MAART 2023 **NL.PLANET-BUSINESS.BE**

mediaplanet
A CAYBON COMPANY

Veiligheid

Streven naar wederzijds respect

Hulpverleners bij de brandweer, Civiele Bescherming en noodcentrale 112 getuigen over de soms moeilijke samenwerking met de burger.

© FOTO: PRIVÉ

IN DEZE EDITIE

Voorwoord

Naar een veilige, toekomstgerichte en weerbare samenleving

Elke dag opnieuw zetten ontelbare mensen zich in om bij te dragen aan een samenleving waarin iedereen zich veilig kan voelen. “Toch worden we nog te vaak geconfronteerd met zinloos geweld of criminaliteitsvormen die onze maatschappij ontwrichten”, zegt Annelies Verlinden, minister van Binnenlandse Zaken. “Geweld ook tegen de vele mensen die dag en nacht paraat staan om te helpen, dit vaak in zeer moeilijke omstandigheden.”

Annelies Verlinden

MINISTER VAN BINNENLANDSE ZAKEN

Het is mijn prioriteit om de veiligheid te garanderen van de mensen die zelf instaan voor onze veiligheid. Hulpverleners krijgen namelijk al te vaak te maken met agressie of zinloos geweld.

Als minister van Binnenlandse Zaken werk ik elke dag samen met alle partners om te garanderen dat burgers in een veilige, toekomstgerichte en weerbare samenleving kunnen leven. Zeker in deze uitdagende tijden, waarin veiligheid geen zekerheid meer is en de middelen schaarser worden, is dat broodnodig. Een eerste uitdaging is de veiligheid garanderen van de mensen die zelf instaan voor onze veiligheid. Zij krijgen al te vaak te maken met agressie of geweld. Veiligheidsdiensten en hulpverleners moeten hun job kunnen uitoefenen in de meest optimale omstandigheden, zodat ze over ons kunnen waken en ons de best mogelijke hulp kunnen bieden. Al sinds mijn aantreden als minister maak ik er een prioriteit van om hen beter te beschermen, met gedragen maatregelen en de juiste middelen en instrumenten die daarop impact hebben.

Intrafamiliaal geweld

Zich veilig voelen in de samenleving begint bij het zich veilig en geborgen kunnen voelen op de plaats waar we thuis zijn. Tijdens de coronacrisis zagen we jammer genoeg een stijging in het aantal meldingen van intrafamiliaal geweld. Meer tijd samen doorbrengen dan voorheen heeft in sommige gezinnen geleid tot meer spanningen, waarbij fysiek of psychisch geweld niet werd geschuwd. Eén op de vijf vrouwen in ons land wordt slachtoffer van deze vormen van geweld. Om lokale besturen aan te zetten actie te ondernemen tegen deze problematiek, konden ze zelf projecten indienen en daarvoor subsidies ontvangen. Steeds opnieuw zie ik de bewustwording en de gedrevenheid waarmee besturen, gespecialiseerde hulpverleners, politiediensten en vrijwilligers aan de slag gaan om binnen hun stad of gemeente ruchtbaarheid te geven aan deze problemen en om te voorzien in een drempelverlagende aanpak gericht op een luisterend oor, doorverwijzing en professionele hulpverlening, ook op juridisch vlak. Samen met de FOD Binnenlandse Zaken blijf ik de projecten van nabij opvolgen.

Duurzame oplossingen

Er wordt met verenigde krachten gewerkt aan een omgeving die garanties wil bieden op het vlak van veiligheid en bescherming, zodat we er samen kunnen wonen, werken en leven in de best mogelijke omstandigheden. Het is belangrijk dat alle diensten en partners uit de veiligheidsketen, niet in het minst de lokale overheden en de federale overheid, aandacht blijven hebben voor onze snel veranderende maatschappij, en dus ook de daardoor veranderende noden en behoeften van ons allen. We moeten elk dag samen blijven zoeken naar de juiste oplossingen: duurzame oplossingen die de waarden van onze democratische rechtstaat respecteren. Zodat elke inwoner kan leven in een veilige, toekomstgerichte en weerbare samenleving. ■

04

Totaalconcept

Ontdek hoe je zowel de fysieke als digitale deur op slot houdt.

06

Expertise

Volgens Marc Vael heeft 90% van de raden van bestuur te weinig kennis over online risico’s.

#Ontdek onze podcast!

Beluister onze podcast ‘Knappe Koppen’ en kom alles te weten over cyberveiligheid.

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
E-mail: laurens.de.grave@mediaplanet.com
Project Manager: Jérémy Verkercke
Redactie: Joris Hendrickx
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/2023/12.996/14

Cyberveiligheid:

“Slechts één klein gat in het net kan ervoor zorgen dat alle moeite voor niets is geweest”

Nooit eerder was er zo’n grote dreiging op het vlak van cybercriminaliteit. Bedrijven dienen dan ook absoluut maatregelen te nemen om zich preventief te beschermen en voor te bereiden op een mogelijke aanval. “Artificiële intelligentie zal daar een belangrijke rol in spelen”, zegt Antonietta Mastroianni, Chief Digital & IT Officer bij Proximus. **Tekst:** Joris Hendrickx

Wat zijn vandaag de belangrijkste cyberrisico’s?

“Gezien de huidige geopolitieke situatie is er een sterk verhoogd risico op cyberoorlogen en cyberactivisme. We zien nu meer disruptieve aanvallen met bijvoorbeeld malware die als doel hebben om de IT-infrastructuren en netwerken van landen lam te leggen. Daarnaast stellen we ook een flinke toename vast van het aantal aanvallen op kritieke infrastructuur (elektriciteitsleveranciers, oliepijpleidingen, telecom, ziekenhuizen,...). Financiële winst blijft het hoofddoel van cybercriminelen. Vaak proberen ze hun slachtoffers in meerdere stappen af te persen met een combinatie van ransomware en DDoS-aanvallen, of door data te stelen en dan te dreigen om die te publiceren. Buiten de financiële schade die ontstaat door het lamleggen van het bedrijf of het moeten betalen van het geëiste geld, veroorzaakt dat ook vaak heel wat reputatieschade.”

© FOTO: PRIVÉ

Ons excellentiecentrum brengt cyberveiligheid en artificiële intelligentie samen om de uitdagingen van vandaag en morgen aan te gaan.

Antonietta Mastroianni

CHIEF DIGITAL & IT OFFICER PROXIMUS

> Bedrijven moeten goed monitoren op welke manieren ze online worden blootgesteld.

In welke zin vormt de toenemende digitalisering op zich ook een risico?

“Het groeiende aantal digitale ecosystemen, met daarin verschillende bedrijven in de waardeketen die met elkaar verbonden zijn, zorgt inderdaad voor een groter risico. Ook daar is een goede cyberbeveiliging extreem belangrijk. De publieke cloud is eveneens een aandachtspunt. Ze is vandaag een belangrijke facilitator van technologische innovatie, en dient dus zeer veilig te zijn. Bedrijven moeten ook goed monitoren op welke manieren ze online worden blootgesteld. Steeds vaker maakt een bedrijf deel uit van een open dataspace of een platform waar data worden gedeeld. Al die informatie moet goed worden beveiligd. Hetzelfde geldt voor alles wat via API’s wordt gedeeld met de buitenwereld. Je kan dan als bedrijf zelf wel alle mogelijke veiligheidsmaatregelen hebben getroffen, mogelijk loop je nog steeds een groot risico indien dat niet goed zit.”

Hoe kunnen bedrijven best omgaan met die risico’s?

“Investeren in cyberveiligheid is belangrijker dan ooit. Vaak gebruiken cybercriminelen phishingtechnieken om toegang te krijgen tot een bedrijfsnetwerk. Steeds meer bedrijven maken er daarom een prioriteit van om hun medewerkers bewust te maken van de risico’s, in combinatie uiteraard met technische maatregelen. De recent uitgevaardigde NIS2-richtlijn van de EU is een sterk signaal dat cybersecurity niet langer een optie is, maar een must. Uiteraard moeten ook alle maatregelen van het ‘cybersecurity business continuity plan’ worden opgevolgd en beheerd. Bedrijven moeten investeren in een cyberbeveiligingsprogramma. End-to-end access management, offline back-up, endpoint detection en response, security orchestration & automation, device access control, DDoS-protection, API-security, noem maar op: het moet allemaal met de grootste discipline worden uitgevoerd. Slechts één klein gat in het net kan ervoor zorgen dat alle moeite voor niets is geweest.”

“Cybercriminaliteit en de gebruikte technieken evolueren heel snel. Het is daarom cruciaal om te blijven leren, investeren, je zeer bewust te zijn van de nieuwe technieken en ervoor te zorgen dat je daar dan ook in de praktijk mee om kan gaan. Ook innovaties binnen het domein van postkwantumcryptografie en key distribution moeten goed worden opgevolgd, omdat ze zullen bepalen hoe data in de toekomst zullen worden uitgewisseld. Managed security service providers zoals Proximus kunnen bedrijven bijstaan wanneer zij zelf niet over de nodige competenties beschikken om daar correct mee om te gaan.”

In welke zin kan artificiële intelligentie een gamechanger zijn?

