

TOP SECURITY

SECURITY, BUILDING & RISK MANAGEMENT

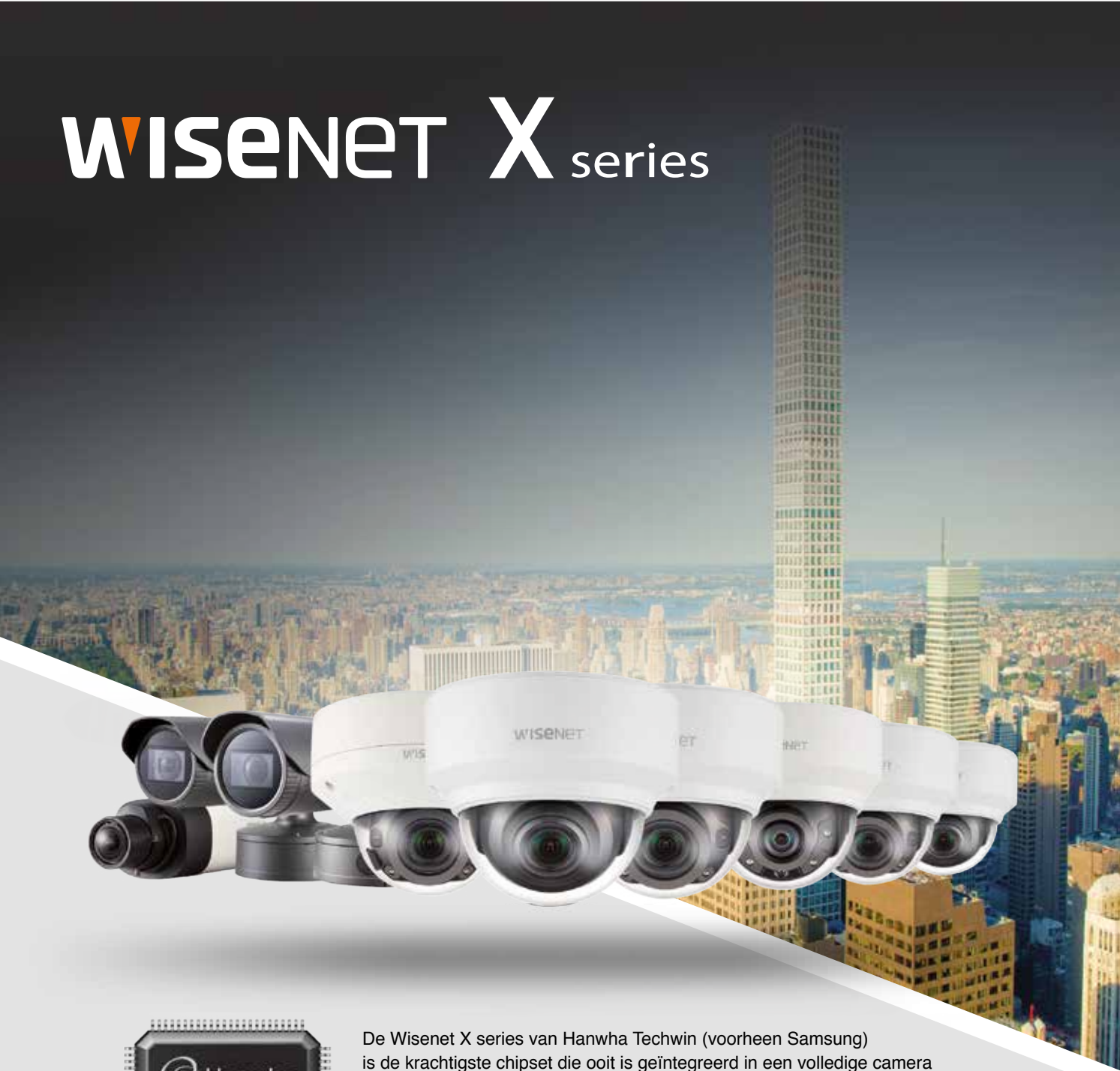
143 | JUL/AUG/SEP 2017

met de
medewerking van



**Recente ontwikkelingen op het vlak
van biometrische beveiliging**

Wisenet X series



De Wisenet X series van Hanwha Techwin (voorheen Samsung) is de krachtigste chipset die ooit is geïntegreerd in een volledige camera reeks. De door Hanwha zelf ontwikkelde Wisenet 5 chip is voorzien van een volledig nieuwe lay-out, waardoor deze beelden veel sneller kan verwerken. Hiermee heeft de Wisenet 5 range een ongekend hoge beeldkwaliteit met unieke features die kunnen worden toegepast voor een brede range aan video surveillance applicaties.

**150dB WDR bij full HD • Uitgebreide analytische functies
Superieure lichtgevoeligheid**



SmartSD NV-SA
Neerlandweg 22A
2610 Wilrijk
T 03 369 80 80
E info@smartsd.com
W www.smartsd.com



Colofon

TOP Security. Vakblad voor de beveiligingssector. Gratis verspreid naar veiligheidschefs in bedrijven, handelszaken, warenhuizen en banken; installatiebedrijven voor veiligheidssystemen; telebewakingsbedrijven; fabrikanten; verdelers; bewakingsondernemingen; Facility Managers, gebouwenbeheerders en voorschrijvers.

PERIODICITEIT

Driemaandelijks

HOOFDREDACTIE

Tilly Baekelandt
T 056/33 42 72
E tilly.baekelandt@fcomedia.be

REDACTIETEAM

Philip Declercq
Philip Vandenberg
Sammy Soetaert

T 056/77 13 10 | F 056/77 13 11
E redactie@topsecurity.be

VORMGEVING

Ruth Van Thuyne
E ruth.vanthuyne@fcomedia.be

RECLAME - ADVIES

FCO Media
Boulevard des Canadiens 118,
7711 Dottignies
T 056/77 13 10 | F 056/77 13 11
E filip.cossement@fcomedia.be

VERANTWOORDELIJKE UITGEVER

Filip Cossement
Boulevard des Canadiens 118
7711 Dottignies

ADRESWIJZIGINGEN

info@topsecurity.be

Version française: sur simple demande

Niets uit deze uitgave mag worden vervoelvoudigd en/of openbaar gemaakt worden door middel van druk, fotokopie, microfilm of op welke wijze ook, zonder voorafgaande schriftelijke toestemming van de uitgever. Voor onderkende artikels zijn alleen de auteurs aansprakelijk. Voor de inhoud van de advertenties zijn enkel de adverteerders aansprakelijk. De uitgever erkent geen enkel verplichting tot opname van aangeboden advertenties.



LID VAN DE UNIE VAN DE UITGEVERS
VAN DE PERIODIEKE PERS

www.topsecurity.be

04	NEWS
	OPINIE - SLOTENMAKERSUNIE
12	Waarom de vergunning van de slotenmaker wordt tegengehouden
	INTERVIEW OLIVIER DEMOULIN - NIEUWE VOORZITTER ALIA
17	“Ons beroep zal de komende vijf jaar volledig veranderen”
	VISIE
21	Dynamische securityplanning volgens gezond boerenverstand
	REPORTAGE
24	AnB-Rimex breidt aanbod aan geïntegreerde veiligheidsoplossingen uit
26	Paxton on tour met software-update en nieuw paneel
29	Hikshow toont toekomst vol innovatie
33	Biometrie: de aders in onze handpalm liegen niet
36	Bosch Talks 2017 stelt focus op veiligheid scherp
41	Gluren bij de burens
	EVENT
44	SST2017: geavanceerde security-oplossingen in Onderzeebootloods
47	Een halve eeuw brandpreventie
50	PRODUCT NEWS

Paxton wint IF Design award met Net2 Entry Touch Paneel

Het nieuwe Net2 Entry Touch Paneel is dit jaar in de prijzen gevallen in de categorie product design. Het paneel won de design award omwille van zijn nieuwste materialen en technieken. Tevens sprong het eruit vanwege het design. De jury was vol lof over de materialen zoals het scherm, de bediening en de gemakkelijke installatie.

<http://ifworlddesignguide.com/search/?search=paxton#/page/entry/199973-paxton-entry-touch/>



Vakbeurs New Security nu ook in Nederland!

