoord is, dat enkel websites met ‘https’ in de url veilig zijn en dat je in e-mails van onbekende zenders niet zomaar op links mag klikken. Cyberrisico’s kunnen je bedrijf platleggen en zelfs failliet laten gaan. Een attitudeverandering is dus essentieel, want de mens is nu eenmaal de zwakste schakel die het veiligheidsniveau van je bedrijf bepaalt. Kijk naar de recente hack van Uber: die begon met sociale engineering en een werknemer die zich liet vangen. De eerste stap is dus niet de aankoop van een IT-tool, maar wel investeren in het trainen van je werknemers. Je bedrijf beschermen, kan natuurlijk ook niet zonder technologische beveiliging. Het komt er daarbij wel op aan om een goede balans te vinden tussen gebruiksgemak en beveiliging. Tweefactorauthenticatie is in dat opzicht alvast een grote meerwaarde.”

Op welke manier vult een cyberriskverzekering deze preventieve maatregelen verder aan?

“Een nulrisico bestaat niet. Je kan je woning nog zo goed beveiligen tegen brand of diefstal, er blijft steeds een risico over dat je best verzekert. Hetzelfde geldt voor cyberrisico’s. Enerzijds zal je zonder preventieve maatregelen geen adequate verzekering vinden. Anderzijds is een maximale beveiliging onbetaalbaar. Het komt er dus op aan om eerst een redelijke inspanning te doen op het vlak van preventieve beveiliging en het restrisico af te dekken met een verzekering.”

Hoe helpt CyberContract als gespecialiseerde aanbieder van cyberriskverzekeringen bedrijven om een risicoassessment te maken?

“Met CyberTest.be lanceerden we een onafhankelijke online zelftest waar je als bedrijf op basis van een korte vragenlijst je eigen cyberveiligheid in kaart kan brengen. Het resultaat is een radardiagram waar je risicodomeinen en te nemen acties worden afgewogen ten opzichte van waar je de grootste schade mag verwachten. Vandaag beseffen verzekeraars overigens dat cyberveiligheid vaak een systemisch gegeven is. Als er iets gebeurt, heeft dat vaak een effect op grote delen van de portefeuille. Hierdoor worden verzekeraars steeds strenger. Die screening incorporeren wij uiteraard ook mee in onze werking. Daarnaast werken we volop aan de uitbouw van een ecosysteem en investeren we in de versterking van de intussen meer dan 150 professionele makelaars waarmee we samenwerken. Een makelaar is als risicospecialist immer de geknipte persoon om bedrijven te adviseren over cyberrisico’s.”

> De mens is de zwakste schakel die het veiligheidsniveau van je bedrijf bepaalt.

> Het komt er steeds op aan om eerst een redelijke inspanning te doen op het vlak van preventieve beveiliging en het restrisico af te dekken met een verzekering.

“We werken ook samen met Belgische specialisten aan de ontwikkeling van een set niet-intrusieve testen die we op de achtergrond kunnen laten lopen. Zo kunnen we bedrijven een aanbod doen waarbij zij op een eenvoudige manier een idee krijgen van hun cyberveiligheid, uitgenodigd kunnen worden voor relevante seminaries of kunnen zoeken naar aanbieders van diensten die kunnen helpen om hun cyberveiligheid te verhogen.”

Op welke bijstand kunnen bedrijven rekenen wanneer het misloopt?

“Veel kmo’s hebben geen uitgeschreven en getest businesscontinuityplan, en als ze dat al hebben zijn cyberrisico’s daar vaak niet in opgenomen. Hierdoor weten ze ook niet waar ze terechtkunnen bij een incident en hoe ze zich dan moeten organiseren. Het feit dat ze op dat moment volledig offline zijn en hun IT uitligt, maakt de chaos compleet. Daarom hebben we een unieke hotline die 24/7 bereikbaar is in geval van een incident. We werken hiervoor samen met gerenommeerde en gerespecteerde specialisten zoals CRONOS Security en Johan Vandendriessche.”

“Ons eerste doel is om ervoor te zorgen dat het incident en dus de schade zo klein mogelijk blijven. Dat is niet enkel goed voor de verzekeraar, maar ook voor het bedrijf omdat het dan sneller terug operationeel is. Bij een gebrek aan een business continuity plan moeten we soms bv. ransomware betalen aan hackers omdat dat de enige manier is om de schade klein te houden of de klant weer operationeel te krijgen. Het nadeel daarvan is dat je een crimineel ecosysteem voedt en dus groter en sterker maakt.”

“Sowieso betrekken we ook altijd meteen de eigen IT-partner van de klant. In tweede instantie kijkt onze hotline naar de diepliggende oorzaken van het incident. Op die manier krijgt de verzekeraar zicht op wat er precies is gebeurd en hoeven onze klanten zelf geen aangifte meer te doen.” ■

Debat

“Digitaal vertrouwen zal ervoor zorgen dat bedrijven veerkrachtig zijn”

De digitalisering blijft zich razendsnel verderzetten. Naast de vele voordelen die daarmee gepaard gaan, krijgen bedrijven ook met enkele valkuilen af te rekenen. Welke zijn dit en hoe kunnen we hier een antwoord op bieden? Wij brachten vijf experten samen voor een open gesprek over de toekomst van IT en het belang van cyberveiligheid in dat evoluerende landschap.

Tekst: Joris Hendrickx

Hoe kunnen bedrijven mee blijven met de snelle evoluties in de IT-wereld?

Danielle Jacobs: “Elk jaar vragen wij onze leden wat hun huidige prioriteiten zijn. Bij de meest recente bevraging zagen we dat er in de top tien maar liefst vijf te maken hebben cyber security.”

Antonietta Mastroianni: “In de telecomsector is momenteel iedere operator aan het evolueren van klassieke telecom naar het aanbieden van ecosystemen voor B2C-klanten. Ze treden daarbij buiten hun kernactiviteiten en worden ook actief in gezondheid, financiën, energie,... Ook B2B-klanten willen steeds vaker volledig geïntegreerde en veilige end-to-endoplossingen die ook nog eens snel en gebruiksvriendelijk zijn.”

Ine Segers: “Dé grote uitdaging voor veel bedrijven is om hun continuïteit te verzekeren. Tegelijk moeten ze hun concurrentievoordeel behouden. De vraag die velen zich stellen, is hoe ze dat op de efficiëntste en snelste manier kunnen doen. Het is in dat kader cruciaal dat ze zich laten adviseren door ervaren en gespecialiseerde partners.”

Jan De Blauwe: “Er is enerzijds een enorm potentieel voor bedrijven om hun diensten op een meer geïntegreerde manier aan te bieden. Anderzijds kunnen backofficeprocessen via digitalisatie en automatisatie heel wat efficiënter worden gemaakt. Zeker in het licht van de huidige inflatie en energiecrisis kijken veel bedrijven naar IT als een middel om hun groei te blijven verzekeren.”