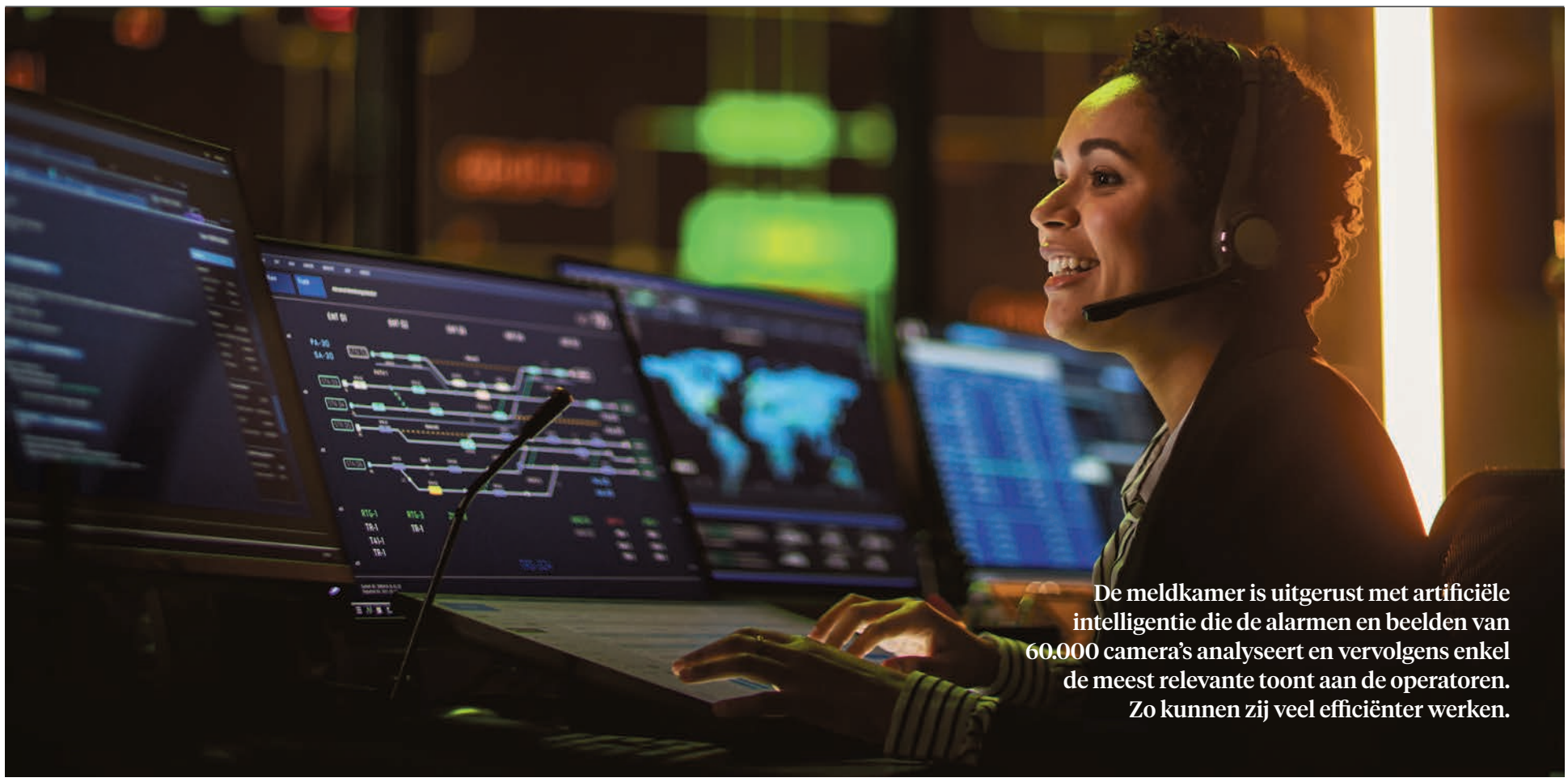
“Het zal een belangrijke rol spelen omdat het binnen vier domeinen excelleert op een niveau dat niet haalbaar is met menselijke kennis: schaalbaarheid, aanpasbaarheid, snelheid en accuraatheid. Bij Proximus beschikken we over vijf terabyte aan data die geanalyseerd kan worden om ons te beschermen tegen cybercriminaliteit. Zo’n schaal kan uiteraard onmogelijk worden bereikt door mensen. Ook de aanpasbaarheid aan nieuwe bedreigingen en technieken is noodzakelijk, aangezien cybercriminaliteit een snel veranderend domein is. De tijd die nodig is om een aanval te detecteren en vervolgens te reageren, moet minimaal zijn. De snelheid die AI kan bieden, is dus cruciaal. Tot slot is de accuraatheid een belangrijke troef bij het correleren van diverse informatie en het herkennen van patronen in grote datasets om zo voorspellingen te doen.”

Wat kan Proximus ADA betekenen op dat vlak?

“Proximus ADA is een excellentiecentrum dat cyberveiligheid en AI samenbrengt om de uitdagingen van vandaag en morgen te kunnen aangaan. We bieden advies en trainingen aan over cyberveiligheid en AI, en hoe beide domeinen kunnen samenwerken. Daarnaast investeren we in specialisten en het opzetten van samenwerkingen om tot nieuw intellectueel eigendom te komen. Dat kan dan vervolgens worden verkocht aan bedrijven en overheden zodat die zich kunnen verdedigen op basis van hun eigen data en noden.” ■

proximus ada

Meer weten?
proximus-ada.com



De meldkamer is uitgerust met artificiële intelligentie die de alarmen en beelden van 60.000 camera's analyseert en vervolgens enkel de meest relevante toont aan de operatoren. Zo kunnen zij veel efficiënter werken.

Hoe je de fysieke én digitale deur goed op slot houdt

Bart Verhaert

SALES DIRECTOR
SECURITAS TECHNOLOGY
SECURITAS BELGIUM

Alessandro Cordaro

ICT & WIRELESS PRESALES
MANAGER SECURITAS BELGIUM

Als marktleider en een innovatieve voortrekker binnen de beveiligingssector, heeft Securitas via de combinatie van fysieke en digitale beveiliging een unieke positie uitgebouwd. Dubbelinterview met Bart Verhaert en Alessandro Cordaro van Securitas Belgium: "We bieden een totale ontzorging via één aanspreekpunt." **Tekst:** Joris Hendrickx

Geïntegreerde beveiliging, wat betekent dat voor jullie?

Alessandro Cordaro, ICT & Wireless Presales Manager bij Securitas Belgium: "Securitas staat voor het volledige plaatje. Zo zijn er enerzijds onze bewakingsagenten, die fysiek aanwezig zijn bij onze klanten, en anderzijds onze mobiele teams, die controlerondes doen en op interventie gaan. In onze meldkamer komen alle alarmen en camerabeelden binnen. Het is het kloppend hart van onze operaties. Op basis daarvan kunnen onze operatoren vanop afstand beoordelen of het over een reëel of vals alarm gaat, om vervolgens onze mensen ter plaatse gericht te kunnen ondersteunen. Deze meldkamer is uitgerust met artificiële intelligentie die de alarmen en beelden van onze 60.000 camera's analyseert en vervolgens enkel de meest relevante toont aan onze operatoren. Zo kunnen zij veel efficiënter werken."

Bart Verhaert, Sales Director Securitas Technology bij Securitas Belgium: "Deze meldkamer is dus een soort van commandocentrum waar alle connecties binnenkomen en van waaruit vervolgens alle technische en operationele sturingen gebeuren. Dat kunnen incidenten zijn zoals een diefstal of inbraak, maar net zo goed een brand of technisch probleem. De paniekknoppen van onze bewakers zijn er eveneens rechtstreeks mee geconnecteerd om ook hun veiligheid te vrijwaren."

Cordaro: "Dan heb je tot slot ook de pure technologiecomponent. Die bestaat uit vaste en mobiele camera's, maar ook uit diverse sensoren zoals geluids- en bewegingssensoren, gas- en branddetectie. Al deze data worden verzameld in de Securitas Cloud, waar we deze verwerken, verrijken en via artificiële intelligentie omvormen tot bruikbare informatie waarmee we de bewakings- en veiligheidsdiensten audiovisueel kunnen ondersteunen. Dat gebeurt allemaal volgens de regels van de kunst én de geldende privacywetgeving."

Wat zijn voor jullie de gamechangers voor de toekomst?

Verhaert: "Dankzij de snelle ontwikkeling van 5G en fiber kunnen de beelden van camera's nu rechtstreeks naar slimme platformen worden doorgezonden en is ook de kwaliteit van de beelden enorm verbeterd. Daarop kan dan artificiële intelligentie worden toegepast om tot een lerend geheel te komen. Zo kan meteen ook veel beter het verschil worden gemaakt tussen een echt incident en een vals alarm."

We werken vandaag al sterk mee aan de slimme steden en gebouwen van de toekomst.

Securitas Technology

Meer weten?
securitas.be

Cordaro: "Naast het installeren van bijvoorbeeld een camera kunnen wij meteen ook de nodige connectiviteit, ICT-expertise en slimme platformen aanbieden. Daarom werken we vandaag al sterk mee aan de slimme steden en gebouwen van de toekomst. Zopas presenteerden we ons 5G-proefproject in het kader van een subsidietraject onder leiding van minister Petra de Sutter. Samen met Robovision en Orange Belgium kunnen we onveilige situaties sneller capteren."

Hoe dragen naast die interne innovatiekracht ook overnames bij aan jullie leiderspositie?

Verhaert: "Securitas stond altijd al heel sterk op vlak van connectiviteit en platformen. Met de overname van STANLEY Security in 2022 vergroten we ook onze installatiecapaciteit omdat we hiermee nu heel wat waardevol talent in huis hebben, denk maar aan ingenieurs en techniekers. Zo versterken we onze positie als een expert in geïntegreerde beveiligingsoplossingen onder de noemer Securitas Technology. Waar je vroeger tal van kleine, interne meldkamers had, merken we dat alsmaar meer bedrijven en organisaties ervoor kiezen om voor hun sterk beveiligde sites een beroep te doen op een centrale meldkamer zoals die van Securitas. Zo doen drie van de vier Belgische grootbanken een beroep op ons. Ook onze acquisitie van NIT Technologies, de voormalige meldkamer van BNP Paribas Fortis, kadert hierin."