Na het succes van New Security dit jaar in Leuven werd beslist om het evenement ook in Nederland te organiseren. Als locatie werd gekozen voor Expo Houten nabij Utrecht. Houten is vlot bereikbaar en heeft alle faciliteiten. De formule zal identiek zijn aan de Belgische versie van New Security. De beurs duurt twee dagen en zal ook tweejaarlijks plaatsvinden. Exposanten zijn importeurs, fabrikanten en groothandels. De bezoekers zijn installateurs en professionele eindklanten. New security NL vindt plaats op 5 en 6 april 2018. New Security BE is gepland op 14 en 15 februari 2019. Op die manier is New Security een Benelux-organisatie alternerend in België en Nederland. Langs deze weg hopen we tegemoet te komen aan de wensen van de exposanten en bezoekers. Voor alle praktische informatie kunt u steeds terecht op

www.new-security.nl

Dahua Europe biedt gratis productinformatie via Open Icecat

Een ruime selectie van de producten van Dahua is vanaf heden opgenomen in de Open Icecat-catalogus. Door de samenwerking met Icecat zal de Dahua productdata online beschikbaar zijn voor alle channelpartners, die de informatie zo makkelijk en snel kunnen integreren in hun e-commerce-platforms. Deze oplossing is gratis voor de channel partners, die op deze manier hun portfolio up-to-date kunnen houden met Dahua's huidige productlijn, inclusief artikelnummers, specificaties, marketingteksten en afbeeldingen. De investering in Icecat biedt de channelpartners diverse voordelen zoals meer efficiëntie, tijdswinst, een verhoogde online zichtbaarheid en een stijgende verkoop. De inhoud wordt meertalig en geoptimaliseerd voor eenvoudige productvergelijking. "Dankzij de connectie met Icecat kunnen wij onze klanten een nog betere service bieden en hen elk moment van de dag voorzien van de meest actuele en volledige digitale productdata van al onze producten. We zijn er zeker van dat deze samenwerking ons en onze channelpartners helpt om de salesdoelstellingen van de komende jaren te behalen", aldus Martijn Peeters (marketing manager Dahua Benelux).

www.dahuabenelux.com/nl/

Nextel winnaar Belgian HR Award

Nextel heeft op de uitreiking van de Belgian HR Awards door Trends en Kanaal Z, de HR Award for Internal Communication in de wacht gesleept. De jury heeft unaniem de campagne 'NForce Eachother' aangeduid als winnaar van deze felbegeerde titel. Aan de Award is een cheque van 33.500 euro verbonden. De 'NForce Eachother'-campagne die werd gelauwerd, kadert in het NForce 2020-plan waarmee Nextel tegen 2020 een aantal ambitieuze doelstellingen wil waarmaken. Een vlotte interne samenwerking is daarbij noodzakelijk. Daarom krijgt elke afdeling de kans om zich een week lang in de kijker te zetten binnen het bedrijf, en dit in de periode 2016 tot 2018. Zo leren de teams elkaar beter kennen: wie zijn ze, wat doen ze, en wat verwachten ze van de andere afdelingen? Dit alles op een ludieke manier. De jury was onder de indruk van het feit dat de volledige campagne een initiatief is van, voor en door de Nextel-collega's.

www.nextel.be



HIKVISION



H.265+ GROOTSE PRESTATIES

LAGE BANDBREEDTE

Met de H.265+-codec tilt Hikvision video-surveillance naar een ongeëvenaard niveau. Bij Full HD gebruikt H.265+- nog geen 20% van de bandbreedte die H.264 nodig heeft; live streams zijn voortaan standaard van ongekend hoge kwaliteit.

MINIMALE OPSLAG

Ook qua opslag laat H.265+ iedereen ver achter zich. Ongeacht de omgeving of de toepassing reduceert de H.265+ de vereiste opslagruimte met meer dan 80%.

Met H.265+ slaat u dus twee vliegen in één klap. Niet alleen neemt u beelden met een duizelingwekkend hoge resolutie op, maar u minimaliseert bovendien de benodigde opslagcapaciteit. De ideale oplossing voor 24-uurs surveillance!

Hikvision Europe
Dirk Storklaan 3
2132 PX Hoofddorp
The Netherlands
T +31 23 5542770
info.eu@hikvision.com

www.hikvision.com

Hikvision lanceert Access Control oplossing in Europa

Hikvision heeft zijn nieuwe Access Control-oplossing gelanceerd op de Europese markt. Dit biedt klanten een veilige omgeving via beveiligde toegang, met een complete end-to-end oplossing – van camera's tot controllers, van alarm relais naar IP-architectuur, van deursloten naar DVR's. Deze oplossing zorgt voor volledige integratie met de Hikvision-intercom- en intrusion klassen via de iVMS-software. Het geeft klanten ook de mogelijkheid om de producten op afstand te bedienen via de mobiele app Hik-Connect. Met de oplossing kunnen klanten volledige controle hebben over de toegang tot het gebouw, de kamers en gevoelige gebieden. Het geeft hen de mogelijkheid om de aanwezigheid bij te houden, terwijl de activa beschermd worden. Met een breed scala aan opties is de oplossing zeer flexibel. Er zijn bijvoorbeeld meerdere kaartlezerontwerpen beschikbaar. Het biedt multi-door interlock, multi-card, anti-pass back en super card/super wachtwoord functies, en kan tot 100.000 kaarten en 30.000 event records verwerken.

www.hikvision.com/europe



Vereniging Erkende Beveiligingsbedrijven bestaat 30 jaar

De Vereniging Erkende Beveiligingsbedrijven viert feest. De branche-vereniging bestaat 30 jaar en opende op 8 juni in Woerden een nieuw kantoor. Al sinds 6 augustus 1987 behartigt de VEB de belangen van haar leden in de breedste zin van het woord. Met zo'n 600 leden is de vereniging een belangrijke partner binnen de Nederlandse beveiligings-sector. De missie is om veiligheid in Nederland optimaal te waarborgen, onder meer door alle noodzakelijk te nemen maatregelen duidelijk op elkaar af te stemmen. Bij de VEB hebben zich diverse beveiligingsbedrijven met uiteenlopende disciplines aangesloten. De VEB vindt het van groot belang dat particulieren en ondernemers weten wat kwaliteit in beveiliging inhoudt. Daarom wordt een grootschalige promotiecampagne gestart. Daarin wordt het belang benadrukt van aantoonbare betrouwbaarheid, kwaliteitsborging en vakkenis. Door deze vorm van bewustmaking, helpt de vereniging burgers weerbaar te worden en te blijven tegen criminaliteit.

www.veb.nl

Privacycommissie publiceert activiteitenbrochure en digitaal jaarverslag 2016

De Privacycommissie publiceert haar jaarverslag van het voorbije werkingsjaar 2016. De dagelijkse werking werd het voorbij jaar gekenmerkt door de voorbereidende werkzaamheden rond de AVG. Maar er stonden ook stevige adviesdossiers op de agenda over actuele thema's zoals cloudcomputing, de anti-terrorisemaatregelen en de lage emissiezone van de Stad Antwerpen. De overwinning in kortgeding tegen Facebook werd in 2016 in beroep teruggedraaid. Mede door toedoen van de AVG ziet de Privacycommissie het aantal kerndossiers opnieuw stijgen. En het jongerenplatform 'ik beslis' stak haar website in een nieuw kleedje en ging aan de haal met de allereerste M-award van Mediawijs voor haar campagne over het recht op afbeelding.

www.privacycommission.be

Eric Vermaas nieuwe directeur Trigion Brand en Beveiligingstechniek

Erik Vermaas is sinds 5 juni aangesteld als nieuwe directeur van Trigion Brand en Beveiligingstechniek. Daarmee krijgt deze business unit een directeur die vanuit zijn kennis en ervaring zal bijdragen aan de technologische component binnen de integrale propositie van Trigion. Na succesvolle afronding van de opleidingen Electrical Engineering (BSc) en Business Administration (MBA) deed Eric Vermaas ruime ervaring op bij Siemens. In uiteenlopende functies was hij er de afgelopen jaren verantwoordelijk voor het managen en transformeren van diverse bedrijfsonderdelen in de domeinen telecom, brandpreventie, beveiliging en comfort. Deze baggage vormt een ideale basis voor de verdere uitbouw van de integrale propositie waarmee Trigion veiligheid creëert. De organisatie komt met integrale oplossingen waarbij fysieke dienstverlening wordt gecombineerd met techniek en (data) intelligentie, vertrouwde domeinen voor de nieuwe directeur.

www.trigion.nl



Ongeveer **1.25** miljoen mensen sterven elk jaar door verkeersongevallen. Verkeersongevallen zijn de voornaamste reden van overlijden voor jonge mensen, tussen de **15 en 29** jaar. Zonder actie is de voorspelling dat verkeersongevallen zullen stijgen tot de 7e voornaamste doodsoorzaak tegen **2030**.

— Bron World Health Organization

Naast de wereldwijde inspanningen om een veiliger verkeer te verwezenlijken, biedt Dahua een brede reeks oplossingen om verkeersdrama's te voorkomen.