Danielle Jacobs
CEO BELTUG

Regelgeving wordt alsmaar belangrijker in de digitale wereld. De hoeveelheid aan data blijft groeien, maar tegelijk is de grote vraag wie eigenaar is van die data.

Egide Nzabonimana: “Er moet een digitaal vertrouwen worden ingebouwd in alle interacties met klanten, partners en leveranciers, maar ook in alle transities waar externe partijen bij betrokken worden is dat noodzakelijk. Digitaal vertrouwen zal ervoor zorgen dat bedrijven veerkrachtig zijn.”

Danielle Jacobs: “Bedrijven zoeken ook naar manieren om hun medewerkers bewust te maken en scherp te houden wanneer het op cyberveiligheid aankomt. Daarnaast is er in veel bedrijven nog een grote kloof tussen de CIO en het bestuur. CIO’s hebben vaak moeite om uit te leggen waarom het budget voor cyberveiligheid zou moeten worden verhoogd.”

Antonietta Mastroianni: “De rol van IT is compleet aan het veranderen. Het neemt nu een meer centrale en zelfs leidende rol op in het bedrijf. Niet iedereen is klaar voor die shift, maar toch zal het gebeuren.”

Waar is de moderne IT-klant vooral naar op zoek?

Antonietta Mastroianni: “In de telecomsector is men vooral op zoek naar geïntegreerde diensten, maar ook unified communications, procesautomatisatie, low latency

© FOTO'S: MAARTEN DE BOUW

technologies en Internet of Things (IoT) zijn momenteel hot topics. Dat vereist uiteraard wel de juiste steun. Telecom- en IT-bedrijven kunnen hier een belangrijke rol in opnemen om dat veilig te laten verlopen."

Danielle Jacobs: "Ook in onze survey zagen we dat IoT momenteel al in de top tien staat van prioriteiten, en ieder jaar neemt het belang ervan toe. Veiligheid speelt uiteraard ook op dat vlak een cruciale rol, want alles zal met elkaar worden geconnecteerd."

Ine Segers: "Het brengt vooral een ander soort van bedreigingen met zich mee. Aangezien alles gedigitaliseerd en geautomatiseerd is, kunnen criminelen je infrastructuur makkelijk misbruiken. Soms zie je nu eenmaal niet meer waar de potentiële bedreigingen en zwakheden zich bevinden. Dat vergt een compleet nieuwe manier van het beoordelen van en omgaan met risico's, ook vanuit het bestuur."

Antonietta Mastroianni: "Security as a Service zal in belang toenemen. Bedrijven kunnen hierdoor steunen op een team van experten, zowel in het geval van een cyberaanval of crisis als voor preventie en detectie."

Danielle Jacobs: "Voor de interne IT'ers in een bedrijf zal dit vaak te complex worden. Daarom zal er inderdaad een grote shift zijn naar het uitbesteden van cyberveiligheid aan externe experts."

Jan De Blauwe: "Veel bedrijven denken momenteel na over wat ze zelf nog willen doen en wat ze liever uitbesteden, ook wanneer het IT betreft. Enerzijds biedt IT een toolset die extreem krachtig is, die nauw verbonden is met de kern van het bedrijf en die dus een grote strategische waarde heeft. Anderzijds outsourcen bedrijven vaak heel belangrijke IT-managementverantwoordelijkheden naar cloud providers, zodat ze zich zelf meer kunnen focussen op de functionele laag die ze daarop kunnen bouwen."

Wat zijn vandaag de risico's op vlak van cyberveiligheid?

Ine Segers: "Cyberrisico's gaan in feite steeds over blootstelling. Het moeilijkste is om te identificeren waaraan je blootgesteld bent. Vervolgens moet je bepalen wat de impact is. Het heeft immers geen zin om veel geld uit te geven aan risico's die weinig impact hebben. Op basis daarvan kan je dan je riskmanagementstrategie uitbouwen."

Egide Nzabonimana: "Bedrijven moeten dat niet enkel voor zichzelf doen, het is hun plicht naar alle partners en klanten toe om ervoor te zorgen dat er vertrouwen kan zijn in hoe ze omgaan met digitalisering en hun data. Alles staat met elkaar in interactie. Wie zijn data ergens achterlaat, moet zeker kunnen zijn dat die op de juiste manier wordt behandeld. Bedrijven moeten dus op elk moment waken over de integriteit daarvan en de juiste voorbereidingen treffen op vlak van risicomanagement indien er toch iets fout loopt. Dat is trouwens ook cruciaal voor hun reputatie. Blijkt hier niet voldoende aandacht aan te zijn besteed, dan is het vertrouwen voor altijd verbroken. En je reputatie herwinnen, is een moeilijke én kostelijke zaak."

Danielle Jacobs: "Je moet als bedrijf enerzijds de veiligheid van je eigen systemen in orde hebben, maar je moet er ook op toezien dat je IT-provider de gepaste maatregelen neemt. Dat heeft inderdaad te maken met vertrouwen."

Ine Segers: "De meeste recente cyberaanvallen waren allemaal gebaseerd op de samenwerking tussen bedrijven en derde partijen. De aanval werd daarbij uitgevoerd via de derde partij."

Antonietta Mastroianni: "Zeker voor de bedrijven met heel wat legacysystemen vormt dat een grote uitdaging. Hun data bevinden zich op diverse locaties en zijn vaak verzameld in tijden dat er nog minder strenge regels golden. Veel bedrijven, waaronder ook Proximus, proberen daarom om over te schakelen van DevOps naar SecOps. Daarbij staat cyber security in elke fase van de levenscyclus van producten of projecten centraal. Het is extreem belangrijk om security vanaf het begin mee te nemen, maar ook in bestaande omgevingen moet je goed onderzoeken of er ergens mogelijke bedreigingen zijn."

Wat is de rol van de mens vs. die van automatisering en artificiële intelligentie?

Ine Segers: "Als je enkel vertrouwt op artificiële intelligentie (AI) en automatisatie zullen die valse positieven identificeren die eigenlijk geen probleem vormen. Er zijn dus altijd mensen nodig die kunnen valideren wat geautomatiseerde systemen doen."

Egide Nzabonimana: "Uiteindelijk is AI slechts een tool die organisaties kan helpen om de juiste beslissingen te maken en sneller zaken te detecteren, maar de menselijke factor blijft essentieel bij het maken van belangrijke beslissingen. Door de digitalisering moeten bedrijven matuurder worden, zowel wat betreft hun medewerkers als hun processen. Enkel dan kunnen ze, wanneer dat nodig is, snel en correct reageren. 100% veiligheid bestaat immers niet."