Waarom is het cruciaal dat jullie ook over expertise beschikken inzake cyberbeveiliging?

Cordaro: "Een inbreker tracht vandaag vaak eerst om via hacking je beveiligingssysteem buiten werking te stellen, alvorens fysiek binnen te dringen. Daarom is het cruciaal om een bijkomende cybersecuritylaag te voorzien."

Verhaert: "Zo bieden we een totale ontzorging via één aanspreekpunt. Onze klanten weten dat wij dus zowel de fysieke als de digitale deur beveiligen." ■

“Preventieve maatregelen en cyberverzekering vullen elkaar aan”

Een gespecialiseerde cyberrisicoverzekering op maat biedt een antwoord op de toegenomen dreiging én schade door cyberrisico’s. Toch dienen bedrijven in de eerste plaats preventieve maatregelen te nemen. Ook daar kan de verzekeraar en makelaar een belangrijke ondersteunende rol in spelen. **Tekst:** Joris Hendrickx

Anne-Sophie Coppens

CYBER PRACTICE LEADER BELUX MARSH

© FOTO'S: PRIVÉ

Tim Merci

HEAD OF MARSH CONSULTING SOLUTIONS BELUX

Welke uitdagingen stellen zich vandaag inzake het verzekeren van cyberrisico’s?

Anne-Sophie Coppens, Cyber Practice Leader BeLux bij Marsh: “De hoeveelheid cyberrisico’s neemt ieder jaar toe en bovendien wordt hun impact steeds groter. We worden door de digitalisering nu eenmaal alsmaar afhankelijker van technologie en IT. Dat geldt trouwens voor zowel kleine als grote bedrijven - cybercriminelen viseren iedereen. Ook de manier waarop we moeten omgaan met risico’s is geëvolueerd. We bieden in dat kader al meerdere jaren gespecialiseerde cyberrisicopolissen aan met aangepaste clausules, in plaats van bijvoorbeeld een algemene verzekering burgerlijke aansprakelijkheid waar cyberrisico’s slechts een klein deel van uitmaken en maar deels gedekt zouden zijn. In 2017 en 2018 was er echter een veel groter aanbod aan zulke verzekeringen dan dat er vraag was, waardoor de prijzen hiervan relatief laag lagen.”

“Omdat het aantal risico’s en hun impact echter bleven stijgen, groeide de discrepantie tussen de prijs en de risico’s die moesten worden gedekt. Het portfolio van de verzekeraars dreigde dus uit balans te raken. Daarom zijn de premies intussen gestegen en bepaalde dekkingen gedaald. Vandaag wordt niet meer elk risico zomaar verzekerd. Ook worden verzekeringen nu afgestemd op het type en de grootte van het bedrijf, de sector,...”

> Onze verzekeraars gaan aan de slag met een checklist van twaalf punten. Afhankelijk van de score van bedrijven op al deze twaalf controles krijgen zij een bepaalde dekking, vrijstelling en limiet toegewezen.

Op welke manieren onderscheidt een gespecialiseerde cyberrisicopolis zich van een algemene verzekering?

Tim Merci, Head of Marsh Consulting Solutions BeLux: “Cyberrisicopolissen adresseren drie risico’s die traditionele polissen niet dekken. Ten eerste ben je ook verzekerd voor het omzetverlies dat ontstaat omdat je business stilligt terwijl een datalek moet worden geïdentificeerd en opgelost. Ten tweede zijn de bijkomende kosten gedekt, denk maar aan het herstellen van de integriteit van interne en externe systemen en processen, maar ook van beschadigde eigendommen. Ten derde is er de aansprakelijkheid ten aanzien van derden: ook de schade die door een cyberincident ontstaat bij je klanten, leveranciers of andere betrokken partijen is verzekerd.”

Hoe gaan jullie tewerk bij het samenstellen van een verzekeringspolis op maat?

Coppens: “Om te beoordelen of een bedrijf verzekerbaar is en hoe die verzekering dan best is opgebouwd, kijken wij naar bepaalde basiselementen. Die hebben we in een gebruiksvriendelijke en overzichtelijke tool gegoten. Zo hoeven onze verzekeraars niet meer voor iedere klant een reeks van uiteenlopende vragen te stellen, maar kunnen zij steeds terugvallen op deze gestandaardiseerde checklist. Deze kan trouwens al vanaf de eerste assessment worden gebruikt als leidraad om te werken aan het verbeteren van de risico’s. Concreet bestaat de checklist uit twaalf controles: multi factor authentication, endpoint detection, secured & encrypted backup, privileged access, e-mail filtering & web security, patch management,... Afhankelijk van de score van bedrijven op al deze twaalf controles krijgen zij een bepaalde dekking, vrijstelling en limiet toegewezen.”

In welke zin gaan jullie verder dan enkel het verzekeren van cyberrisico’s?

Merci: “De door ons ontwikkelde tool kan bedrijven ook helpen om een grondige self assesment uit te voeren en op basis daarvan de juiste prioriteiten en investeringen te bepalen op het vlak van cyberveiligheid. Aanvullend kunnen wij dan met onze ruime kennis binnen dat domein een adviserende rol opnemen en extra hulp bieden bij het inzichtelijk maken van alles wat cyberveiligheid betreft.”

Coppens: “Een cyberverzekering is inderdaad slechts één onderdeel van een goed beleid op het vlak van cyberveiligheid. We raden bedrijven steeds een holistische aanpak aan: neem eerst zoveel mogelijk preventieve maatregelen die een positieve impact hebben op je verzekeringspremie, waardoor je vervolgens een lagere vrijstelling kan nemen. Een verzekering is daarna je laatste verdedigingslinie wanneer het toch fout loopt. Bij die analyse en denkoefening is het cruciaal dat iedereen in je bedrijf mee is, en dus niet enkel de CIO en de IT-afdeling. Je cyberrisico’s verminderen, is een globaal project en vergt een goede wisselwerking tussen de diverse stakeholders.” ■

#Wist je dat?

- Bijna **75%** van de organisaties wereldwijd heeft al te maken gekregen met cyberaanvallen.
- **61%** van de organisaties heeft een verzekering die bescherming biedt tegen de gevolgen van cyberrisico’s.
- Slechts **3%** van de organisaties beoordeelt zijn algemene cyberhygiëne als ‘excellent’, terwijl 40% toegeeft dat verbetering mogelijk is.
- Slechts **26%** van de organisaties meet de financiële schade van cyberrisico’s.
- **64%** van de organisaties geeft toe dat ze hun investeringen in cyberbeveiliging pas hebben verhoogd na een aanval te hebben ervaren.
- **43%** van de organisaties heeft een risicobeoordeling uitgevoerd bij de partners waarmee ze zijn verbonden in de waardeketen.

“Digitale transformatie kan niet zonder proactieve beveiliging”

Johan Van Looy

CEO INNOCOM

Bij ieder digitaal transformatietraject dient cybersecurity zo vroeg én zo breed mogelijk te worden opgenomen. Vanuit dat besef besliste defensie om voor een kritisch project een beroep te doen op een specialist in deze materie. Johan Van Looy, CEO bij INNOCOM, legt uit.

Tekst: Joris Hendrickx

Waarom moet security zo vroeg en breed mogelijk worden opgenomen?

“Bij het vormgeven van een digitale transformatiestrategie kijken bedrijven vaak vooral naar het realiseren van waardecreatie. Je moet in die denkoefening echter ook al rekening houden met hoe die waardecreatie kan worden bedreigd én hoe je je daartegen kan beschermen. Dat heeft immers een grote impact op de keuzes die je daarna gaat maken om je strategie te ondersteunen. Het speelveld van cybercriminelen is bovendien erg groot en ze zijn vaak erg creatief in het vinden van zwakheden. Er zitten soms zelfs volledig professionele businessmodellen achter. Je moet dus zorgen dat je álle deuren dichttimmert: het digitale, fysieke én menselijke aspect. Het traditionele security operations center dient te worden getransformeerd naar een security intelligence center dat veel proactiever werkt, meer context meegeeft en elke potentiële dreiging meteen analyseert en aanpakt. Dat betekent dan wel dat de hele organisatie continu stand-by moet zijn en er dus een breed draagvlak nodig is.”

Hoe slagen jullie erin om dat in de praktijk te realiseren?

“INNOCOM is dé Belgische referentie op het vlak van bedrijfsarchitectuur. Onze specialiteit is het vertalen van de strategie naar bepaalde keuzes qua opstelling en de juiste roadmaps om die keuzes te kunnen implementeren. Gezien cyberbeveiliging zo vroeg mogelijk in de ontwerpfase dient te gebeuren en zo breed mogelijk moet worden gedragen, maakt dat inherent deel uit van wat wij doen.”