EEN BETERE EN VEILIGERE WERELD

Dahua Intelligent Transportation Solution (ITS)



ANPR

Het opnemen van het voertuig en het herkennen van de kentekenplaat bij de snelheid van 180km/h



Snelheid waarneming

Het waarnemen- en registreren van het voertuig, met bijbehorende classificatie en wegvak door radar en camera te integreren



Rood licht handhaving

Het waarnemen en registreren van de rood licht doorrijder met het volgen van ITS-camera en 3D-radar



Mobiele surveillance

Zorg voor de rijveiligheid en vereenvoudigd het werk van het management omtrent het zenden van voertuigen

CE FC CC UL ISO 9001:2000



DAHUA TECHNOLOGY EUROPE B.V.

Luzernestraat 2
2153GN Nieuw Vennep
Tel: +31 (0)252 745 082
E-mail: sales.benelux@global.dahua.com
www.dahuabenelux.com

License plate Recognition

Face Recognition

Crowd Monitoring

People Counting

Suspect search

Abandoned Object Detection

Loud sound Detection

Heat map

Tracking

CamTech VMS

Maak iedere camera intelligent met CamTech VMS

CamTech VMS is het nieuwe videoplatform van ARAS Security dat meer dan 4.000 camera's van ruim 130 merken slimmer maakt. Elk opgenomen beeld, zelfs van verouderde camera's, is bruikbaar voor geavanceerde analyse van live én opgenomen beelden en tal van geavanceerde mogelijkheden zoals kenteken- en gezichtsherkenning. Qua mogelijkheden, stabiliteit, kracht en gebruiksvriendelijkheid op niveau van menig marktleider, maar dan met eenmalige licentiekosten.

De voordelen van CamTech VMS

- Eenmalige investering in licenties, dus geen verborgen jaarlijkse extra kosten
- Enorme hoeveelheden data worden gefilterd naar één overzichtelijk geheel
- Efficiënt en gebruiksvriendelijk beheer van live- en opgenomen beelden
- Geselecteerde integratie van CamTech NXT en UNV recorders
- Verzekerd van de vertrouwde ARAS ondersteuning



Wilt u een demonstratie?

We komen graag bij u langs met onze demobus en u bent ook van harte welkom in onze showroom.

CamTech VMS is een merk van ARAS Security.

Bezoek www.aras.be of bel **03 825 16 26** voor meer documentatie en informatie over CamTech VMS.



Axis en HID Global presenteren de eerste geïntegreerde open IP-oplossing voor mobiele toegangscontrole

Axis Communications kondigt de integratie aan van Mobile Access van HID Global in de AXIS A1001-netwerkdeurcontroller- en AXIS Entry Manager-software. De gecombineerde, mobiele toegangsooplossing van Axis en HID speelt in op de toegenomen mobiliteit van werknemers. Zo zorgt de oplossing ervoor dat mobiele apparaten, zoals smartphones, kunnen fungeren als vervanging van kaarten en/of toegangscode voor beveiligde gebouwen, kamers of gebieden. Smartphones en andere mobiele apparaten worden steeds belangrijker voor veel mensen naarmate ze meer functionaliteit krijgen, zoals contactloos betalen of het bijhouden van de gezondheid. Dankzij de integratie van Mobile Access van HID Global in de software en deurcontrollers van Axis, is er een oplossing die de eenvoud van de mobiele wereld combineert met het beveiligingsniveau dat bedrijven en hun medewerkers verwachten.

www.axis.com



Securitas klaar om nieuwe wet op de Private Veiligheid toe te passen

Securitas reageert positief op de definitieve goedkeuring van de nieuwe wet op de Private Veiligheid, onlangs in het Federaal Parlement. "De nieuwe wet toont aan hoe de private veiligheidssector is uitgegroeid tot een professionele partner van de politie en veiligheidsdiensten, mede door onze technologische kennis. De wet is dan ook een belangrijke hefboom om samen te werken aan een integraal veiligheidslandschap", benadrukt Securitas-woordvoerder Koen Colpaert. De vorige wet (Wet Tobback) op de Private en Bijzondere Veiligheid bestond bijna 30 jaar en kende in die periode verschillende wijzigingen, maar was intussen achterhaald en niet mee-geëvolueerd met de veranderingen in de sector. Het proces om de nieuwe wetgeving in lijn te brengen met de mogelijkheden en capaciteiten van de private veiligheidssector, is de voorbije jaren in een stroomversnelling gekomen. Securitas is tevreden over de manier waarop de wetgeving werd aangepast. "Samen met alle veiligheidsactoren in de samenleving (politie, brandweer, burgemeesters, provinciegouverneurs, burgers, ...) streven we zo naar de best mogelijke samenwerking."

www.securitas.be



INTERNATIONAL TRADE FAIR
WITH CONGRESS

- SAFETY
- SECURITY
- HEALTH AT WORK

17 - 20 OCTOBER 2017
DÜSSELDORF, GERMANY

PEOPLE
MATTER.

DE UITDAGINGEN WORDEN NIET MINDER MAAR WORDEN ANDERS.

de arbeidsomstandigheden veranderen. Niemand weet dit beter dan de werkende mens: digitalisering, nieuwe technologieën, stijgende flexibiliteit en toegenomen werkdruk. Bereidt u voor op nieuwe uitdagingen: met de nummer 1 vakbeurs en rond 1900 exposanten vanuit de hele wereld.

www.AplusA-online.com

Voor meer informatie:
Fairwise BVBA
Hubert Frère-Orbanlaan 213 _ B-9000 Gent
T: 09 245 01 68 _ F: 09 245 01 69
info@fairwise.be





De effecten van de aanslagen: bewakingssector groeit met 9,7% in 2016

De Beroepsvereniging van Bewakingsondernemingen (BVBO) groeide in 2016 met 9,7% ten opzichte van 2015. Dat is het gevolg van de aanslagen in Frankrijk en Brussel, eind 2015 en in 2016. De operationele winst daalde licht, naar 3,4% op de omzet tegenover 3,5% in 2015. Er was een bijkomende vraag naar bewaking van goederen en naar persoonscontrole. Anderzijds deden de banken minder beroep op de bewakingsfirma's. Het aantal personeelsleden van de bewakingsfirma's steeg met 10,2% of 1.297 voltijdse jobs (FTE). Opvallend is dat 31,1% van de in 2016 tewerkgestelde mensen 45+ was. De bewakingssector is effectief een belangrijke aanwerver van 45+'ers, waaronder heel wat laaggeschoolden. Ten slotte investeerde de sector actief in nieuwe technologie waardoor ze mensen gericht kunnen inzetten.

2016 is het jaar waarin de activiteiten van de bewakingsfirma's op veel bredere basis gerespecteerd werden en de sector als volwaardige partner erkend werd door de verschillende partijen in de veiligheidsketen. "We hebben ons vorig jaar snel aangepast aan de gewijzigde markt- en veiligheidsomstandigheden", licht Danny Vandormael (voorzitter BVBO) toe. "Onze agenten hebben zich zeer flexibel ingezet. We hebben overtuigd door ons professionalisme en we hebben goed samengewerkt

met de publieke veiligheidsdiensten. Ons imago kreeg een mooie boost. Daar zijn we blij mee want we hebben de voorbije jaren enorm geïnvesteerd in materialen en opleiding. Onze bewakingsagenten zijn trouwens de best gescreende in Europa".

Omzet + 9,7%, winst lager dan in 2015

De sector kende met een omzet van 726,6 M€ zoals verwacht een mooie omzetgroei in 2016: +9,7% in vergelijking met de 662 M€ omzet van 2015. Het bedrijfsresultaat

evolueerde iets minder dan proportioneel in dezelfde richting en bedroeg +3,4% op de omzet – tegenover 3,5% op de omzet in 2015.

In 2016 gaven de opleidingsinstellingen van de BVBO-leden maar liefst 656.054 lesuren opleiding, of 13,7% meer dan in 2015. Dat komt op jaarbasis neer op 374,9 FTE's of 2,6% van het totale personeelsbestand. Dit is het gevolg van de plotse pieken in de vraag naar bewakingsdiensten na de aanslagen.

"De onverwachte piek van de vraag na 22 maart, bracht meer dan proportionele kosten met zich mee", stelt Vandormael. "Je moet extra inzetten op aanwervingen, mensen opleiden, materiaal bijkopen, onregelmatige en extra werkuren kosten meer, en ga zo maar door. Daarom is de winst minder dan proportioneel geëvolueerd. In het najaar van 2016 nam de vraag, ondanks het aanhoudende dreigingsniveau 3, terug af. Wellicht trad er een zekere gewenning op aan het dreigingsniveau, dat nochtans nog altijd op 3 staat", besluit Vandormael.

Met de tijdelijke inzet van bijkomend bewakingspersoneel, wilden organisaties de mensen duidelijk door 'zichtbare' maatregelen een veiliger gevoel geven. Op langere termijn is een meer structurele aanpak opportuun, zoals extra bewakingsmensen in combinatie met meer middelen en technologie. BVBO stimuleert haar leden om volop te gaan voor nieuwe, innovatieve technologie en dit in combinatie met bewakingsmensen aan te bieden. Een voorbeeld van zo'n nieuw aanbod is de terbeschikkingstelling van drones met operatoren, bijvoorbeeld voor sportmanifestaties.