Jan De Blauwe: "AI is niet enkel een instrument dat cyberveiligheidsteams kan helpen. Het kan vooral ook worden aangewend om de business te laten groeien. Wanneer bedrijven data-analyse beginnen toe te passen, moeten ze ervoor zorgen dat cyberveiligheid deel uitmaakt van het design én dat de medewerkers getraind zijn in het omgaan met risico's en het herkennen van een incident."

Lees het vervolg van dit debat op pagina 10-11.

Egide Nzabonimana

VOORZITTER ISACA BELGIUM EN CO-FOUNDER SOCRAI

AI is slechts een tool die organisaties kan helpen om de juiste beslissingen te nemen en sneller zaken te detecteren, maar de menselijke factor blijft essentieel.

Antonietta Mastroianni

CHIEF DIGITAL & IT OFFICER PROXIMUS

De rol van IT is compleet aan het veranderen. Het neemt nu een meer centrale en zelfs leidende rol op in het bedrijf.

Danielle Jacobs: "De hoeveelheid aan data blijft maar groeien, maar tegelijk is de grote vraag vaak wie eigenaar is van die data. Met wie deel je je data en wie is er verantwoordelijk voor? We hebben al meermaals meegemaakt dat bedrijven een mooie AI-software laten ontwikkelen door een partner, die achteraf dan op basis van de inzichten uit die samenwerking de software verder verkoopt aan de concurrenten van de klant. Het delen van data, bijvoorbeeld in een ecosysteem, vormt dus een enorme uitdaging."

Antonietta Mastroianni: "Ook met AI blijven mensen voorop staan, maar het kan uiteraard een enorme meerwaarde betekenen in het dagelijkse leven van die mensen. Zo zullen zij zich meer kunnen focussen op creatieve taken, terwijl AI eerder de repetitieve taken overneemt. De mindset van de mensen zal dan wel moeten veranderen. In plaats van één job te leren en die dan steeds op dezelfde manier te blijven uitoefenen, zullen mensen eerder actief participeren in de innovatie en de creativiteit van de oplossing."

Hoe belangrijk zijn regels en richtlijnen?

Antonietta Mastroianni: "Bij Gaia-X werken we momenteel aan een verfijning van de richtlijnen opdat data niet op de foute manier worden gebruikt. Ook werken we aan de creatie van veilige dataspaces waar bedrijven die elkaar vertrouwen op vlak van security en privacy de krachten kunnen bundelen."

Danielle Jacobs: "Regelgeving wordt alsmaar belangrijker in de digitale wereld. Security en privacy zijn erg veelzijdig geworden, en dat is nieuw voor bedrijven."

Antonietta Mastroianni: "Vandaag is iedereen een concurrent van iedereen. We bieden bijvoorbeeld mogelijkheden voor onze klanten in de financiële/bancaire sfeer. Maar Proximus zet ook ten volle in op energie met zijn oplossingen om het energiebeheer te monitoren en te verminderen. Tegelijk gaan we enorm veel partnerships aan, zelfs met concurrenten. Het landschap is dus erg complex geworden. Regulering op vlak van security en privacy is daarom erg belangrijk. Veel mensen zijn zich immers zelf niet bewust van de waarde van de data die ze genereren."

Danielle Jacobs: "Samen met de CIO-associaties van andere landen geeft Beltug input aan de Europese Commissie voor het vormgeven van de Data Act. Die zal bepalen wie welke verantwoordelijkheid draagt en hoe data kunnen worden gedeeld. Maar we zullen ook modelcontractclausules voorstellen zodat niet iedereen het wiel opnieuw moet uitvinden."

Ine Segers: "De regelgeving zegt vaak wat er moet worden gedaan, maar niet hoe dat moet gebeuren. Dat maakt het erg moeilijk voor bedrijven. Een goed voorbeeld daarvan is de GDPR. De regels daarvan zijn duidelijk, maar hoe kan je je er als bedrijf aan houden?"

Egide Nzabonimana: "Eigenlijk gaat dit allemaal over data-integriteit. Bedrijven die samenwerken en daarbij data delen, moeten op dezelfde lijn zitten over welke data op welke manier kan worden gebruikt. Ze moeten op een even hoog beveiligingsniveau zitten. Regulering kan één van de oplossingen zijn hiervoor, maar innovatie is minstens even belangrijk. Alles evolueert zo snel dat je als bedrijf de dingen ook anders moet aanpakken. Voor elk bedrijf is dat trouwens anders, waardoor je in een ecosysteem verschillende werkwijzen zal tegenkomen."

Ine Segers: "De digitale identiteit speelt hierin een sleutelrol. Daarmee kan je duidelijk aangeven welke data open zijn en dus mogen worden gebruikt door derde partijen. Het laat je daarnaast ook toe om de toegang tot bepaalde data te autoriseren."

Antonietta Mastroianni: "Het lijkt me erg belangrijk om, gezien de evolutie richting ecosystemen, één digitale identiteit te hebben. Zo kan je je veilig voelen. Terwijl het vroeger eerder ging over de veiligheid van het netwerk, gaat het nu over de applicaties waarmee je toegang krijgt tot het netwerk."

Ine Segers: "Er is inderdaad een shift van 'on premise' - waar je strikte grenzen hebt - naar een identiteit die toegang krijgt tot bepaalde data, waar die zich ook bevindt."

Zouden certificaties kunnen helpen om het digitale vertrouwen te garanderen?

Egide Nzabonimana: "Het zou zeker een goede stap kunnen zijn. Ze garanderen immers dat alle grote en kleine bedrijven met dat certificaat op hetzelfde niveau zitten. De Cybersecurity Act zal op dat vlak alvast voor een grote shift zorgen bij bedrijven. Een certificaat houdt in dat ieder bedrijf weet welke overeengekomen stappen het moet ondernemen wanneer het fout gaat. Het zorgt er ook voor dat iedereen dezelfde taal spreekt. Maar het helpt ook om de maturiteit van de community en het ecosysteem te verhogen."

Danielle Jacobs: "In het licht van de Europese Cybersecurity Act hadden we hierover gesprekken met andere Europese associaties. We geloven zeker in certificatie, maar willen tegelijk ook niet dat te hoge standaarden innovatie bemoeilijken. We werken momenteel aan een checklist met vragen over cyberveiligheid die bedrijven kunnen stellen aan hun IT-provider."

Ine Segers: "Certificatie is in feite een framework dat je ondersteunt om op een matuur niveau te werken."

Egide Nzabonimana: "Bedrijven zijn met elkaar geconnecteerd. Met ISACA verzamelen we wereldwijd meer dan 165.000 mensen die in diverse omgevingen en bedrijven werken. Onze leden delen kennis en ervaringen met elkaar, wat professionals enorm helpt om vooruit te blijven gaan. We gaan daarmee verder dan certificaties, die inderdaad eerder een framework vormen dat ieder bedrijf anders kan toepassen. Het zorgt er ook voor dat iedereen dezelfde taal spreekt."