“Een goed voorbeeld is de ESI-missie (Essential Security Interests) die gelinkt is aan het F35-programma van defensie. We richten ons daarbij op drie doelen. Het eerste doel was de overdracht en het uitbouwen van een state-of-the-artexpertise voor zowel defensie als andere kritische instellingen. We vertrokken daarbij vanuit de kennis van F-35 leverancier Lockheed Martin rond cybersecurity om die dan te verrijken met onze kennis. Ten tweede ontwerpen we nu een architectuur voor een ‘world class’ security intelligence center binnen defensie. Onze architectuur zal de uitwisseling van informatie, afkomstig uit de diverse systemen waar defensie mee werkt, mee optimaliseren en integreren. Ook de hele governance werken we uit én we definiëren welke concrete projecten dienen te gebeuren. Tot slot bestaat de samenwerking ook uit een onderzoeks- en innovatietraject dat de kennisdomeinen en actoren identificeert die België kunnen helpen om zich beter te wapenen tegen cyberrisico’s.” ■

INNOCOM.

Meer weten? **inno.com**

Bij het vormgeven van een digitale transformatie-strategie moet je ook al rekening houden met hoe de waardecreatie kan worden bedreigd én hoe je je daartegen kan beschermen.

“90% van de raden van bestuur kent te weinig over cyberveiligheid”

Marc Vael

VOORZITTER STUDIECENTRUM VOOR AUTOMATISCHE INFORMATIEVERWERKING (SAI VZW)

Vanuit zijn meer dan 55 jaar ervaring met kennisdeling over IT helpt SAI.be nu ook raden van bestuur om een proactieve rol op te nemen op vlak van cyberveiligheid.

Tekst: Joris Hendrickx

“Bestuurders dragen de ultieme verantwoordelijkheid voor hun organisatie. Vanuit die rol en ervaring zijn zij doorgaans ook goed in controleren en in risicobeheer”, opent Marc Vael, voorzitter van het Studiecentrum voor Automatische Informatieverwerking (SAI vzw). “Een sterk groeiend risico dat sinds enkele jaren in de top drie staat van belangrijkste risico’s, is cybersecurity. Helaas hebben veel bestuurders daar vandaag geen of onvoldoende kennis van omdat cybersecurity veelal wordt gepercipieerd als een technologieprobleem.”

Proactief in plaats van reactief handelen

“Bestuurders spelen het thema daarom door met de vraag om erover te rapporteren wanneer het fout loopt. Die reactieve aanpak is echter niet meer voldoende: bestuurders moeten ook proactief naar cyberrisico’s kijken én er een visie op hebben. De Amerikaanse beurswaakhond SEC eist daarom nu dat minstens één bestuurder technische kennis heeft over cybersecurity. Daarnaast dient de raad van bestuur minstens enkele keren per jaar het thema cybersecurity proactief te behandelen. Helaas is vandaag maar liefst 90% van de raden van bestuur niet klaar om daar aan te voldoen”, aldus Vael.

Kennisoverdracht op maat van bestuurders

Om die kloof te dichten, ondersteunt SAI.be onder andere Guberna, de Belgische vereniging van bestuurders, om hun kennis rond cyberveiligheid te verhogen. Zo kan er een betere governance ontstaan waarbij bestuurders proactief naar cyberrisico’s kijken en ook de nodige maatregelen treffen om die risico’s onder controle te houden. Vael: “We streven er constant naar om de principes van cybersecurity op een toegankelijke manier uit te leggen zodat iedere bestuurder deze kan begrijpen, zonder dat hij of zij een cybersecurityspecialist dient te worden. Deze kennis moet hen vooral toelaten om tijdens raden van bestuur de juiste vragen te stellen en op basis van de antwoorden de juiste beslissingen te nemen.”

Basisvragen voor iedere organisatie

“Daarnaast heeft SAI.be het CCB (Centrum voor Cybersecurity België) actief mee ondersteund bij het opstellen van enkele basisvragen die iedere organisatie zich zou moeten stellen om te weten waar het staat op vlak van cyberveiligheid en welke thema’s moeten worden verbeterd. Antwoorden op vragen als ‘Wie is er mee bezig binnen de organisatie?’, ‘Met wie werken we samen?’, ‘Welke maatregelen zijn momenteel in werking en worden deze gecontroleerd?’, ‘Hoe moeten we reageren als het fout loopt?’, ‘Zijn we ervoor verzekerd?’, enz. moeten ervoor zorgen dat bestuurders op elk moment de juiste beslissingen kunnen nemen rond cybersecurity”, besluit Vael. ■

SAI | Meer weten? **sai.be**

Veel bestuurders hebben vandaag geen of onvoldoende kennis van cybersecurity omdat het veelal wordt gepercipieerd als een technologie-probleem.

MDR: als een expert vanop afstand een oogje in het zeil houdt

Jurgen van Eynde

SECURITY EXPERT WORTELL

Philippe Buyle

HEAD OF ICT STAD LOKEREN

Organisaties dienen continu te werken aan hun cybersecurity. Dat kan door het bewustzijn te verhogen, maar ook door zich te laten bijstaan in het detecteren van risico's en het correct reageren daarop.

Tekst: Joris Hendrickx

Waarom is het zo belangrijk om de security awareness bij organisaties te verhogen?

Jurgen van Eynde, Security Expert bij Wortell: "Phishing is vandaag de belangrijkste aanvalsformule. Bij maar liefst 80% van de succesvolle aanvallen is een menselijke actie betrokken. Vaak zijn mensen met minder technische vaardigheden het slachtoffer. Het is dus cruciaal om dat via trainingen te verbeteren. Een belangrijke boodschap daarbij is dat mensen vooral moeten durven aan te geven dat ze iets hebben gezien dat niet ok is en vervolgens hulp moeten zoeken. De IT-afdeling heeft trouwens veel liever dat je op voorhand een vraag stelt dan dat ze achteraf veel tijd moet steken in het proberen oplossen van ernstige problemen."

Wat is in dat kader de meerwaarde van 'Managed Detection and Response'?

van Eynde: "Het grootste voordeel van Managed Detection and Response (MDR) is dat je gegarandeerd 24/7 expertise ter beschikking krijgt, kennis waar veel bedrijven niet de middelen voor hebben om die intern te voorzien."

Philippe Buyle, Head of ICT bij Stad Lokeren: "IT-diensten zijn vaak onderbemand en daardoor niet in staat om de toenemende workload op te vangen. Ze zien de meldingen en potentiële risico's wel binnenkomen op hun dashboards, maar hebben onvoldoende tijd en kennis om alles te correleren en begrijpen. In die zin is MDR een enorme meerwaarde omdat er dan continu iemand vanop afstand meekijkt. Dat maakt dat we ook veel sneller en gerichter kunnen ingrijpen,."

Hoe verloopt dat in de praktijk bij Stad Lokeren?

Buyle: "Hoewel wij bij Stad Lokeren een voldoende ruim IT-team hebben, besef ik dat een team nooit voldoende competenties heeft om alle nieuwe ontwikkelingen te kunnen opvolgen, exploreren en toepassen. Daar is nu eenmaal bijkomende externe expertise voor nodig. Bovendien helpt het ook om een tunnelvisie te vermijden. We zijn vertrokken vanuit een analyse van de omgeving waarbij de pijnpunten werden geïdentificeerd, aangepakt en gemonitord. Nu hebben we nog steeds een maandelijkse meeting met het MDR-team om te bespreken wat er gebeurd is en welke verbeteringen mogelijk zijn in onze omgeving. Security is nu eenmaal een continu proces."

van Eynde: "We gaan inderdaad verder dan enkel bescherming. Philippe en zijn team worden maandelijks gestimuleerd en geholpen om te blijven verbeteren. Cybersecurity evolueert immers iedere dag. Je moet er dus aan blijven werken." ■

IT-diensten zijn vaak onderbemand en daardoor niet in staat om de toenemende workload op te vangen. Dankzij MDR kunnen ze veel sneller en gerichter ingrijpen in geval van dreiging.

wortell

Meer weten?
wortell.be

"Preventie begint bij het identificeren van de risico's"

Dries Plasman

DIRECTOR OF MARKETING AND PRODUCT MANAGEMENT CEEYU

Preventie tegen cybercriminaliteit begint bij het zo goed mogelijk identificeren van de risico's, om ze daarna op een efficiënte manier te kunnen aanpakken. Bij die preventieve detectie dien je trouwens ook je kritische leveranciers te betrekken.

Tekst: Joris Hendrickx

Hoe belangrijk is het om je cyberrisico's preventief te identificeren?

Dries Plasman, director of marketing and product management bij Ceeyu: "De cybercriminaliteit neemt exponentieel toe. Bedrijven worden hierdoor steeds meer blootgesteld aan externe cybersecurityrisico's, denk maar aan een hacker die van buitenaf probeert om het bedrijfsnetwerk binnen te dringen door gebruik te maken van zwakheden in de systemen. De kosten daarvan kunnen al snel enorm omlopen. Het is daarom cruciaal dat je als bedrijf alles uit de kast haalt om er - binnen een redelijke kost weliswaar - voor te zorgen dat je je risico's minimaliseert. Dat doe je niet door enkel een cybersecurityverzekering af te sluiten. Je kan namelijk best eerst jezelf zo goed mogelijk beschermen. De verzekeraars worden daar trouwens alsmaar strenger op én hebben bovendien hun prijzen sterk verhoogd, net door de toegenomen impact van cybercriminaliteit en de beperkte bescherming die kmo's vandaag vaak voorzien. Het Europees Parlement vaardigde bovendien eind 2022 de NIS2-directive uit. Hierdoor zullen bedrijven vanaf vijftig werknemers in een tiental kritische sectoren vanaf eind 2023 aan minimale vereisten moeten voldoen inzake cybersecurity. Eén daarvan is een regelmatige audit van kritische leveranciers."

Waarom moeten bedrijven ook hun leveranciers hierin betrekken?