Ongelijke stijging in de sectoren

Het aantal klanten steeg licht. Het waren vooral de bestaande klanten die meer diensten afnamen. De gemiddelde omzet per klant bedroeg 51.478€ in 2016 tegenover 48.076€ in 2015. Met name de vraag in de transportsector steeg significant. Er werden maar liefst 43,8% meer diensten geleverd aan luchthavens, zeehavens en treinstations. Deze sector is nu de derde grootste afnemer van de BVBO-leden, na overheidsorganisaties en de industrie in het algemeen, met 16% van de totale omzet. Hun vraag steeg in reactie op de aanslagen in Frankrijk en Brussel.

De banken namen 1,1% minder diensten af, door de verdere daling van het aantal klassieke bankkantoren en de vermindering van de geldtransporten. Het aandeel van de banken in de omzet van de leden van BVBO daalde daarmee van 12,4% in 2015 naar 11,2% in 2016. Ze zijn nu de vierde belangrijkste sector voor de BVBO-leden.

Een andere belangrijke sector is de distributie (groothandel). De vraag in deze sector steeg met 8,7%, tot 9,8% van de omzet in de sector. Opmerkelijk is dat de vraag naar

bewakingsdiensten op evenementen met 30,8% steeg, tot 1,8% van de totale omzet. Qua activiteiten kwam het gros van de omzet uit goederenbewaking (68,6%). Op de tweede plaats komt de bewaking en controle van personen (18,5%). Dit is het toezicht op het gedrag van personen, bijvoorbeeld de toegang tot een plaats. Geldtransporten komen met 11,6% op de derde plaats.

Naast het feit dat men heel wat mensen bijkomend heeft aangeworven, investeert de bewakingssector ook actief in nieuwe technologie waardoor personen gericht kunnen worden ingezet.

De sector zet actief in op innovatieve technologie in combinatie met mensen. Naast het feit dat men heel wat mensen bijkomend heeft aangeworven, investeert de bewakingssector ook actief in nieuwe technologie waardoor personen gericht kunnen worden ingezet.

Een voorbeeld van zo'n toepassing is technologie waarbij men met operators vanop afstand kan werken via camera's om bijvoorbeeld winkeldiefstal te zien en de bewakingsagent in de winkel naar de dief te leiden, eerder dan dat winkelinspecteurs (bewakingsagenten) fysiek in voldoende mate moeten aanwezig zijn om het gedrag van (alle) klanten zelf te observeren. Een ander voorbeeld hiervan is het maken van virtuele bewakingsrondes via camera's door operatoren in meldkamers, of nog het openen en sluiten van deuren en het in- en uitschakelen van alarmsystemen vanop afstand.

Een andere toepassing is het gebruik van X-ray om de tassen van bezoekers te screenen. Tot voor kort werd deze technologie enkel op de luchthaven gebruikt. Vandaag wordt ze meer en meer ingezet, bijvoorbeeld in rechtbanken. De bewakingssector levert hiervoor de totaaloplossing, inclusief technologie en mensen.

Actief op zoek naar 50+'ers

De bewakingssector is een mensgedreven sector. Er kwamen bij de leden van BVBO dan ook maar liefst 1.297 FTE's bij, of

10,2%, in 2016. Van de totale tewerkstelling in 2016 waren er 16,8% medewerkers in de leeftijdscategorie 18-25; 52% tussen 26 en 45; en 31,1% ouder dan 45. Als we er van uitgaan dat de leden van BVBO goed zijn voor meer dan 90% van de tewerkstelling in de sector, wil dat zeggen dat er in de hele bewakingssector minstens 1.441 FTE's zijn bijgekomen.

"We gaan actief op zoek naar 45+'ers en 50+'ers, die we in combinatie met jongere mensen inzetten", aldus Vandormael. "Het is altijd de bedoeling om mensen die snel zijn en goed in de fysieke actie in te zetten samen met mensen die wat bezadiger zijn. We streven naar een goed evenwicht tussen de leeftijdsgroepen en tussen snelheid en maturiteit. 50+'ers die omwille van bijvoorbeeld fysieke klachten hun beroep niet meer verder kunnen uitoefenen, krijgen zo bij ons een tweede carrièrekans."

83% van de tewerkgestelden had enkel een diploma middelbaar. 10,1% had zelfs enkel een diploma lager onderwijs. Er is een lichte stijging van het aantal tewerkgestelden met minstens een diploma middelbaar onderwijs (89,9%) ten opzichte van de tewerkgestelden met enkel een diploma lager onderwijs. 15,3% van de tewerkgestelden bij de BVBO-leden in 2016 waren vrouwen, dat was 0,3% meer dan het jaar ervoor.

📞 www.apeg-bvbo.be



Danny Vandormael (voorzitter BVBO): "We hebben overtuigd door ons professionalisme en we hebben goed samengewerkt met de publieke veiligheidsdiensten. Ons imago kreeg een mooie boost."



OVLD, waarom hou je de vergunning van de slotenmaker tegen?

Het mysterie van Open VLD: waarom ze de burger niet tegen oplichters-slotenmakers wil beschermen door in de Wet Private Veiligheid een vergunning op te nemen. Chapeau aan het Meldpunt Malafide Slotenmakers dat een schriftelijk standpunt kreeg... een uur na de definitieve goedkeuring van de wet (Mail van Diederik Pauwelyn (Inhoudelijke coördinatie, Operationeel management van Open VLD) van 8 juni 2017, terug te vinden op de Facebook-pagina van het meldpunt.)

Op 8 juni werd de nieuwe wet inderdaad goedgekeurd zonder deze vergunning. CD&V had haar wetsvoorstel hiervoor een stille dood laten sterven in de Commissie Binnenlandse Zaken. Zelfs een ultiem amendement waarmee de oppositiepartijen sp.a, PS en cdH, met steun van de volledige oppositie, het CD&V voorstel weer opvisten, werd genadeloos weggestemd door de regeringspartijen, CD&V inclusief. Open VLD haalde met haar argumenten haar slag thuis. Wat stellen die voor? Nog maar een jaar geleden pleitte een kamerlid van CD&V met veel overtuiging voor ons project, en diende hij zelfs een wetsvoorstel in. Door ziekte tijdens de cruciale commissievergaderingen kon hij zijn voorstel niet verdedigen, maar ondanks de bevestiging dat de collega's het nodige zouden doen, verloren zij toch het voorstel uit het oog, en lieten het vervallen. Vorige

donderdag stemde zijn hele CD&V-fractie in de plenaire vergadering van het parlement gewoon *tegen* de amendementen die zijn tekst weer voorstelden. Waarom stemden naast CD&V ook N-VA en MR tegen? Zij hadden toch ook niets tegen ons voorstel? Simpel: Open VLD, ook lid van de regering, verzette zich tegen een vergunning voor de slotenmakers. Natuurlijk kan de regering het voorstel dan niet indienen, maar de regeringspartijen hadden overeengekomen dat hier dan maar het parlement de kwestie moest oplossen. Dan is het niet normaal dat alle regeringspartijen – ook zij die ons eerst steunden – ook daar de zaak kelderden, en elke discussie afblokken. Laten we daarom eens kijken naar de motivatie van Open VLD. Als dit de enige motivatie is waarom de regering onze vergunning afwees, moet ze wel nagels met koppen slaan.

1) “Malafide slotenmakers zorgen voor veiligheidsrisico's en voor oneerlijke concurrentie”, zegt Open VLD.

Vreemd dat Open VLD dit ter sprake brengt, want geen van beide redenen doen er echt toe. De oplichters zorgen niet echt voor veiligheidsrisico's. Deze risico's zijn wel een reden om de vergunning als slotenmaker in te voeren, waarmee confidentialiteit beter verzekerd kan worden. Er is ook geen oneerlijke concurrentie omdat de malafide slotenmakers niet dezelfde regels volgen, want er zijn gewoon geen regels voor slotenmakers. En als er regels zouden zijn, zouden deze oplichters er zich gewoon niet aan houden als er geen controle is. Open VLD wil hier blijkbaar de aandacht verleggen naar problemen waar zij beweert een oplossing voor te hebben. Maar de olifant in de kamer wil Open VLD niet zien:

de criminele oplichting waar mensen via specifieke websites naar dit soort uitbuiters gelooft worden. Daar moet wat aan gedaan worden, en dat kan enkel effectief met een vergunningsplicht, die gecontroleerd en gesanctioneerd wordt, en die ook deze websites als tussenpersonen aanpakt.

2) “Ja maar, een vergunningsplicht brengt lasten mee: startpremie, retributies,...”, zegt Open VLD.