Antonietta Mastroianni: "Gaia-X werkt momenteel aan het definiëren van labels voor dataspaces. Er zullen duidelijke regels gelden om binnen een bepaald niveau te vallen. Op die manier kunnen partners die op hetzelfde niveau zitten op vlak van veiligheid en privacy elkaar in alle vertrouwen toelaten in hun dataspace."

Jan De Blauwe: "Certificatie en standaarden zijn misschien geen perfecte tool, maar kunnen wel zeer waardevol zijn. Ze helpen om vertrouwen te bouwen. Zonder het framework van certificaties is het erg complex om transacties met andere partijen te standaardiseren. Je zou

Ine Segers

BUSINESS UNIT MANAGER CYBER TRUST DEVOTEAM BELGIUM

Dé grote uitdaging voor veel bedrijven is om hun continuïteit te verzekeren. Tegelijk moeten ze hun concurrentie-voordeel behouden.

Jan De Blauwe

VOORZITTER CYBER SECURITY COALITION EN MANAGING DIRECTOR NVISO

Zeker in het licht van de huidige inflatie en energiecrisis kijken veel bedrijven naar IT als een middel om hun groei te blijven verzekeren.

telkens terug vanaf nul moeten beginnen. Maar het moet dan wel internationaal gebeuren, het heeft weinig zin om deze lokaal op te stellen."

Danielle Jacobs: "De NIS Directive zal in alle landen van de Europese Unie worden ingevoerd. Uiteraard kan ieder land er wel deels zijn eigen invulling aan geven."

Egide Nzabonimana: "We moeten ervoor zorgen dat professionals dezelfde taal spreken en elkaar makkelijk begrijpen. Daarom werken we bij ISACA aan certificaties waardoor bedrijven zeker kunnen zijn dat zij de nodige kennis en vaardigheden hebben. Er zullen verschillende certificaties zijn voor ieder domein: governance, security, risk management,... Hierdoor ontstaat een gemeenschappelijk framework en zit iedereen op dezelfde lijn over de verwachtingen. Daarnaast zetten we in op het delen van content. In dat kader werken we nauw samen met de Cyber Security Coalition en Beltug. Tot slot tekenen alle leden van ISACA een ethische code die als doel heeft om meer vertrouwen te brengen in de community."

Hoe kunnen we alle cybersecurityprofessionals op hetzelfde niveau brengen én houden?

Ine Segers: "Het is zeker een uitdaging om mensen up-to-date te houden rond nieuwe technologieën. Het zou in dat kader een enorme meerwaarde zijn indien alle vendors dezelfde taal zouden spreken. Dat is nu totaal niet het geval. Bedrijven kunnen hierdoor heel moeilijk verschillende oplossingen met elkaar vergelijken. Er is nood aan een framework met een gedeelde terminologie. Zo zullen bedrijven alles makkelijker kunnen begrijpen en evalueren, en zullen consultants sneller mee kunnen zijn met nieuwe technologieën."

Jan De Blauwe: "Bij NVISO leggen we tijdens het rekruteringsproces cases en uitdagingen voor aan kandidaten waarmee zij hun vaardigheden kunnen demonstreren. Daarnaast investeren we sterk in gespecialiseerde trainingsprogramma's, aangevuld met on the job-training. Maar het blijft natuurlijk een uitdaging. Toch zie ik het liever zo dan een bedrijf dat op enkele interne IT-mensen steunt waarvan het veronderstelt dat het ook experten op het vlak van cybersecurity zijn. Onze experten richten zich voltijds op dit domein, waardoor ze diepgaande en meer relevante vaardigheden ontwikkelen."

Danielle Jacobs: "Het maakt in die zin niet uit hoe groot of klein je bedrijf is. Het is vooral belangrijk op welke mensen je kan rekenen voor je cyber security."

Ine Segers: "Veel hangt ook af van hun passie. Hands-ontraining en een omgeving waar zij continu kunnen blijven leren, zijn cruciaal."

Egide Nzabonimana: "Bij de verschillende events die we organiseren, merken we dat mensen elkaar uitdagen en van elkaar leren. We moeten mensen van verschillende bedrijven dus met elkaar connecteren, zodat ze oplossingen kunnen bedenken en ideeën kunnen uitwisselen over gemeenschappelijke uitdagingen. Dat helpt om hun vaardigheden te verbeteren."

Ine Segers: "Hackathons en 'capture the flag'-competities zijn interessante manieren om mensen samen te brengen en uit te dagen."

Wat zal de impact van 5G zijn?

Antonietta Mastroianni: "Bij 5G en glasvezel is het niet zozeer het netwerk op zich dat een grote impact heeft, maar wel het enorme aantal mogelijkheden waar we ons zelfs vaak nog niet bewust van zijn. 5G is ongetwijfeld een technologie die onze manier van leven volledig zal veranderen, denk maar aan slimme steden, zelfrijdende wagens, de gezondheidszorg, energieconsumptie,... In al die domeinen zal de beperking van de latency wegvallen. Reacties zullen onmiddellijk gebeuren en betrouwbaar zijn."

Danielle Jacobs: "5G is de infrastructuur van de toekomst. Er zijn enorm veel digitale innovaties, maar het is ook cruciaal dat we erop kunnen vertrouwen. Dat vereist een gegarandeerde communicatie waarbij geen uitval mogelijk is. We kunnen ons momenteel zelfs nog niet voorstellen welke mogelijkheden er alleen al binnen de B2B-omgeving zullen zijn. Het ongeziene kwaliteitsniveau en het wegvallen van de latency zullen werkelijk voor een revolutie zorgen."

Antonietta Mastroianni: "Ik herinner me dat er twintig jaar geleden al ongelofelijk innovatieve technologieën en ideeën bestonden, maar wegens een gebrek aan snelheid en betrouwbaarheid in de communicatie was het nog te riskant om deze te lanceren. Het wegvallen van die limieten zorgt nu voor haast onbegrensde opportuniteiten."

Danielle Jacobs: "Na het aflopen van de 5G-veilingen is dé grote vraag bij bedrijven wat er zal gebeuren op de markt, en wanneer dat zal gebeuren."

Ine Segers: "5G zal niet enkel de wereld veranderen, maar ook de risico's en hoe we die vanuit een cybersecurityperspectief moeten behandelen. Cybercriminelen zullen nieuwe manieren zoeken om hun slag te slaan, dus we moeten ons daarop voorbereiden."

Danielle Jacobs: "Meer data en meer connecties zorgen inderdaad voor nieuwe risico's."