"Steeds vaker verkrijgen criminelen toegang tot de netwerken van bedrijven via een derde partij die digitaal met dat bedrijf verbonden is. Aanvallen via derde partijen zijn vandaag zelfs de belangrijkste oorzaak van cyberaanvallen op bedrijven. Vaak worden er bij zo'n derde partij ook data gestolen die vervolgens worden gebruikt voor een inbraak of phishingaanval. Zelfs wanneer de inbraak toch beperkt blijft tot je leverancier, ondervind je als bedrijf impact omdat die leverancier zijn activiteiten tijdelijk moet onderbreken."

Steeds vaker verkrijgen criminelen toegang tot de netwerken van bedrijven via een derde partij die digitaal met dat bedrijf verbonden is.

Ceeyu

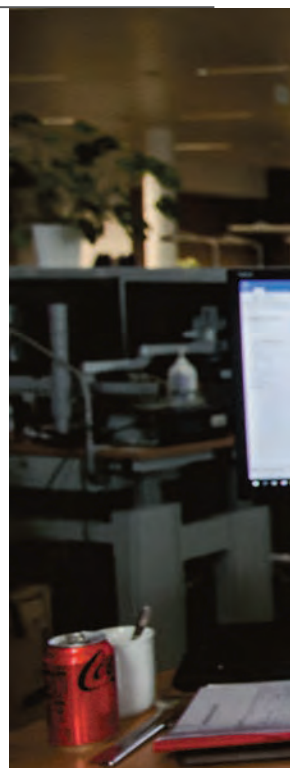
Meer weten?
ceeyu.io

#Wist je dat?

- Meer dan één Belgische kmo op vijf was al slachtoffer van een IT-beveiligingsincident.
- Ongeveer de helft van de Belgische kmo's riskeert haar gegevens te verliezen in geval van een cyberaanval.
- Maar liefst 80% van de Belgische kmo's doet geen beroep op een expert voor de IT-beveiliging.

Hoe kan Ceeyu bedrijven hierin ondersteunen?

"Ceeyu vertrekt steeds vanuit het perspectief van de hacker. We scannen je bedrijf van buitenaf om zwakheden te detecteren. Hetzelfde doen we bij je kritische leveranciers. We doen dat niet enkel geautomatiseerd, maar hebben ook een digitale assessment tool uitgewerkt waarmee je als bedrijf vragenlijsten kan opstellen voor leveranciers en klanten. Beide vormen zijn een noodzakelijke aanvulling van elkaar: de automatische assessment zorgt voor efficiëntie en objectiviteit, de vragenlijst voor aanvullende informatie over zaken die niet via een geautomatiseerde scan kunnen worden achterhaald." ■



Veiligheidsberoepen doen noodoproep aan burgers:

“We streven naar een relatie van wederzijds vertrouwen en respect”

De campagne ‘Wederzijds Respect’ van de FOD Binnenlandse Zaken beoogt een versterkte relatie tussen burgers en veiligheidsberoepen met meer wederzijds vertrouwen en respect, en minder agressie en geweld. Om te illustreren hoe het wel en niet moet, verzamelden we enkele getuigenissen van hulpverleners bij de brandweer, de Civiele Bescherming en de noodcentrale 112.

Tekst: Joris Hendrickx

Verbale agressie naar ambulanciers

Eddy Van Havere, preventieadviseur brandweerzone Rivierenland: “Brandweermannen en ambulanciers moeten soms in erg moeilijke omstandigheden werken. Zo werd onlangs een ziekenwagen opgeroepen om hulp te bieden in een flatgebouw. Voor de hoofdingang stond echter al een wagen geparkeerd, waardoor de ambulanciers genoodzaakt waren om zich op de openbare weg te plaatsen. Terwijl zij binnen hulp aan het bieden waren, stond er intussen een andere wagen geparkeerd, waardoor de draagberrie er niet meer langs kon. Toen de ambulanciers vroegen om de wagen te verplaatsen, kregen zij al snel te maken met verbale agressie. Dit soort van omstandigheden komt steeds vaker voor in onze job. Ook bij de brandweer stellen we een toename vast. Zo begrijpen veel mensen niet dat ze tijdens een filevorming een hulpstrook moeten vrijhouden voor de hulpdiensten. Soms worden we zelfs bewust gehinderd. Er is af en toe een gebrek aan wederzijds respect, terwijl wij er net zijn om mensen te helpen. Onze mensen proberen nochtans steeds rustig te blijven en geen geweld uit te lokken.”

Bekogeld met flessen, stenen en vuurwerk

Mohamed Chelh, brandweerman en ambulancier in Brussel: “Op nieuwjaarsnacht werd onze ziekenwagen opgeroepen voor een jongere die van de vierde verdieping was gevallen. Ondanks een snelle aankomst en een reanimatiepoging stierf de patiënt ter plekke. Daarna sloeg de sfeer om en werden we bekogeld met flessen, stenen en vuurwerk. Samen met de familie, vrien-

© FOTO'S: PRIVÉ/BRUNO BOSILO

Veel mensen begrijpen niet dat ze tijdens een filevorming een hulpstrook moeten vrijhouden voor de hulpdiensten. Soms worden we zelfs bewust gehinderd.

Eddy Van Havere

PREVENTIEADVISEUR BRANDWEERZONE RIVIERENLAND

We krijgen regelmatig te maken met mensen die geagiteerd naar onze centrale bellen en vragen om onmiddellijk een ambulance te sturen zonder dat we daar vragen bij mogen stellen.

Christophe Orban

PLOEGCHEF BIJ DE NOODCENTRALE 112 LUIK

De hulpdiensten rukken enkel uit wanneer iemand hulp nodig heeft. In plaats van ons verbaal of fysiek te belagen, zouden mensen ons net moeten verwelkomen en helpen.

Mohamed Chelh

BRANDWEERMAN EN AMBULANCIER IN BRUSSEL

din en vrienden van de jongen moesten we vluchten. Ik voelde me enorm gegeneerd, zeker omdat ik zelf ben opgegroeid in de Brusselse wijken. Hoewel mijn vrienden en ikzelf ook niet altijd even braaf waren, wisten we wel waar de grens lag en dat je respect moest tonen voor de hulpdiensten. Wij rukken enkel uit wanneer iemand hulp nodig heeft. In plaats van ons te bekogelen, zouden ze ons moeten verwelkomen."

"Als antwoord hierop werk ik nu samen met een jeugdwerker aan een sessie om jongeren te leren wat de brandweer precies doet, waarom het zo belangrijk is dat we ons werk op een veilige manier kunnen doen, hoe ze ons kunnen helpen of bij ons kunnen komen werken, en hoe ze iemand kunnen reanimeren. Ik ben ervan overtuigd dat zo'n educatieve en toegankelijke aanpak, in combinatie met bestraffing, de beste impact zal hebben."

Onbegrip en frustratie door moeilijke keuzes bij overstromingen

Pascal Pirotte, brandweerman-ambulancier in de hulpverleningszone Vesdre, Hoëgne & Plateau: "Bij de overstromingen in Wallonië in 2021 werkte ik samen met mijn collega's de klok rond om mensen zo goed mogelijk te helpen. Personeel was er genoeg, maar helaas kwamen we heel wat materiaal tekort omdat we te maken hadden met een nooit eerder geziene ramp. Zo waren de motoren van onze boten niet opgewassen tegen de sterke stroming, waardoor we niet overal hulp konden bieden. Bovendien ontbrak er door de omvang van de ramp een duidelijke hiërarchie en coördinatie. Onze teams waren verspreid en deden op basis van hun eigen afwegingen elk hun best. We beslisten al snel om ons volledig te focussen op het redden van mensen. Helaas kregen we ook te maken met heel wat onbegrip en frustratie van mensen die helemaal radeloos waren en niet begrepen waarom we bepaalde keuzes moesten maken."

Nood aan betere medewerking bij noodoproep

Christophe Orban, ploegchef bij de Noodcentrale 112 Luik: "Wij zijn er om hulpdiensten uit te sturen naar burgers die dringende medische hulp of brandweerhulp nodig hebben. We krijgen echter regelmatig te maken met mensen die geagiteerd naar onze centrale bellen en vragen om onmiddellijk een ambulance te sturen zonder dat we daar vragen bij mogen stellen. Op dat vlak zou er meer begrip en respect voor onze job moeten zijn. Wij zijn als professionals opgeleid om op basis van bepaalde vragen snel een correct beeld samen te schetsen van wat er gaande is, en dan te beoordelen welke middelen we waar moeten inzetten. Maar dat kan dus enkel als men onze vragen beantwoordt. Daarnaast is er soms een gebrek aan bewustzijn en respect vanwege hulpverleners die door ons worden uitgestuurd. Onze job is nu eenmaal erg complex. Wij dienen met slechts een kort telefonisch gesprek de juiste informatie te verzamelen om vervolgens zo objectief mogelijk in te schatten hoe ernstig de noodvraag is en welke middelen en dringendheid daarvoor nodig zijn."

Maar ook: dankbaarheid bij bouw van veldhospitaal in Turkije

Tom Van Loon, Civiele Bescherming Brasschaat: "Vlak na de verwoestende aardbeving in Turkije trok ik naar ginder om er samen met mijn collega's van de Civiele Bescherming een veldhospitaal te bouwen. Toen we op de locatie aankwamen, was er niets en wist de lokale bevolking ook niet wat we er precies kwamen doen. De eerste nachten moesten we in vriestemperaturen slapen en de eerste vijf dagen waren er geen sanitaire voorzieningen. Ondanks de zeer uitdagende omstandigheden en de moeilijke logistiek slaagden we er na het nivelleren van het terrein in om in slechts drie dagen het volledige hospitaal op te zetten, in te richten met de nodige materialen en onze eigen waterzuivering en stroomtoevoer te voorzien. Op de vijfde dag was het hospitaal operationeel en ontvingen we onze eerste patiënten."