Vreemd argument, dat geen probleem is voor installateurs van alarmsystemen, van camerabewaking, of voor de vele grote en kleine bewakingsondernemingen, interne bewakingsdiensten en veiligheidsadviseurs. Om en bij de 2.000 bedrijven die samen ruim 20.000 werknemers tewerkstellen!

Met de startpremie bedoelt men de eenmalige dossierkost (bij alarminstallateurs 1.000 euro), met de retributies de jaarlijkse vergoeding die een vergund bedrijf moet betalen (500 euro vast per vergunning, plus 135 euro per werknemer). Maar voor de veiligheidsscreening die Open VLD voorstelt moet er elke vijf jaar ook een retributie betaald worden, die tot 250 euro oploopt (en die al jaren niet meer aangepast is). Niets verhindert trouwens dat de regering deze kosten aanpast aan de draagkracht van de bedrijven. Andere lasten die niet ter sprake komen, zijn juist noodzakelijk. Het is echt geen luxe dat slotenmakers hun klantendossiers, sleutels en duplicaten beveiligd en geanonimiseerd te bewaren. Lasten als het vermelden van het vergunningsnummer op alle stukken en op het voertuig horen ook gewoon bij een vergunde activiteit. Dat Open VLD dergelijke lasten te berde brengt, is bovendien verwonderlijk, omdat het zelf een zwaardere en veel tijd vergende veiligheidsscreening wil invoeren voor de slotenmaker. Wat is werkelijk de bedoeling van Open VLD?

3) “We riskeren op een hellend vlak te komen na de opname in de wet, waarbij men gaat vragen om identiteitscontroles, wapens, bijstand van de politie”, zegt Open VLD.

Mooi hoe Open VLD hier het risico van het hellend vlak, dat de partij bij elke uitbreiding van de taken van de bewakingssector zelf als een duivel in een wijvatervat moet ontkrachten, recycleert. Slotenmakers vragen wat nodig is, niet meer. In ons voorstel

maakten we er geen geheim van dat slotenmakers om goede redenen eindelijk *moeten* toegelaten – en verplicht – worden de identiteit en toegangsrechten te controleren van wie hen om een noodopening van een deur vraagt. Anders blijven ze de deur openen voor dieven, ex-partners of stalkers. Politiebijstand is enkel nodig in gevallen waar er van risico sprake is, en wapens zijn al helemaal niet aan de orde.

4) “Er kunnen nog ongewenste neveneffecten zijn bijvoorbeeld in het geval van deurinstallateurs”, zegt OVLD.

Tja, dat werd precies uitgesloten in ons voorstel. Daarin werd voorzien dat schrijnwerkers of plaatsers van deuren (zoals iedereen) altijd gewoon sluitwerk kunnen plaatsen. En elke fabrikant of schrijnwerker die een deur of raam maakt, kan zijn producten met reeds geplaatst veiligheidssluitwerk leveren, zoals vandaag vaak gebeurt. Open VLD brengt dus geen enkel argument aan dat aan enige kritiek weerstaat.

Welk alternatief stelt Open VLD voor?

Open VLD wil “de wet op de veiligheidsscreenings uitbreiden naar de slotenmakers”. Zoals gezegd zijn deze zwaarder dan de controles in de Wet Private Veiligheid, terwijl er toch niet gekeken wordt naar de vakkennis of het naleven van correcte handelspraktijken. Die wet bepaalt echter ook niet wanneer screenings verplicht worden. Er is dus in elk geval nog bijkomende wetgeving nodig. Die wetgeving zou tenslotte ook nog moeten voorzien hoe de naleving van de screeningsplicht gebeurt, en hoe niet-naleving gesanctioneerd wordt. Open VLD veronderstelt toch niet dat het bejaarde koppel dat met de oplichters te maken kreeg en 865 euro moest betalen, deze kerels naar hun screening zou vragen, om ze vervolgens aan de politie uit te leveren? Controle vraagt controlemechanismen, en of men nu wil of niet, die zijn het makkelijkst te creëren in een bestaande context, waar controle en sancties al bestaan. In de Wet Private Veiligheid is dit systeem volledig uitgebouwd en operationeel. Maar het voordeel van deze veiligheidsscreening is natuurlijk dat het juist niet om een *vergunning* gaat. Daar was het Open VLD blijkbaar om te doen. Daarom wilde Open VLD nooit

haar motivatie geven (tenzij een uur na de definitieve goedkeuring van de wet), en was ze ook nooit bereid om alternatieven te bespreken. ‘Open’ is wat anders.

De werkelijke motivatie van Open VLD

Dat een regeringspartij met zo'n zwakke argumentatie erin slaagt de andere hun principes en standpunten te doen vergeten, doet wel vragen rijzen. Open VLD had inderdaad andere belangen te verdedigen, voor wie het slecht zou uitkomen dat men voor slotenmakerswerk vergund moet zijn. Wanneer een deurwaarder een deur moet laten openen, uiteraard door een slotenmaker, moet een politieagent erop toezien dat alles correct verloopt. Open VLD pleit er al jaren voor dat bewakingsagenten hier de politieagent mogen vervangen. Nu moet men weten dat het de politieagent is die in principe de slotenmaker kiest. Echter, eens de bewakingsagent er staat, zal die proberen de deuropening zelf te doen. De nieuwe Wet Private Veiligheid laat dat voortaan toe, voor zover... *er voor dat werk geen vergunning gehaald moet worden*. Anders gesteld: wanneer er wel een vergunning nodig is voor slotenmakerswerk, kunnen bewakingsagenten hun werk niet overnemen. Eens bewakingsagenten wél kunnen optreden in plaats van de politieagenten, verliezen de slotenmakers werk aan mensen zonder vakkennis. Door die ingreep staan er uiteindelijk 100 jobs in onze sector op de tocht.

Epiloog

Het is onbegrijpelijk dat een open liberale partij dergelijke politiek voert, laat staan dat de andere regeringspartijen haar daarin helpen. Voor de slotenmaker eindigt het verhaal hier dan ook niet. De vergunning is noodzakelijk, nu meer dan ooit.

Geert Herbots

Juridisch adviseur VSU en FNS

www.vsu.be

www.serrurier.be



**Vlaamse
Slotenmakers
Unie**





ALARM INDUSTRIES ASSOCIATION

Distributeurs, invoerders en fabrikanten, aangesloten bij ALIA staan u steeds ter beschikking voor studies en leveringen van alarmmateriaal, CCTV en toegangscontrole.

Installateurs van beveiligingssystemen kunnen bij de distributeurs van alarmmateriaal, die lid zijn van ALIA, rekenen op een uitstekende dienstverlening: herstellingen, leveringen, nieuwe producten, opleiding en documentatie.

Neem gerust met hen contact op.

ADI Global Distribution NV / SA
 Helststraat 150 • 2630 Aartselaar
 (T) 03 877 30 30 • (F) 03 877 31 28
 Excelsiorlaan 4A, 1930 Zaventem
 (T) 02 482 08 50 • (F) 02 465 78 56
 info.be@adiglobal.com
 www.adiglobal.com/be

TEL: 071/85 13 13 • FAX: 071/85 31 52
 e-mail: info@ais-security.be
 http://www.ais-security.be

Manufacture & Distribution
 Intrusion - CCTV - IP Solutions
 Access Control - Fire
 Structured Wiring - Domotics
 Integrated Systems - Home Anywhere
 Rue de l'Abbaye, 89 4040 Herstal
 Tel : 04/229.37.97 Fax : 04/229.50.94
 Email : info@anb-sa.be Web : www.anb-rimex.be

ISO 9001
 Da Vinci Science Park
 Av. de Bâle 7
 1140 BRUXELLES
 TEL: 02/726 99 10 • FAX: 02/726 56 12
 e-mail: mail@euromatec.be
 http://www.euromatec.be

DISTRIBUTEURS EN FABRIKANTEN TOT UW DIENST

> protection garantie
France Nizet Distribution
 Rue de la Paix, 7 | B-4671 Barchon
 Tél. +32 (0)4 370 12 13 | Fax +32 (0)4 370 11 60
 fnd@fnd-distribution.com | www.fnd-distribution.com

We make it work.
 Vliegveld 37
 8560 Wevelgem
 T: +32 (0)56 78 20 20
 F: +32 (0)56 78 20 21
 E: info@lobeco.be
 www.lobeco.be

Kouterveldstraat 2
 1831 Diegem
 T: +32 2 715 8930
 F: +32 2 725 2061
 E-mail: sales.belgium@fs.utc.com

Kantoren:
 Brugsesteenweg 257
 8500 Kortrijk
 T: +32 (0)56 36 37 40
 F: +32 (0)56 36 08 12
 E-mail: ras.contact@rassecurity.com

RISCO Group Benelux SA/NV
 Drogenbos Techno Center
 Boulevard de l'Humanité 233
 B-1620 Drogenbos - Belgium
 Phone: +32 (0)2 522 76 22 - Fax: +32 (0)2 524 49 29
 www.riscogroup.com

Paepsem Business Park
 Boulevard Paepsem 18B, 1070 Bruxelles
 TEL: +32 (0)2 380 97 97 / FAX: +32 (0)2 380 68 47
 e-mail: sabelco@sabelco.com
 www.sabelco.com

Milestone NV/SA
 Herengracht 25A
 2000 Antwerpen, Belgium
 T: +32 (0)3 238 99 00
 www.milestone.com

Manufactured with European
 Components (VIA, VLSI, etc.)
 1070 Brussels
 info@idis.com
 www.idisglobal.com



Olivier Demoulin (53, CEO van ETAC Alarme Service): "In de toekomst zullen we geen hardware meer verkopen maar een product as a service. Dit zal de manier waarop de verkoper tewerk moet gaan veranderen."