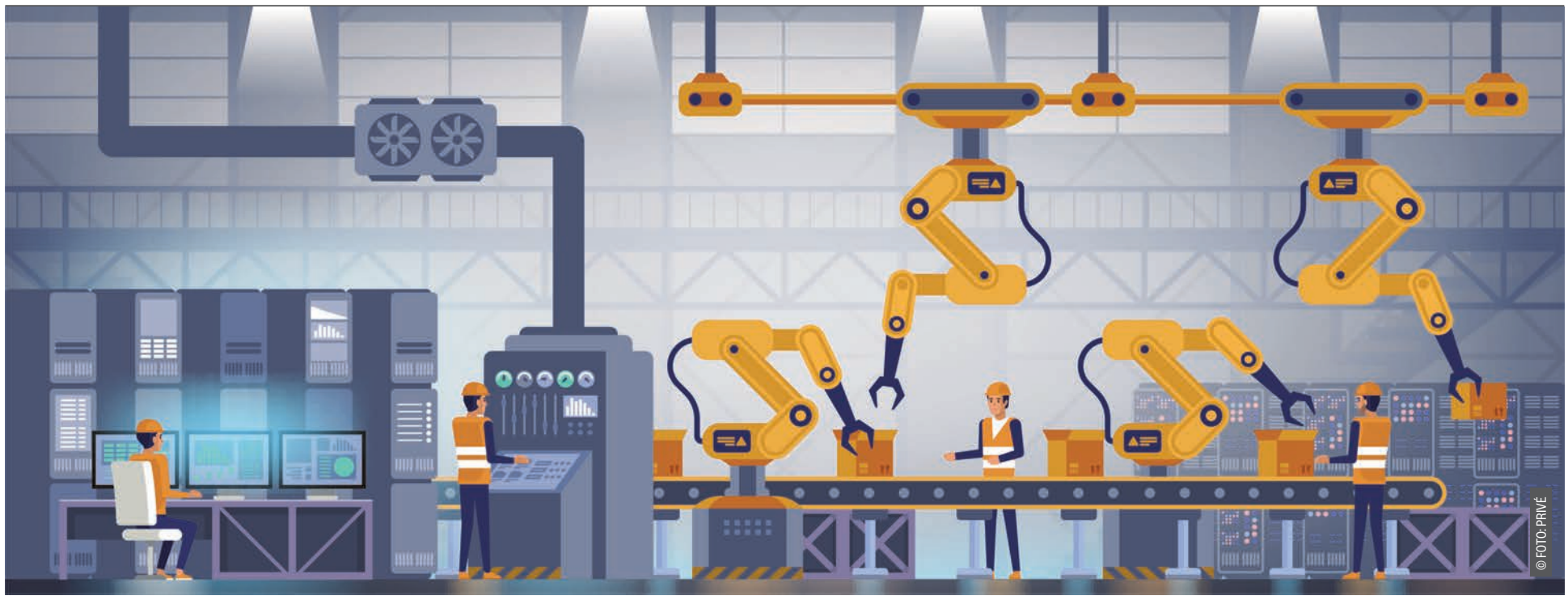
Antonietta Mastroianni: "Er zijn ook heel wat vragen over ethiek. Machines moeten immers instructies krijgen. Mensen blijven zichzelf altijd uitdagen, maar machines doen dat niet."

Ine Segers: "Betrouwbaarheid is cruciaal. Als er toch iets gebeurt, zal de impact vaak enorm zijn."

Jan De Blauwe: "5G is een fantastische innovatie, maar we moeten ook waakzaam zijn over onze enorme afhankelijkheid hiervan. De onderliggende structuur moet daarom zeer betrouwbaar zijn."

Antonietta Mastroianni: "Wanneer een machine voor erg gevoelige taken afhankelijk is van een netwerk, dan zijn de betrouwbaarheid, snelheid en precisie van dat netwerk inderdaad cruciaal."

Egide Nzabonimana: "5G creëert vooral heel wat opportuniteiten. Het is enorm snel, waardoor de impact bij een incident ook wel veel groter kan zijn. Bovendien gaat het over veel kleine devices en applicaties die allemaal onderling geconnecteerd zijn. We moeten dus waakzaam zijn voor wat kan gebeuren en hoe we daarop kunnen reageren. Het komt dus aan op een goede voorbereiding en een design waar veiligheid integraal deel van uitmaakt." ■



“Als een OT-systeem platligt, wordt een hele productieketen onderbroken”

Is een veilige OT-omgeving minder belangrijk dan een sterke IT-infrastructuur? Niet als je het aan Pascal Vercammen en Misja Caluwé van Process Automation Solutions vraagt. “Het klopt dat IT vooral focust op veiligheid, maar als een OT-systeem platligt, wordt een hele productieketen onderbroken. Vaak met verstrekkende gevolgen voor je business flow.” **Tekst:** Valérie Deridder

Wat is het verschil tussen IT en OT?

Pascal Vercammen, Global IT-manager bij Process Automation Solutions: “IT richt zich voornamelijk op veiligheid en het waarborgen van vertrouwelijkheid van informatie. Maar Operational Technology - kortweg ‘OT’ - focust eerder op de beschikbaarheid en de integriteit van systemen en industriële processen die worden gestuurd door middel van hard- en softwaresystemen. Bij OT is het belangrijk dat werkende processen kunnen blijven verderlopen, zodat de werkketen niet gestopt of onderbroken wordt zonder grote gevolgen. Bij OT is die beschikbaarheid dus van cruciaal belang. Wat betreft veiligheid zijn er ook een aantal belangrijke verschillen tussen de twee. Hackaanvallen in een IT-omgeving zijn schering en inslag en zijn daardoor vaak heel generiek. In een OT-omgeving zijn deze echter heel specifiek en doelgericht. Ook wordt malware sneller ontdekt in een IT-omgeving en is het mogelijk dat die langer onopgemerkt blijven binnen een OT-infrastructuur.”

In hoeverre biedt de veiligheidsinfrastructuur van vandaag een antwoord op specifieke OT-noden?

Vercammen: “Vandaag de dag evolueren we steeds meer naar een connected world en cloudtoepassingen. In IT, maar ook in de OT-wereld. Dat zorgt voor een stukje industrieel ‘Internet of Things’, waarbij data rechtstreeks van het veld naar de cloud wordt gestuurd. Daar moet natuurlijk ook security op toegepast worden. Bijgevolg groeit de nood voor veilige en betrouwbare OT-netwerken met de dag. Momenteel is er echter nog geen platform dat beide taken volledig op zich neemt, dus wordt er gebruikgemaakt van een combinatie van meerdere platformen.”

Wat voor soorten dreigingen zijn er?

Vercammen: “Qua dreigingen kan je een onderscheid maken tussen interne dreigingen of externe dreigingen, en tussen kwaad opzet en per ongeluk. Een werknemer kan bijvoorbeeld bewust kwade bedoelingen hebben, maar in de praktijk gaat het vooral om nalatigheid wanneer die een ‘security breach’ veroorzaakt.”