"We leefden in die eerste weken niet enkel heel intensief samen met alle Belgische hulpverleners, ook met onze Turkse patiënten en de omwonenden bouwden we een nauwe band op. Zij waren enorm gastvrij en boden ons zelfs vanaf onze aankomst al voedsel aan."

Conclusie: naar een versterkt vertrouwen en een positieve dialoog

Zoals blijkt uit de laatste getuigenis zijn er ook positieve verhalen, maar helaas halen deze te weinig de media. Het is duidelijk dat elke vorm van geweld tegen hulpverleners ontoelaatbaar is. Daarom riep minister van Binnenlandse Zaken Annelies Verlinden in 2021 de campagne 'Wederzijds Respect' in het leven. Burgers moeten de veiligheidsberoepen leren kennen en dienen bewust te worden gemaakt van het belang van hun taken. Zo kan een relatie van wederzijds vertrouwen en respect worden opgebouwd. De FOD Binnenlandse Zaken zal blijven werken aan acties om de burger en de veiligheidsberoepen dichter bij elkaar te brengen. ■

CAMPAGNE

De campagne 'Wederzijds Respect' heeft als doel om burgers te laten kennismaken met de veiligheidsberoepen en het belang van de taken van hulpverleners die dagdagelijks in de weer zijn om anderen te helpen. Informatie over alle acties vind je op de campagnewebsite

wederzijdsrespect.be

ibz
Civiele Veiligheid
Sécurité civile

ibz BeSafe | AD Veiligheid & Preventie

GTV

STAY CONNECTED

Gentsesteenweg 125, 8530 Harelbeke

056 / 730 730 www.gtv.be info@gtv.be

Cloud & IT

cloud office | professionele wifi | IT netwerk



Camera & Telefonie

telefonie | camerabewaking | gsm versterker



Scan de QR code voor een GRATIS analyse

Radiocommunicatie

walkietalkies | gidssystemen | CB



Automotive

achteruitrijcamera | gps tracking | autosport



Onze missie: Bedrijven en organisaties voorzien van technologische **communicatie-oplossingen** die hun dagelijkse werking **efficiënter** en **veiliger** maken.

Vergunning en certificatie verhogen kwaliteit van elektronische beveiliging

ALIA Security, de Belgische beroepsvereniging van elektronische beveiliging, onderschrijft de meerwaarde van vergunde en gecertificeerde installateurs om de kwaliteit in de sector te verhogen. **Tekst:** Joris Hendrickx

Patrick Van Liempt

SECRETARIS-GENERAAL
ALIA SECURITY

Waarom is het belangrijk om bij het plaatsen van elektronische beveiliging een beroep te doen op een vergunde installateur?

Patrick Van Liempt, secretaris-generaal bij ALIA Security: "De plaatsing van alarm- en camerasystemen is onderhevig aan de wet tot regeling van de private en bijzondere veiligheid, beter bekend als de 'Wet Jambon'. Die stelt dat iedere installateur van zulke systemen vergund moet zijn door de FOD Binnenlandse Zaken. Bovendien moet elke werknemer voldoen aan bepaalde opleidingscriteria en beschikken over een identificatiekaart met vermelding van zijn functie. We raden vanuit ALIA Security dan ook aan om steeds samen te werken met een vergunde installateur die de nodige opleidingen heeft gevolgd, in staat is om een kwalitatieve conceptie en risicoanalyse uit te voeren, een 24/7 service biedt én achteraf uiteraard ook kan instaan voor het verplichte jaarlijkse onderhoud. Een handig overzicht van vergunde installateurs vind je op onze website."

Wat zijn de risico's als men dat niet doet?

"Doe-het-zelfsystemen worden vaak foutief geplaatst omdat particulieren geen kennis van conceptie hebben en deze ook niet worden onderhouden. Dat leidt vaak tot een onnodig alarm en dus overbelasting van de ordediensten, met sancties tot gevolg. Bovendien kunnen deze systemen vaak makkelijk worden gehackt om bijvoorbeeld toegang te krijgen tot de woning of via camera's mee te kijken in de privésfeer."

Wat is de meerwaarde van een vrijwillig kwaliteitslabel als INCERT?

"INCERT is al twintig jaar lang het enige Belgische vrijwillige kwaliteitslabel voor diefstalbeveiliging. Deze certificatie van installateurs, producten en alarmcentrales gebeurt volgens specifieke kwaliteitsnormen en technische nota's die rigoureus dienen te worden gevolgd. Bovendien worden ze daar ook jaarlijks op geauditeerd, wat aantoont dat de vrijwillig aangesloten installateurs het echt ter harte nemen. Intussen zijn al zo'n driehonderd installateurs INCERT-gecertificeerd. Via de website kan je trouwens opzoeken welke installateurs in jouw regio dit kwaliteitslabel dragen."

"De grote meerwaarde van dit kwaliteitsmerk is dat het ook wordt onderschreven door verzekeringsmaatschappijen, fabrikanten, certificatieorganismen, preventieadviseurs en adviesbureaus voor veiligheid. Dat laat toe om door middel van werkgroepen steeds verder te zoeken naar technische evoluties om die dan zo goed mogelijk toe te lichten aan de gecertificeerde installateurs." ■

Doe-het-zelfsystemen worden vaak foutief geplaatst. We raden dan ook aan om steeds samen te werken met een vergunde installateur.

Meer weten?
aliasecurity.be
incert.be

De preventieadviseur vs. de facility manager: wie neemt welke rol op binnen je organisatie?

Tanja Barella

DIRECTOR BELFA

Veiligheid, preventie en welzijn. De begrippen worden vaak in één adem genoemd, maar *what's in a name* en wie is waarvoor verantwoordelijk binnen organisaties? Welke rol spelen de facility manager en de preventieadviseur? Tanja Barella, director bij belfa, legt uit.

"Het antwoord gaat verder dan een pure taakomschrijving, en de functies dreigen weleens te botsen. Dit terwijl beide partijen, net zoals hun werkgever, hetzelfde doel nastreven: het maximale welzijn van de werknemer. Zoals zo vaak is er echter de kloof tussen de theorie en de praktijk. We zien nog te vaak dat de preventieadviseur en facility manager op een andere golflengte zitten, niettegenstaande ze mekaar in principe moeten aanvullen en versterken. De verklaring ligt voor de hand. De preventieadviseur handelt vanuit de pure wet en heeft een informerende of instruerende rol. De facility manager probeert de wettelijke verplichtingen zo goed mogelijk te rijmen met de realiteit op de werkvloer, waarbij het creëren van een optimale werkplek voor de werknemers centraal staat. Hij probeert hen, de bezoekers én derden maximaal te ontzorgen en te ondersteunen. Geen gemakkelijke opdracht

© FOTO: PRIVÉ

in tijden waarin de functie van de werkplek nieuwe invullingen krijgt, de interne en externe klanten alsmaar kritischer worden en de war for talent hevig woedt. Komt daarbij dat de facility manager een budgettaire verantwoording moet afleggen en nog te vaak puur als 'de kostenpost' wordt gezien."

Onbekend is onbemind

"Hoe deze kloof te dichten valt? Mits goede afspraken, die worden gestuurd vanuit de risicoanalyse. Door in overleg te treden over de taakomschrijvingen, nauwer en constructiever samen te werken en vooral de werkgever te betrekken bij de acties. Onbekend is immers onbemind. Je vraagt je misschien nog af of het mogelijk is om de functie van preventieadviseur en facility manager in één persoon te verenigen? Ja, afhankelijk van de grootte van de organisatie en mits duidelijke afbakening van de taken en verantwoordelijkheden. En vergeten we ook hier de rol van de HR-afdeling niet, met het oog op constructief overleg. Facility management speelt zich immers meer en meer af op de raakvlakken tussen diverse afdelingen in een bedrijf. Een kruisbestuiving die het hoger doel enkel ten goede komt: de veiligheid en het welzijn van de mens centraal stellen." ■

De preventieadviseur handelt vanuit de pure wet en heeft een informerende of instruerende rol.

De facility manager probeert de wettelijke verplichtingen zo goed mogelijk te rijmen met de realiteit op de werkvloer.

Veiligheid op het werk: met deze tips verminder je de risico's op arbeidsongevallen


© FOTO: PRIVÉ

Uit de statistieken blijkt dat de meerderheid van de ongevallen met uitzendkrachten aan het begin van een opdracht plaatsvindt.

Belgische werkgevers doen jaarlijks een beroep op ruim 600.000 uitzendkrachten. Om deze samenwerking optimaal te laten verlopen, bestaan er tools om de gezondheid en veiligheid van deze arbeidskrachten te helpen waarborgen.

Als werkgever verwacht u dat een uitzendkracht in een mum van tijd een werknemer met ziekteverlof vervangt of uw team ad hoc versterkt. Die persoon dient zich in een recordtijd te integreren en aan te passen. Het spreekt dan voor zich dat het onthaal dat u moet organiseren, bepalend is voor de kwaliteit van zijn prestaties, motivatie en - vooral - zijn veiligheid en gezondheid op het werk. Het onthaal vormt met andere woorden een cruciale fase voor alle betrokken partijen.