"Ons beroep zal de komende vijf jaar volledig veranderen"

Olivier Demoulin – Nieuwe voorzitter ALIA Security

Roger De Grave gaf onlangs na drie jaar voorzitterschap van ALIA Security de fakkel door aan Olivier Demoulin (53, CEO van ETAC Alarme Service). De nieuwe voorzitter benadrukt dat het beroep de komende vijf jaar volledig zal veranderen. Kwaliteit zal meer dan ooit het sleutelwoord zijn om de uitdagingen het hoofd te bieden. Een gesprek over opportuniteiten en bedreigingen. En over de rol van de beroepsvereniging.

Olivier Demoulin staat aan het roer van ETAC Alarme Service, een onderneming sinds 1949 actief in de sector en lid van de Connex Group, leader op de markt van elektronische beveiliging. Het bedrijf is gespecialiseerd in het ontwerp, de installatie, het onderhoud en de after-sales service van elektronische beveiligingssystemen (inbraak-en branddetectie, camerabewaking, toegangscontrole enz.) Tot nu toe werden meer dan 15.000 installaties gerealiseerd in alle marktsegmenten (particulieren, bedrijven, instellingen ...) en regio's van het land. De onderneming stelt een vijftigtal bedienden te werk waaronder een dertigtal gespecialiseerde technici. Het bedrijf beschikt over het ISO 9001-2015 certificaat, is Belgisch Hofleverancier en realiseerde in 2016 een omzet van 7.700.000,00 euro. Olivier Demoulin is reeds meer dan twintig jaar geëngageerd in het verenigingsleven. De laatste jaren is hij lid van het directiecomité van INCERT en van diverse comités binnen ALIA Security, waar zijn technisch en strategisch inzicht in het bijzonder gewaardeerd worden. Vanwaar zijn engagement? "Ik vind het heel belangrijk om de belangen van de kleinere KMO's te verdedigen en de contacten met de diverse stakeholders, zoals bijvoorbeeld de FOD Binnenlandse zaken, de verzekeringsmaatschappijen of de controleorganismen, goed te onderhouden. Een beroepsvereniging helpt bij het uitbouwen

van een netwerk en is een manier om op de hoogte te blijven van het reilen en zeilen binnen de sector. We zijn momenteel binnen dat kader bezig met een inhoudelijke herziening van onze website."

"Veel kleinere KMO's hebben te weinig tijd om zich bezig te houden met strategisch denken. Hierin ligt een rol voor de beroepsvereniging weggelegd."

Strategisch denken

België telt ongeveer 950 erkende beveiligingsondernemingen, waarvan er circa 350 INCERT-gecertificeerd zijn. Olivier Demoulin: "Zeker de helft van onze leden is gecertificeerd. Net als mijn voorganger Roger De Grave wil ik volop inzetten op kwaliteit. Ons beroep zal de volgende vijf jaar volledig veranderen. Installateurs zijn zich hier niet altijd bewust van. Veel kleinere KMO's hebben te weinig tijd om zich bezig te houden met strategisch denken. Hier ligt een rol voor de beroepsvereniging weggelegd. Ik zie momenteel diverse bewegingen. Zo is er de trend 'Provider to consumer'. Fabrikanten stellen hun oplossingen alsmaar vaker rechtstreeks aan de eindklant voor. Dit kan een gevaar betekenen voor zowel de distributeurs als voor de installateurs. Daarnaast is er het

hele e-commerce gebeuren. Andere uitdagingen zijn het Internet of Things (IoT) en hoe ermee om te gaan, de App's voor smartphone, de dematerialisatie van de beheersystemen... . We zullen in de toekomst minder hardware verkopen maar producten as a service. Dit zal de manier waarop de verkoper tewerk moet gaan veranderen. Daarbovenop zijn er ook de juridische aspecten. De sector is zich nog niet voldoende bewust van al deze uitdagingen. Ze kunnen een opportuniteit maar ook een bedreiging zijn. We maken er dan ook een punt van om de bedrijven hierover te informeren via infomeetings en workshops. Opleiding van ons personeel staat eveneens hoog op de agenda. We zoeken meer en meer technici die IT-competenties hebben en daar moet in geïnvesteerd worden. Op dat vlak willen we onze goede contacten met de kabinetten en opleidingscentra verder uitdiepen."

Nieuwe certificatie INCERT Video

ALIA Security organiseerde in juni twee infosessies inzake de nieuwe certificatie INCERT Video, die nu ook beschikbaar is voor professionals van beveiliging. De beroepsvereniging is ervan overtuigd dat de certificatie zeer belangrijk is omdat ze een referentieel kader opvult dat vandaag leeg is. Olivier Demoulin: "We zijn er reeds meer dan vier jaar mee bezig. Camerabewaking is in volle evolutie. Er zijn echter een

groot aantal spelers op de markt waarvan de installatie van camera's niet de belangrijkste activiteit is. Ik denk bijvoorbeeld aan informaticabedrijven. Sommige oplossingen lijken misschien aantrekkelijk op financieel vlak, maar het eindresultaat is niet conform de verwachtingen van de klanten. We raden dan ook professionele installateurs aan hun bedrijf te laten certificeren. Net zoals de certificatie voor inbraak is INCERT Video een uitstekend kwaliteitslabel, dat meer en meer zal worden gevraagd. We merken een ruime interesse op de infoavonden, waarop we 150 inschrijvingen telden. Ons doel is dat er tegen eind dit jaar een dertigtal 'early adopters' ondernemingen gecertificeerd zullen zijn. We zijn er ons bewust van dat camera's alle segmenten van ons beroep

zullen beïnvloeden. Ik denk aan onder meer brand- en toegangscontrole."

Nieuwe Wet private veiligheid

De Nieuwe wet private veiligheid werd op 8 juni goedgekeurd en vervangt de wet Toback. Olivier Demoulin: "We blikken terug op een heel goede samenwerking met de kabinetten en zijn zeer tevreden over de nieuwe wet. Zo is er het behoud van de onderaanneming van het deel bewaking, waardoor bedrijven die geen erkenning hebben voor bewaking deze dienst toch in onderaanneming kunnen blijven aanbieden aan hun klanten. We zijn ook blij met de nieuwe verplichte camera erkenning en zijn verheugd dat er nu een verbod is op deur-aan-deur verkoop van alarmsystemen."

ALIA Security ontmoette op 18 april de inspecteurs van de FOD Binnenlandse Zaken. Het ministerie heeft 25 inspecteurs geëngageerd om te controleren. Diverse punten werden aangehaald in een constructieve dialoog: multolerantie voor bedrijven die niet erkend zijn, alsook de context en problematieken van de sector. Olivier Demoulin: "We hebben de inspecteurs over de specificaties van ons sector geïnformeerd en hen de boodschap gegeven dat het belangrijk is dat er slagkracht is, maar ook begrip voor de realiteit van de sector."

Door Tilly Baekelandt

www.aliasecurity.be

ALIA Security

ALIA Security is de Belgische beroepsvereniging van de elektronische beveiliging. Ze vertegenwoordigt de installateurs, fabrikanten en distributeurs inzake inbraakdetectie, branddetectie, toegangscontrole en camerabewaking.

De leden van één van de installateursverenigingen ELOYA, FEDELEC of NELECTRA en de leden van FEE, de vereniging van fabrikanten, importeurs en verdelers van elektronische beveiliging, zijn automatisch lid van ALIA Security.

ALIA telt ongeveer 600 leden, die in aantal twee derde van de erkende beveiligingsondernemingen vormen, en vertegenwoordigt circa 80% van de totale omzet op de markt.