Misja Caluwé, OT-teamlead in het DISO departement bij Process Automation Solutions: “Denk dan vooral aan wachtwoorden die niet op tijd werden veranderd, aan security patches die maar één keer per jaar worden geïnstalleerd en aan het roekeloos gebruik van USB-sticks.”

Hoe pakken jullie dreigingen aan?

Vercammen: “Om dreigingen toekomstgericht en gestructureerd aan te pakken, zou elk bedrijf een ‘OT-Security Program Roadmap’ moeten uitwerken. Daar kunnen wij hen uiteraard in begeleiden volgens de IEC62443 standaard.”

Caluwé: “We verbieden bijvoorbeeld USB-sticks, dat kan softwarematig zijn, maar ook fysiek. Daarnaast gaan we regelmatiger patches en updates doorvoeren wat in een OT-omgeving een andere aanpak vergt als in een typische bedrijfs IT-omgeving. Secure remote access binnen een OT-omgeving is zeer actueel, waarbij het gebruik van het oude ‘jump server’-concept niet meer toegestaan wordt. Bovendien zorgen we ervoor dat er voldoende back-ups voorhanden zijn.”

> IT richt zich voornamelijk op veiligheid en het waarborgen van vertrouwelijkheid van informatie. OT focust eerder op de beschikbaarheid en de integriteit van systemen en industriële processen.
>
> **Pascal Vercammen**
>
> GLOBAL IT-MANAGER BIJ PROCESS AUTOMATION SOLUTIONS

Wat is IT/OT-convergentie precies? En wat zijn de uitdagingen?

Vercammen: “Om daarop te antwoorden, moeten we minstens twee decennia terug in de tijd reizen, toen de typische IT backoffice-omgeving nog ‘air gapped’ kon zijn van de OT- of productionele omgeving. Vandaag de dag convergeert die operationele technologie zodanig dat meer en meer standaard IT-technologie gebruikt wordt dan vroeger. De convergentie wijst dus op de neiging om dezelfde IT-hard- en software ook binnen een OT-omgeving toe te passen, wat de uniformiteit en kostprijs ten goede komt. Er zijn verschillende voordelen verbonden aan zo’n convergentie, maar er zijn ook heel wat uitdagingen. Typisch zijn OT-toestellen vooral ontwikkeld met als doel beschikbaarheid en betrouwbaarheid, ‘cyber secure by design’ neemt mondjesmaat toe. Hypergeconnecteerde IT-toestellen binnen de OT-infrastructuur zorgen voor meer afhankelijkheid tussen de OT-systemen onderling. Dat brengt natuurlijk heel wat risico’s met zich mee. Zo kan het hele systeem in ‘shutdown’ gaan zonder dat de afzonderlijke componenten in gevaar leken. Met ons TINA-platform (the Industrial Network Analyzer) komen we tegemoet aan verzuchtingen betreffende de betrouwbaarheid van een IT/OT-omgeving.” ■

Waarvoor staat DISO?

Eén van de deelaspecten waarop DISO (Digital Solutions) focust, is een zeer ruim aanbod aan platformen en dienstverlening betreffende ICS (Industriële Cyberveiligheid) en de volledige OT-infrastructuur tot op applicatieniveau.

PROCESS AUTOMATION SOLUTIONS an ATS company

Meer weten?
pa-ats.com/nl/oplossingen/cyber-security

“DevOps geeft IT een strategische rol binnen je bedrijfsstructuur”

Patrick Dewael
MANAGING PARTNER BRYXX

Dries Dams
DEVOPS ARCHITECT BRYXX

Steeds meer bedrijven beseffen dat ze verder moeten gaan dan het implementeren van IT-tools op zich en denken na hoe DevOps voor hen een meerwaarde kan betekenen. “DevOps heeft een impact op alle lagen van een onderneming. De processen en de organisatie moeten helemaal opnieuw worden bedacht”, zeggen Patrick Dewael en Dries Dams van BRYXX.

Tekst: Joris Hendrickx

“DevOps is een werkwijze waarbij we de silo’s van de IT-organisatie (business, security, netwerk, database, operations,…) trachten te doorbreken om zo meer als één organisatie naar buiten te komen die samenwerkt aan één oplossing. Om dat te realiseren, zetten we sterk in op cultuur en automatisatie. Uiteraard komt daar ook technologie bij kijken. Bij development praten we dan bijvoorbeeld over continuous integration & delivery, terwijl het bij de operations gaat over configurations management. Wat betreft security is continuous compliancy erg belangrijk en vanuit maintenance-oogpunt evolueren we naar self healing systems. In slimme steden kan dat ervoor zorgen dat systemen zichzelf monitoren en zelfs onderhouden en herstellen. De afgenomen nood aan menselijke tussenkomst, de strakke structuur en standaardisatie leveren daarbij een aanzienlijke besparing op.”

Process over tooling

“DevOps gaat breder dan een scrum en kan dus enkel volledig worden uitgebouwd wanneer je de hele organisatie aligneert op de processen. We kijken daarom samen met bedrijven hoe zij waarde bieden aan hun klanten en welke IT-processen daar achter zitten. Zo zien we vervolgens waar de organisatie van het bedrijf een obstakel vormt om deze processen en alles hierachter nog sneller en beter te propageren naar de klant toe. Dat resulteert in een snellere go-to-market, een webshop die sneller up-to-date kan worden gehouden of een gemeentelijke administratie en website die veel sneller kunnen inspelen op wijzigingen in de wetgeving.”

IT krijgt strategische rol

“We trekken het tegenwoordig zelfs nog verder open dan DevOps. IT staat immers ten dienste van de business. Steeds vaker zien we daarom dat de administratieve en commerciële diensten mee worden betrokken. Zo wordt heel duidelijk wat de doelen en de missie van het bedrijf zijn, en hoe IT dat kan ondersteunen. Door de bruggen tussen IT en de business te verbreden, krijgt IT een meer strategische rol. Het is cruciaal geworden in de businessprocessen, waardoor het enkel maar pijnlijker wordt wanneer deze niet gealigneerd blijkt met de business. De partijen die in staat zijn om de doorstroom van data naar de business te versnellen en te verbeteren, zijn de winnaars.” ■

De partijen die in staat zijn om de doorstroom van data naar de business te versnellen en te verbeteren, zijn de winnaars.

BRYXX | Meer weten? **bryxx.eu**

“Dankzij **FinOps** krijg je meer controle over je kosten in de cloud”


© FOTO: PRIVÉ

Danny Roefflaer
COUNTRY CHIEF TECHNOLOGIST WESTPOLE BELGIUM

Door de vele strategische voordelen kiezen steeds meer bedrijven ervoor om gebruik te maken van de innoverende diensten in de cloud. Het is dan wel cruciaal om de kosten hiervan onder controle te houden. “FinOps biedt een antwoord op die nood”, zegt Danny Roefflaer, Country Chief Technologist bij WESTPOLE Belgium.