Het onthaal als cruciale factor

Het onthaal van nieuwe werknemers is een wettelijke verplichting volgens de wetgeving inzake welzijn op het werk. Dat is van het grootste belang wanneer de nieuwkomer een uitzendkracht is die de werkpost tijdelijk en in sommige gevallen voor zeer korte tijd zal bekleden. Hij zal in een zeer korte tijdspanne veel informatie moeten opslaan die essentieel is voor zijn veiligheid en zijn gezondheid op het werk, maar ook voor zijn succesvolle integratie in de onderneming. Als werkgever bent u verantwoordelijk voor zijn welzijn op het werk vanaf het moment dat hij uw onderneming betreedt. U moet hem dezelfde bescherming garanderen als uw eigen en vaste werknemers.

Een blik op de statistieken

Uit de statistieken blijkt dat de meerderheid van de ongevallen aan het begin van een opdracht plaatsvindt. De oorzaken zijn divers, maar een gebrek aan kennis van de omgeving en apparatuur, aangevuld met het ongetwijfeld te vaak of ongepast gebruik van 'vindingrijkheid' in bepaalde werkomstandigheden, spelen onvermijdelijk een rol. Het onthaal dient steeds plaats te vinden voor de uitzendkracht zijn opdracht start. Sommige inlichtingen kunnen echter worden doorgegeven naarmate het werk vordert. Daarom is het steeds een goed idee om een 'peter' of 'meter' aan te stellen die de uitzendkracht kan begeleiden na de formele onthaalprocedure. ■

Arbeidsongevallen in cijfers

De statistieken van de arbeidsongevallen met uitzendkrachten in Wallonië tonen aan dat de frequentie- en ernstgraad in deze regio merkbaar hoger liggen dan het nationaal gemiddelde.

- In 2021 bedroeg de **frequentiegraad** - een verhouding tussen het aantal arbeidsongevallen dat zich heeft voorgedaan en het totaal aantal gepresteerde uren - voor het Waalse Gewest 45,71 tegenover 39,53 voor het nationale gemiddelde.
- De **ernstgraad** - het aantal dagen arbeidsongeschiktheid in verhouding tot het totaal aantal gepresteerde uren - bedroeg 3,59 tegenover 2,98 op nationaal niveau. Deze indicatoren liggen iets lager dan het nationale gemiddelde in de twee andere regio's van het land.
- In 2021 was Wallonië goed voor 23,32% van de gepresteerde uren in uitzendarbeid tegenover 68,35% voor Vlaanderen en 8,33% voor het Brussels Hoofdstedelijk Gewest.

Bron cijfers: Preventie & Interim

VEILIG MET VINK

ZORG VOOR PROCESBEVEILIGING

Safety shields als anti spatbeveiiliging

Onze safety shields zorgen voor extra bescherming bij flenzen en kranen indien lekkages zich voordoen. De shields voorkomen een vloeistof spray naar mens en omgeving door deze meteen op te vangen in een hoog chemisch resistente cover.

Monoblok afsluiters voor minder lekkage

Minder dichtingen = minder kans op lekkage. Onze kranen zijn voorzien van veiligheidsvergrendeling om de kraan in de juiste positie te behouden. Bovendien zijn ze beschikbaar in verschillende diameters voor bijna elke toepassing.

CREËER EEN VEILIGE WERKOMGEVING

Verhoogde veiligheid, comfort en energiebesparing met Vink Window Films

Onze veiligheidsfolies voorkomen verwondingen door glasscherven bij elkaar te houden. Bovendien verminderen onze zonwerende windowfolies de inkomende warmte, wat leidt tot besparingen op aircokosten en een aanzienlijke verbetering van het binnenklimaat.

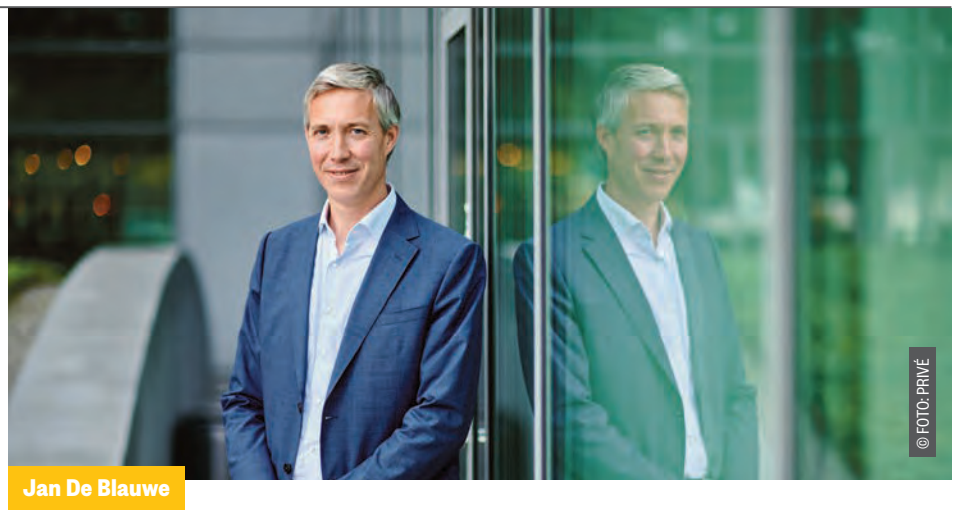
Teddy Pro Beschermende bumpers

TEDDY PRO is een flexibel profiel dat geschikt is voor diverse toepassingen. Het biedt uitstekende bescherming aan werknemers tegen scherpe randen en hoeken van rekken of andere constructies.

VINK

Meer info op onze website

“Data beschermen is als het bouwen aan een nieuwe auto”



Jan De Blauwe

COO NVISO EN VOORZITTER CYBER SECURITY COALITION

Veel bedrijven werken vandaag aan hun digitale transformatie. Ze implementeren nieuwe technologieën, vernieuwen hun interne processen of ontwikkelen een nieuw aanbod aan datagedreven diensten. Deze technologische innovatie gaat gepaard met een aantal nieuwe uitdagingen, zoals cybersecurity. Jan De Blauwe, COO bij NVISO en voorzitter van de Cyber Security Coalition, legt uit hoe we die uitdagingen samen kunnen aanpakken.

“Het beveiligen van je data wordt helaas nog te vaak onderschat. Dat is zelfs begrijpelijk, want vaak is het risico onbekend of moeilijk in te schatten. Soms is men ook bang dat beveiliging de digitale transformatie zal afremmen of duurder maken. En voor een toepassing die enkel intern wordt gebruikt, is cybersecurity meestal niet de hoogste prioriteit. Het gevaar daarvan is dat men finaal vergeet om een cyberbeveiliging in te bouwen of dat er pas op het einde van het transformatieproject een oplossing wordt geïntegreerd. Onze ervaring leert dat het net dan vaak mis gaat. Door (te) lang te wachten, wordt het complexer om nog in het ontwerp in te grijpen en worden het risico op fouten of lacunes in de beveiliging net groter.”

> Samenwerking is cruciaal. Als het over beveiliging gaat, zijn we immers geen concurrenten. De enige concurrenten zijn hackers en andere criminelen.

Een nieuwe auto

“Vergelijk het met het bouwen van een nieuwe auto: het is ondenkbaar dat men eerst een auto zou ontwerpen om de veiligheidsgordels, airbags en andere beveiligingsmaatregelen pas toe te voegen als de wagen bijna van de band rolt. Integendeel: al bij het eerste ontwerp van een nieuw model, staat veiligheid voor de bestuurder en de inzittenden centraal. Veiligheidsgordels zitten standaard ingebouwd in de zetels en airbags worden zo ontwikkeld dat ze netjes verborgen zitten. Ook een hoop technologische snufjes worden van meet af aan in het design meegenomen. En aan het einde wordt dat nieuwe model onderworpen aan hele reeks crashtests.”

Brede waaier aan slimme oplossingen

“Zo moet het ook gaan met het beveiligen van digitale oplossingen. Goede securitymensen zijn specialisten in hun vak en hebben toegang tot een brede waaier aan slimme oplossingen. Als ze in een vroege fase bij een project betrokken zijn, kunnen ze hun kennis en kunde netjes integreren in het ontwerp en kunnen ze alles uitgebreid testen voor de ingebruikname. Het eindresultaat wordt dan een veilige oplossing die de gebruiker comfort geeft en vlot bruikbaar is. En dat is helemaal niet duurder dan wanneer je in een latere fase de cybersecurity aanpakt, integendeel.”

Netwerk van en voor experten

“Uiteraard heeft niet elke organisatie voldoende expertise in huis. Gelukkig kan je rekenen op flink wat ervaren dienstverleners om je cyberbeveiliging op punt te stellen. Het blijft echter een complex vakgebied en de meeste cyberprofessionals werken in een klein team. Net daarom hebben we de Cyber Security Coalition gevormd: een netwerk waar experten met elkaar in contact komen en in alle vertrouwen informatie en best practices met elkaar kunnen delen. Als het over beveiliging gaat, zijn we immers geen concurrenten. De enige concurrenten zijn hackers en andere criminelen. Ons netwerk groeit nog elke dag en wie interesse heeft in de Coalition, is zeker welkom.” ■

“De vraag is niet ‘of’ u slachtoffer wordt van een cyberaanval, maar wanneer”

Het risico op cyberaanvallen neemt voortdurend toe. Gemiddeld zijn er honderd cyberaanvallen per dag, een stijging van 37% ten opzichte van 2019. Bijna 70% van die aanvallen ontsnapt bovendien aan vervolging. Getuigenissen van bedrijven die slachtoffer zijn van cyberaanvallen tonen aan dat ondernemingen vaak in het duister tasten of improviseren op het moment van een cyberincident.