AFIDIS wordt FEE Security

AFIDIS en FEE beslisten eind vorig jaar om de krachten te bundelen en samen te smelten. Op 14 april werd FEE officieel lid van de raad van bestuur van ALIA en werd AFIDIS als vereniging opgedoekt. Eric Piers werd aangesteld als directeur van FEE. Ex-AFIDIS-leden kunnen vanaf nu deel uitmaken van FEE Security, een afdeling die speciaal werd opgericht naar aanleiding van de herstructurering en die de belangen van distributeurs en fabrikanten zal vertegenwoordigen binnen ALIA. Christophe Depuydt (CEO RAS) wordt het aanspreekpunt van FEE Security. Hij volgde ook in het verleden de ALIA-dossiers op voor de distributeurs en fabrikanten.

Welverdiend pensioen Yves Ryckaert

Olivier Demoulin staat er nog op Yves Ryckaert namens ALIA Security te bedanken en hem een welverdiend pensioen toe te wensen. Na meer dan 25 jaar actieve inzet binnen ALIA, besliste Yves Ryckaert om de organisatie te verlaten. Doorheen de jaren heeft hij de belangen van ALIA steeds met overtuiging weten te verdedigen. Hij stond niet alleen aan het ontstaan van de beroepsvereniging en is niet enkel voorzitter geweest, maar heeft vooral een cruciale rol gespeeld in de besprekingen rond het wettelijke kader en het opkomen voor de belangen van de vele KMO's die de sector telt.



Groei mee, met de nieuwste generatie op ip!



- Exclusief verkrijgbaar bij: -

Top Security B.V. | Middelste Groes 10 | 5384 VV Heesch |
Tel. +31 412-475788 | www.topsecurity.nl | info@topsecurity.nl |





tel. +32 9 372 92 88
sales@mce-ups.com

secure your powerbusiness

Een UPS maakt uw alarminstallatie 100% veilig

MCE is uw leverancier voor UPS-systemen, batterijen en batterijladers. Wij bieden klantgerichte oplossingen voor alle problemen in geval van stroomuitval, spanningsvariaties, blikseminslag, ... Daarnaast beschikken wij over een uitgebreid gamma van gelijkstroomvoedingen en transformatoren, geschikt voor alle automatiseringsprocessen in productie en machinebouw.

Voor meer informatie over onze producten, bezoek onze website www.mce-ups.com of contacteer ons via e-mail: sales@mce-ups.com



salicru



Tel.: + 32 (0)9 372 92 88 • Fax: + 32 (0)9 372 74 42 • E-mail: sales@mce-ups.com
MCE nv • Buntstraat 55A • 9940 Evergem • Belgium

www.mce-ups.com



DE TOEGEVOEGDE WAARDE



- Integratie met Home Anywhere - BiBus - MiniDo
- 100% compatibel met Dahua

NEW!!!

IVS (Intelligent Video Systems)



PRODUCT OF 

Voor meer informatie: www.anb-rimex.be

Dynamische securityplanning volgens gezond boerenverstand

Elke security manager krijgt ermee te kampen, de sectorgebonden 'Directives' die, om concurrentieel te blijven, het best asap worden geïmplementeerd binnen de bedrijfsprocessen. Enkele voorbeelden hiervan – naast de ISO-kwaliteitsnormen en de wettelijke veiligheidsvereisten – zijn: de TAPA¹-reglementering voor de opslagmagazijnen, de FSR²-bepalingen voor de logistiek, de ISPS³ Code voor de havenfaciliteiten, de AEO⁴-richtlijnen voor de internationale handel, de LME⁵-standaard voor de industriële metaalverhandeling en het INCERT⁶-label voor inbraakgevoelige bedrijven. En morgen komt er stevast een extra 'spelregel' uw richting uit...

Dynamisch anticiperen

Doordat de restricties en de vereisten van een volgend te behalen certificaat niet altijd evident zijn, ziet de security manager zich genoodzaakt om er een veiligheidsconsulent bij te halen. Deze specialist ter zake zal helpen om het bedrijf in regel te stellen naar de nieuwe normering. Echter, aangezien een goed securityplan altijd een momentopname is, en dus empirisch wordt bijgestuurd, zijn er misschien maar enkele extra maatregelen nodig om de auditor tevreden te stellen.

Hands-on risico controle

Een goede insteek om het securityplan up-to-date te houden is door de nieuwe bedrijfsrisico's in kaart te brengen. De creativiteit én de middelen van agressoren evolueren immers met de technologie, waardoor het aangewezen is om het securityplan 'continu' bij te sturen. Door de actuele berichtgeving van veiligheidsincidenten en van ongekende (ingenieuze) inbraachtechnieken op te volgen, kan al veel onheil worden voorkomen. Dit echter op voorwaarde dat tegenover elk extra risico of elke nieuwe 'Directive' een afdoende oplossing in het 'oude' securityplan wordt voorzien.

Risico-identificatie en -evaluatie

Startpunt bij de risico-identificatie is om eerst goed na te denken over de vraag: 'Wat/wie moet worden beveiligd tegen wat/wie?' Na het oplijsten van de risico's dienen deze in volgorde van belangrijkheid te worden geordend. Brandgevaar is bijvoorbeeld belangrijker dan het risico dat een vliegtuig neerstort op de bedrijfsgebouwen. Beide risico's bestaan, en misschien zou-

den ze evenveel schade berokkenen, maar de kans dat er brand ontstaat is natuurlijk veel groter.

Kwantificeren van de risico's

Om risico's in te delen hebben academici en specialisten tal van technieken ontwikkeld. De meest gekende zijn de Methode van KINNEY en de HAAGSE Methodiek. In grote lijnen komt het erop neer dat de grootte van een risico wordt bepaald door drie hoofdfactoren. Deze zijn: (1) de waarschijnlijkheid van voorkomen (probability), (2) de blootstelling aan het risico (exposure), en (3) de ernst (severity) of de schade indien het risico effectief zou plaatsvinden.

Een goede insteek om het securityplan up-to-date te houden is door de nieuwe bedrijfsrisico's in kaart te brengen.

Risico = Impact x Kans

Een goede risico-inschatting, een vuistregel als het ware, is om het verwachte verlies (Impact) en de frequentie (Kans) van het risico met elkaar te vermenigvuldigen. De uitkomst ervan geeft een objectieve indicatie over de belangrijkheid van het risico. De kwantificering is dan een vereenvoudigd model over elk risico op zich. De restrictie – op alle risico's anticiperen is een illusie – kunnen desgewenst worden verzekerd. Het beste branddetectiesysteem sluit het ontstaan van brand niet uit, noch garandeert een hightech inbraakinstallatie dat een rancuneuze werknemer een dure machine saboteert. Of een cyberaanklacht legt uw bedrijfsnetwerk lam met ransomware. En wat met een gaslek

of een Amok-incident? Laat u deze risico's toe, of neemt u hiervoor een verzekeraar onder de arm?

Actieplan voor beveiliging met het incident als vertrekpunt

De volgende stap, na de veiligheidsbeoordeling en het oplijsten van de risico's, is het opstellen van een actieplan. Dit plan beschrijft in detail de te nemen maatregelen door het security personeel. In geval van een safety-incident zal dit plan logischerwijs worden gelinkt met de nood- en evacuatie-procedures. Het actieplan bepaalt twee situaties: (1) het incident is nog niet gebeurd en in dit geval moet alles in het werk worden gesteld om het incident te voorkomen, of (2) het incident is gebeurd of aan de gang en er moet op gepaste wijze worden gereageerd om erger te voorkomen. In de beide gevallen komt het erop aan sluitende tegenmaatregelen te bedenken door zich op voorhand in de situatie in te leven. En dat proces gebeurt het beste aan de hand van de scenariomethode.

De scenariomethode: 'Wat als...?'

De scenariomethode werd ontwikkeld door militaire strategen alsook door Shell om met meerdere mogelijke toekomstige rekening te houden. Het is een didactisch instrument om aan goed risicomanagement te doen. Aan de hand ervan kan men op een eenvoudige manier tot een brede waaier van conclusies komen. De scenariomethode vertrekt steeds vanuit de vraagstelling 'Wat als...?', waarna het echte brainstormen begint. Geen ingewikkelde formules, wel gezond boerenverstand.



chemie & farma

De chemische industrie en life sciences is goed voor een jaarlijkse omzet van 63 miljard euro, 90.000 jobs en 3 miljard euro investeringen in onderzoek en ontwikkeling.

Eén derde van onze export komt van bedrijven uit de chemie en life sciences.