Tekst: Joris Hendrickx

Waarom is FinOps zo belangrijk?

“Cloud financial management, ook FinOps genoemd, richt zich op het opstellen van een strategie en het implementeren van een governancestructuur om de kosten in de cloud onder controle te houden. Veel bedrijven constateren immers al vrij snel na het in productie nemen van applicaties dat de snel toenemende kost een hele uitdaging is. Omdat meerdere afdelingen die applicaties en hun data gebruiken, is het bovendien vaak moeilijk om de kosten toe te wijzen.”

Waaruit bestaat FinOps?

“Natuurlijk is het belangrijk om bepaalde tools te installeren waarmee iedereen een beter zicht kan krijgen op die kosten, maar dat alleen is niet voldoende. Je moet een multidisciplinair team hebben van onder meer financiële mensen, ontwikkelaars, IT-ingenieurs en businessmensen die samenwerken om een goede return on investment (ROI) te krijgen van de zware investeringen in clouddiensten. Dat vereist echter ook een culturele verandering. Je moet iedereen zover krijgen om te participeren en bepaalde doelen na te streven op het vlak van ROI. Een belangrijk aspect daarbij is bijvoorbeeld dat iedereen de juiste labels gebruikt zodat de rapporten en dashboards goed kunnen werken en de juiste informatie eruit komt.”

“Er is daarnaast ook meer inzicht nodig in wie welke licenties gebruikt in onder meer Microsoft 365, Azure en Amazon Web Services én wat deze kosten. Elk van deze platformen heeft een eigen cost management tool, maar die gaat helaas niet verder dan het eigen platform. Het is dus een hele uitdaging om een algemeen overzicht te krijgen. Zeker het berekenen van de kost per project is een moeilijke oefening.”

Wat kan WESTPOLE in dat kader betekenen?

“WESTPOLE heeft een brede kennis van zowel de verschillende clouddiensten als de achterliggende kostenmodellen. We helpen bedrijven dan ook graag om alles zo optimaal en inzichtelijk mogelijk op te zetten, op maat van hun specifieke noden. Daarnaast betrekken we ook de verschillende personen en teams in het bedrijf met geïndividualiseerde dashboards en rapporten. Tot slot kunnen we de multidisciplinaire teams leiden en advies geven, rekening houdend met het principe ‘klein beginnen en dan groeien’.” ■

FinOps richt zich op het opstellen van een strategie en het implementeren van een structuur om de kosten in de cloud onder controle te houden.

WESTPOLE

Meer weten?
westpole.be

KNAPPE KOPPEN

een mediaplanet podcast.

'Knappe Koppen' is een podcastreeks voor liefhebbers van rake analyses over actuele thema's. We koppelen twee doorwinterde experts aan elkaar en nemen de luisteraar mee in een partijtje pingpong over valkuilen, tendensen en toekomstprognoses.

Meer weten?

Volg Knappe Koppen en Mediaplanet België via Instagram.

Via mail

knappekoppen@mediaplanet.com

mediaplanet

knappekoppen.pdcst

Een cybersecuritybeleid is een continu proces. Cybercriminelen vinden voortdurend nieuwe manieren om je aan te vallen.

© FOTO: PRIVÉ

“Een cyberverzekering vormt het sluitstuk van een holistische aanpak”

IT komt steeds meer centraal te staan bij het runnen van een bedrijf. Naast de vele voordelen die dat biedt, nemen zo echter ook de cyberrisico’s toe. “Een holistisch cybersecuritybeleid met een cyberverzekering als sluitstuk is dan ook aangewezen” zeggen Anne-Sophie Coppens en Tim Merci van Marsh BeLux. **Tekst:** Joris Hendrickx

Anne-Sophie Coppens

CYBER PRACTICE LEADER MARSH BELUX

Tim Merci

HEAD OF ADVISORY SOLUTIONS MARSH BELUX

Hoe kunnen bedrijven zich het best wapenen tegen cyberrisico’s?

Coppens: “Alles begint met het begrijpen van je eigen systemen. Je start dus best met een risicoassessment. Zeker bedrijven met dochtervennootschappen of veel leveranciers dienen goed in beeld te brengen hoe die met elkaar verbonden zijn. Van elke brug tussen personen en/of bedrijven moet je weten hoe je die kan beveiligen. Pas daarna kan je een visie en strategie ontwikkelen en uiteindelijk middelen toekennen. Er is niet één juiste methodologie, ze moet vooral passen bij je sector, activiteit, grootte en filosofie. Sommige bedrijven zijn nu eenmaal meer risicoavers dan andere. Het is ook belangrijk om te benadrukken dat een cybersecuritybeleid een continu proces is. Je dient steeds alert te blijven en ervoor te zorgen dat alles up-to-date blijft. Cybercriminelen blijven immers ook niet stilzitten en vinden voortdurend nieuwe manieren om je aan te vallen.”

Hoe kunnen jullie bedrijven hierin helpen?

Coppens: “Hoewel cybersecurity niet altijd duur hoeft te zijn, zijn de middelen van ieder bedrijf wel beperkt. Je moet dus keuzes maken. Als makelaar adviseren we onze klanten om hun risico’s beter te beheren. Verzekeringen maken daar deel van uit, maar we starten wel vanuit een globaal perspectief op hoe je de risico’s maximaal kan beperken.”

Merci: “We staan klanten bij in de bewustwording, de analyses, het in kaart brengen van de risico’s en het maken van keuzes om deze aan te pakken. Door de feedback die we krijgen vanuit onze verzekeringen weten we waar er incidenten zijn en welk soort incidenten dat zijn. Dankzij onze interne investeringen in IT-kennis kunnen we vervolgens de discussie aangaan en klanten mee helpen om prioriteiten te stellen in hun cybersecuritybeleid.”

Wat kan de rol van een cyberverzekering zijn in dat beleid?

Coppens: “Hoewel een nulrisico uiteraard niet bestaat, dienen in eerste instantie preventieve maatregelen te worden getroffen. Ik denk aan regelmatige back-ups en updates, een firewall, detectie, monitoring, trainingen rond cyberveiligheid, een crisisplan,... Pas daarna kan een verzekering nuttig zijn als bijkomend financieel middel.”

Merci: “Een cyberverzekering is geen einddoel en geen wondermiddel tegen alles. Het is daarom belangrijk om eerst een inzicht te krijgen in wat er kan gebeuren en wat de potentiële impact is op je bedrijf. Pas daarna kijken we of een verzekering eventueel nuttig kan zijn. De verzekering is dus slechts het sluitstuk, terwijl vooral de maturiteit van de onderneming op het vlak van cyberrisicobeleid de essentie moet zijn.”