Sinds de pandemie e-commerce en thuiswerk een stevige duw in de rug heeft gegeven, zijn cybercriminelen er als de kippen bij om daar gebruik van te maken. “Een goede veiligheidsstrategie was altijd al belangrijk voor bedrijven, maar de coronacrisis zette dat nog eens extra in de verf”, vertelt Nathalie Ragheno, eerste adviseur Competentiecentrum Recht & Onderneming bij het VBO. “Uit het jaarrapport van de Cyber Security Coalition - een coalitie van toonaangevende spelers uit de academische wereld, overheden, de private sector en het VBO - blijkt dat organisaties amper 65% van de gestolen data kunnen recupereren, zelfs al wordt er losgeld betaald. Het hoeft geen verdere uitleg dat de gevolgen voor het bedrijf in dat geval catastrofaal zijn. Uit cijfers van sectorfederatie Agoria blijkt ook dat 38% van de bedrijven die slachtoffer worden van een aanval hun activiteiten tijdelijk gedwongen stil moeten zetten. Deze cijfers onderstrepen eens te meer waarom een goed continuïteitsplan onontbeerlijk is voor elke onderneming.”

Stappenplan

“In de ‘Cyber Incident Roadmap’ van het VBO, een gids die bedrijven begeleidt van het moment dat een incident wordt ontdekt tot het normaliseren van de situatie, kunnen we het niet genoeg herhalen: de juiste voorzorgsmaatregelen en een goede voorbereiding op cyberincidenten zijn essentieel. Alle personeelsleden moeten over het risico worden geïnformeerd en gesensibiliseerd, want de gevolgen op het vlak van reputatie, organisatie en financiële lasten kunnen zeer ernstig zijn. Er moeten dus procedures worden ingesteld om op een cyberincident voorbereid te zijn”, klinkt het. Ragheno raadt volgende vier stappen dan ook aan:

65%

Uit onderzoek blijkt dat organisaties **amper 65%** van de gestolen data kunnen **recupereren**, zelfs al wordt er losgeld betaald.

1. Ontwikkel een eigen ‘Cyber Incident Roadmap’ voor je bedrijf en bewaar dit ook op papier.
2. Bewaar een geüpdatete lijst van te contacteren instanties op papier.
3. Organiseer interne opleidingen en sensibiliseringscampagnes om cyberaanvallen te voorkomen.
4. Stel een continuïteitsplan op met de meest essentiële en cruciale bedrijfsinformatie.

“Bedrijven moeten kunnen reageren om hun getroffen kritieke activiteiten, systemen en gegevens te herstellen”, benadrukt Ragheno. “De planning en voorbereiding moeten vóór een incident worden geïmplementeerd en zijn bepalend voor het niveau van cyberweerbaarheid. Bedrijven moeten er zich van bewust zijn dat de vraag vandaag niet meer is ‘of’ uw bedrijf ooit het slachtoffer wordt van een cyberaanval, maar wanneer. Het beste blijft natuurlijk voorkomen in plaats van genezen, maar in het geval van zo’n aanval moet een bedrijf een goed en robuust incidentresponsplan hebben.” ■

Nog voor de inbreker je huis of bedrijf betreedt, zullen trilsensoren al een signaal sturen naar onze meldkamer, die dan onmiddellijk kan reageren en indien nodig de hulpdiensten kan verwittigen.

Omdat we end-to-end alles intern beheersen, kunnen we heel efficiënt werken en nieuwe ontwikkelingen onmiddellijk opnemen in de volledige keten.

Ralph Gijbels

DIRECTOR OF OPERATIONS VERISURE

“Iedere woning en elk bedrijf is gebaat bij een allesomvattende en tegelijk toegankelijke veiligheidsoplossing”

Om een gerust veiligheidsgevoel te kunnen garanderen, dient een beveiligingssysteem allesomvattend te zijn én actief te worden gemonitord. Dat kan enkel met een partner die alle nodige competenties en diensten onder één dak integreert. **Tekst:** Joris Hendrickx

“We doen er alles aan om mensen een veiligheidsgevoel te geven”, vertelt Ralph Gijbels, Director of Operations bij Verisure. “Hiervoor werken we onder meer via een volledig gemonitord alarmsysteem. Concreet zorgen we er vanaf het begin voor dat je als klant op een goede manier wordt beveiligd én correct wordt opgevolgd. Daarmee willen we het verschil maken met doe-het-zelf alarmsystemen die helaas vaak een vals gevoel van veiligheid geven. Wanneer er dan bij afwezigheid wordt ingebroken, wordt daar gewoon niet op gereageerd. Ons gemonitord alarmsysteem, dat in verbinding staat met een professionele meldkamer, biedt op dat vlak een absolute meerwaarde.”

Preventieve functie

“Bovendien werkt ons systeem ook preventief. Alleen al het feit dat aan de buitenzijde van je woning of bedrijf duidelijk staat aangegeven dat er een gemonitord alarmsysteem aanwezig is dat in verbinding staat met een meldkamer, doet inbrekers tweemaal nadenken of ze er wel goed aan zouden doen om in te breken. Stel dat het toch tot een inbraak komt, dan zorgen we ervoor dat die tijdig wordt gedetecteerd. Nog voor de inbreker je huis of bedrijf betreedt, zullen trilsensoren al een signaal sturen naar onze meldkamer, die dan onmiddellijk kan reageren en indien nodig de hulpdiensten kan verwittigen. Als vergunde alarmcentrale hebben we hiervoor een rechtstreekse lijn met de politie, brandweer en andere diensten”, legt Gijbels uit.

Nieuwste evoluties en technologieën

“Bij Verisure bieden we echter nog veel meer dan een gemonitord alarmsysteem. We verzorgen in feite de complete veiligheid van je woning en bedrijf. Zo kunnen we branddetectie voorzien, maar ook SOS-meldingen. Mensen die zich niet goed voelen, kunnen met één druk op een knop heel snel in contact treden met onze meldkamer. Dankzij onze Guardian-app - die we enkele jaren geleden lanceerden - werkt het systeem zelfs buitenshuis: de app precies weet waar je bent wanneer je een hulpoproep lanceert. Hierdoor is ons aanbod ook absoluut niet enkel bedoeld voor de grotere woningen met een hoger risico op inbraak. Iedere woning en elk bedrijf is gebaat bij een allesomvattende en tegelijk toegankelijke veiligheidsoplossing”, klinkt het. “Zodra je klant wordt, houden we te allen tijde je systeem mee up-to-date. Dat gaat over zowel nieuwe componenten als nieuwe diensten. De Guardian-app is daar een goed voorbeeld van. Je bent dus steeds mee met de nieuwste evoluties en technologieën. Eén van de sterke punten van Verisure is dat we alles intern doen. Al onze producten worden door onszelf ontwikkeld en ook onze meldkamer werkt enkel met onze eigen systemen. Zelfs onze helpdesk en techniekers zijn niet uitbesteed. Omdat we dus end-to-end alles intern beheersen, kunnen we heel efficiënt werken en nieuwe ontwikkelingen onmiddellijk opnemen in de volledige keten.”

Anti-inbraakgordijn mét menselijke verificatie

“Op vlak van inbraakpreventie hebben we sinds enkele jaren nog een bijkomende troef in ons aanbod: ZeroVision. Dit anti-inbraakgordijn kan onmiddellijk worden geactiveerd wanneer de operatoren in onze meldkamer zien dat er in je woning of zaak wordt ingebroken. De reactietijd wordt hierdoor enorm ingekort omdat er geen tijd meer verloren gaat tussen het moment van de inbraak en het moment dat de politie arriveert. De inbreker zal dankzij het rookgordijn niets meer zien en bijgevolg niet anders kunnen dan zo snel mogelijk het gebouw terug te verlaten”, aldus Gijbels. “Belangrijk hierbij is om het verschil te maken met andere automatische rookgordijnoplossingen. Ons systeem wordt vanop afstand door een operator bediend, die eerst een grondige inschatting zal maken van de situatie. Hierdoor vermijd je dat het rookgordijn ook bij een vals alarm wordt geactiveerd, wat wel een groot risico is bij automatische systemen. Die menselijke verificatie is dus erg belangrijk.”

Marktleider met enorm groeipotentieel

“Verisure is sinds 2006 actief in België en is sindsdien uitgegroeid tot de nummer één aanbieder van gemonitorde alarmsystemen voor woningen en kmo’s in ons land. We beveiligen hier 150.000 klanten en onze meldkamer behandelt ongeveer 1,5 miljoen alarmen per jaar. Deze meldkamer is het eerste centrum voor bewaking op afstand in België dat voldoet aan de strengste Europese certificaties op het gebied van kwaliteit van de dienstverlening, snelheid van interventie en veiligheid voor de klant. We zijn onderdeel van de Verisure Group, die verspreid over zeventien landen zo’n vijf miljoen huishoudens en kleine ondernemingen beveiligt. In vergelijking met deze andere landen waar we actief zijn, ligt de penetratiegraad van gemonitorde alarmsystemen in België echter nog erg laag. Ondanks onze positie als marktleider zien we in België dus nog heel wat groeiopportuniteiten”, besluit Gijbels. ■

verisure | Meer weten? **verisure.be**

verisure

ZORG VOOR UW BEDRIJF

Dag en nacht

beschermt Verisure uw medewerkers en uw bedrijf. Onze experts staan 24 op 7 klaar en grijpen onmiddellijk in, maakt niet uit wat het noodgeval is. Verzeker uw veiligheid en gemoedsrust met het Verisure alarmsysteem.

Vraag een offerte aan op **Verisure.be**
of bel **0800 90 000**