Waarom is het belangrijk om een cyberverzekering steeds af te stemmen op de noden van een bedrijf?

Coppens: “Bepaalde bedrijven lopen een groter risico op vlak van privacy omdat ze veel persoonlijke data hebben. Andere bedrijven riskeren dan weer eerder omzetverlies indien het bedrijf zou stilvallen. Het is dus steeds kijken welke dekkingen, vrijstellingen en limieten passen voor welk bedrijf. Dat is steeds maatwerk. Sommige bedrijven willen enkel een dekking tegen de grootste catastrofes, waardoor er een hoge vrijstelling mogelijk is en de verzekering bijgevolg goedkoper wordt. Met een financiële analyse helpen we bedrijven om inzicht te krijgen in hoe ze hun budget optimaal kunnen benutten. Vaak betekent dit dat we een holistische aanpak aanraden: eerst preventieve maatregelen nemen die een positieve impact hebben op de verzekeringspremie, waardoor je vervolgens een lagere vrijstelling kan nemen. Die zoektocht en wisselwerking zijn meteen ook erg leerrijk voor onze klanten.”

> De digitalisering zet zich door in elke sector en elke laag van de maatschappij. Net daarom zullen preventie en het verhogen van de maturiteit van je risicobeheer essentieel zijn.

Marsh

Meer weten?
marsh.be

Hoe zien jullie dit verder evolueren?

Merci: “Er is nu een duidelijke shift ingezet richting de kwaliteit van het risico, en dat zal ook de komende jaren de focus blijven. Daarnaast worden risico’s alsmaar complexer. De digitalisering zet zich immers door in elke sector en elke laag van de maatschappij. Dat vertaalt zich ook in meer incidenten. Net daarom zullen preventie en het verhogen van de maturiteit van je risicobeheer essentieel zijn. Misschien zullen we wel evolueren naar een punt waar cyberverzekeringen niet meer interessant zijn ten opzichte van het rendement dat men er uithaalt. Vanuit die holistische visie kan je budget dan mogelijk beter worden ingezet op controlemechanismen binnen je bedrijf.”

Coppens: “De premies zijn de afgelopen jaren alvast fors gestegen. Bepaalde dekkingen zijn bovendien gedaald, met bijvoorbeeld bepaalde sublimieten voor ransomware. Wel denk ik dat de markt nu aan het stabiliseren is omdat verzekeraars bepaalde risico’s nu gewoon niet meer willen verzekeren. Hierdoor is er meteen ook een extra stimulans voor bedrijven om de zaken eerst intern te verbeteren. Bijgevolg zijn er nu minder kostelijke incidenten en kunnen ze makkelijker worden opgelost.” ■

JOIN ISACA & GET CERTIFIED

- A strong network of local IS/IT professionals in Belgium.
- Success in IS/IT audit, risk, control, security, cybersecurity and governance across a multitude of industries.
- Industry leading global conferences offering professional networking and education locally and globally.
- SheLeads Tech promoting women in leadership roles in technology.
- Access to the updated frameworks, publications and research of ISACA.
- Mentorship Programs & connection with other ISACA members for career development and support.

WWW.ISACA.BE

ISACA Belgium Chapter

CERTIFICATIONS :

CISA Certified Information Systems Auditor. An ISACA Certification

CISM Certified Information Systems Manager. An ISACA Certification

CGEIT Certified in the Governance of Enterprise IT. An ISACA Certification

CDPSE Certified Data Privacy Solutions Engineer. An ISACA Certification

CRISC Certified in Risk and Information Systems Control. An ISACA Certification

CSX-P CSX Cybersecurity Practitioner. An ISACA Certification

devoteam

Infinite possibilities to become a digital leader

Join our multidisciplinary team of Data Specialists, Functional Analysts, Business Consultants, Security Experts, Cloud Engineers, Developers, Enterprise Architects, and other extraordinary talents, spread across more than 20 countries across EMEA.

Get the opportunity to work alongside the world's industry-leading partners: AWS, Google Cloud, Microsoft, and ServiceNow.

Take a look at our job openings
devoteam.be/join-us

Creative tech for Better Change

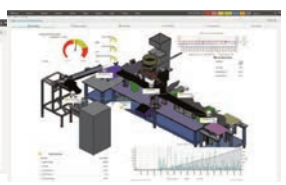
Contact: TINA@pa-ats.com

PA Solutions
TINA: The Industrial Network Analyzer

What is TINA?: Industrial Monitoring Built on the Paessler PRTG Framework

Industrial monitoring is key to ensuring the continued reliability and effectiveness of your business infrastructure, but the OT environment is often overlooked. That's where TINA comes into play. The Industrial Network Analyzer, known as TINA, is PA Solutions' monitoring framework, based on Paessler PRTG, for both the OT and IT environments. It works through a series of connected sensors that promote continued reliability and effectiveness throughout all of your organization's IT/OT devices. The entire system is built on one platform with a convenient dashboard view, allowing your team members to easily track and manage your operation without needing to utilize multiple tools or models. With a massive collection of sensors to select from, this lightweight solution makes monitoring systems, devices, traffic, and applications a breeze. Best of all? TINA is designed with businesses of all shapes and sizes in mind, meaning it's an affordable solution even for companies with limited budgets.


TINA Dashboard within PRTG


TINA Dashboard within PRTG

What Can TINA Do for You?

TINA provides a wide range of advantages to the end user, including:

/ Shutdown, slowdown, and production loss prevention
/ Ease of installation, operation, and scalability
/ Custom sensors
/ Full control over map creation, dashboard information, and data visualization
/ Affordable, all-in-one solution with no hidden fees or add-ons
/ Limitless possibility and reliability — TINA is built on the widely-known, trusted Paessler PRTG framework

TINA: The Affordable Answer

With a **one-time CapEx cost of only €5K** (including installation and deployment) until the end of 2022, TINA is ideal for companies of all varieties. After implementation, your organization will soon realize:

/ 100% availability of IT and OT assets
/ Predictive problem solving
/ Understandable, KPI-driven dashboards
/ Licensed for 1,000 sensors

TINA in Action

The Customer: A Petrochemicals Plant

The Problem:
At this plant, DCS redundant servers would sometimes swap with one another for no clear reason.

The PA Solution:
When the company first looked, no immediate cause of the swap was found. The PA team implemented TINA to analyze hardware and software anomalies in the system.

The Results:
TINA quickly identified a memory leak that caused the company's DCS controller services to crash on the master server, which would then trigger the redundant server to take over.

/ Intuitive operation with inclusive alerts and resolutions
/ Easy, quick deployment with low ongoing maintenance needs and continued support from PA Solutions experts

We engineer a sustainable future.

TINA@pa-ats.com | www.pa-ats.com