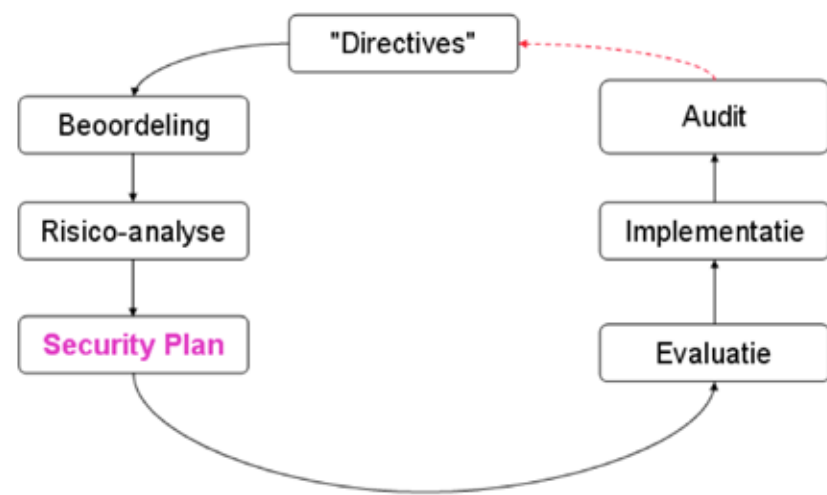
In Z Chemie & Farma brengt Kanaal Z deze sterhouder van de Belgische economie in beeld.



Z Chemie & Farma

Vanaf 26 februari elke donderdag op Kanaal Z of via www.kanaalz.be

kanaal Z
POWERED BY 



Aangezien een goed securityplan altijd een momentopname is, en dus empirisch wordt bijgestuurd, zijn er misschien maar enkele extra maatregelen nodig om de auditor tevreden te stellen.

De scenariomethode in de praktijk

Bij de vraagstelling wordt onderscheid gemaakt tussen drie doelwitgroepen: de personen, de bedrijfsmiddelen en de infrastructuur. Op deze 'targets' wordt de scenariomethode toegepast. Ter info: ook het gecertificeerde Risk Management Systeem (ISO-31000) volgt grotendeels deze denkpiste. Onderstaand voorbeelden van een incidentenvraagstelling die van toepassing is op een Seveso⁷-haventerminal:

- Wat als het IT-lokaal vuur vat?
- Wat als de gasleiding wordt stukgeslagen waardoor een giftige rook zal vrijkomen?
- Wat als de radio in het wachtlokaal wordt gestolen?
- Wat als een bezoeker een verboden zone binnenwandelt?
- Wat als een matroos drugs aan land probeert te smokkelen?
- Wat als een personeelslid wordt bedreigd door een bezoeker met een mes?
- Wat als ongebeleide bagage wordt aangehouden in het administratieve gebouw?
- Wat als een laadinstallatie wordt gesaboteerd waardoor een container in zee valt?
- Wat als iemand over het hekwerk klimt en zich vastketent aan een nucleaire container?
- Wat als een aangemeerd schip met opzet wordt geramd door een sleepboot?
- Wat als een gekaapte LNG-tanker de haven binnenvaart en zijn lading tot ont-ploffing brengt?

Standard Operating Procedures (SOP's) en speciale tegenacties

Het antwoord op deze 'Wat als'-vragen beschrijft welke organisatorische, bouwkundige, elektronische en meldingsmaatregelen nodig zijn om elk risico maximaal in te dijken. Hiermee wordt een proactief actieplan ontwikkeld dat zich onttrekt wanneer een welbepaald risico een incident is of dreigt te worden. Aangezien bepaalde risico's eenzelfde afhandeling vragen kunnen de tegenmaatregelen worden ondergebracht in een soort draaiboek van SOP's, dat door het personeel en de interim is gekend. Het actieplan van speciale procedures en veiligheidsinstructies wordt het best door een ervaren security taskforce-

team opgesteld... én ook regelmatig bijgestuurd. Deze aanpak is de beste garantie opdat uw bedrijf bij een volgende audit het veiligheidscertificaat zal behouden of verkrijgen.

Security Awareness bij het personeel

Een goede manier om incidenten voor te zijn, is door zich voortdurend bewust te zijn van de mogelijkheid op malafide of criminele acties. Alert zijn is hier de boodschap. Dreigend onheil of verdachte handelingen moeten meteen worden gemeld en vervolgens met de nodige omzichtigheid benaderd. Tip: leer het personeel om tijdens het 'spotten' van een verdacht persoon, een voertuig of een lading om zoveel mogelijk relevante informatie te herkennen (efficiënt) te communiceren. Een collectieve anticipatie dus op security-incidenten door meer aandacht te besteden aan de proactieve acties (preventie) in plaats van de reactieve acties (crisis management). En wees extra aandachtig en kijk ook uit voor mogelijke hinderlagen of afleidingsmanoeuvres...

Door Philip Vandenbon

1. TAPA: Transported Asset Protection Association
2. FSR: Freight Security Requirements
3. ISPS Code: International Ship and Port facility Security Code (Europa: EG/725/2004)
4. AEO: Authorized Economic Operator
5. LME: London Metal Exchange
6. INCERT: Intrusion Certification
7. SEVESO: verwijst naar een industriële ramp in Italië (1976) waarna Europese richtlijnen zijn aangenomen.

Impact ↑	Rampzalig	5	10	15	20	25
	Ernstig	4	8	12	16	20
	Hevig	3	6	9	12	15
	Matig	2	4	6	8	10
	Klein	1	2	3	4	5
		Zeer onwaarschijnlijk	Onwaarschijnlijk	Mogelijk	Waarschijnlijk	Zeer waarschijnlijk
		Kans →				

Een goede risico-inschatting, een vuistregel als het ware, is om het verwachte verlies (Impact) en de frequentie (Kans) van het risico met elkaar te vermenigvuldigen.

IDIS ANPR

Baanbrekende nauwkeurigheid kentekenplaat herkenning

- met een multi-lane zicht
- bij een breed scala van weersomstandigheden
- zelfs bij een slecht verlichte kentekenplaat

IDIS ANPR

de nieuwe premium standaard

IDIS ANPR is wederom een revolutionaire innovatie van IDIS.

Deze innovatieve technologie maakt nauwkeurige kentekenplaat herkenning over meerdere rijstroken mogelijk. IDIS ANPR biedt een eenvoudige en snelle implementatie, gebruikersvriendelijkheid, meetbare besparingen en nog veel meer prestatievoordelen in vergelijking met traditionele ANPR technologieën. Het is de perfecte aanvulling op de totale IDIS productenrange.

Belangrijkste kenmerken

- Betrouwbaarheid en toonaangevend niveau op het gebied van nauwkeurigheid in alle omstandigheden
- Echte multi-lane view mogelijk
- Breed zichtveld en superieure beeldkwaliteit
- Eenvoudige plug-and-play technologie
- Flexibiliteit positionering camera en apparatuur
- Minder complex, eenvoudige bediening en onderhoud
- Naadloze integratie met IDIS surveillance-platformen

Belangrijkste voordelen

- Toekomstbestendige technologie, compatibiliteit met toekomstige generatie IDIS camera's en recorders
- Kostenbesparend en lage 'costs of ownership'
- Verbeterde veiligheid en beveiliging
- Verbeterde surveillance, met een hoge kwaliteit bewijskracht beelden
- Operationele efficiëntie door automatisering handmatige taken
- Meer rendement uit commerciële activiteiten
- Betere rapportage en opvolging
- Snelle return on investment

IDIS One Solution. One Company. info@be.idisglobal.com

AnB-Rimex breidt aanbod aan geïntegreerde veiligheidsoplossingen uit

Op New Security lanceerde AnB-Rimex, gespecialiseerd in geïntegreerde oplossingen op het vlak van inbraakbeveiliging, domotica, communicatie, videosystemen en toegangscontrole, haar nieuwe range Belgian Security Articles (BSA). Met deze videobewakingscamera's en toebehoren, op maat van de Belgische markt, breidt het bedrijf uit Herstal haar diversiteit aan geïntegreerde beveiligingsoplossingen verder uit.

Wat NVR-recorders binnen de BSA-range betreft, zijn er onder meer de serie BSA4 en BSA5, in functie van het aantal camera's dat kan worden geconnecteerd. De eerste beschikt over H.265/H.264 videocompressie technologie, 200 Mbps inkomende bandbreedte en 8 MP resolutie voor IP-camera's. De tweede beschikt over maximum 320 Mbps inkomende bandbreedte en 12 MP resolutie voor IP-camera's. Met het compressieformaat H265 kan er dus aan bandbreedte worden ingewonnen waardoor er meer camera's op het netwerk kunnen worden aangesloten en er minder ruimte op de harde schijf wordt ingenomen. "Buitenbeentje is de BSA hybride recorder – die meerdere technologieën combineert – voor bestaande installaties. Pluspunt is dat de coaxiale bekabeling hier volledig kan worden gerecupereerd", aldus Ibrahim Tiryaki, product manager CCTV van AnB-Rimex. Al deze NVR-recorders ondersteunen ingebouwde intelligente videoanalyse (IVS) IP-camera's.

Breed cameraspectrum

Het gamma BSA-camera's bevat een zeer breed assortiment aan camera-systemen met resoluties variërend tussen 3 en 12 MP. Zo zijn er onder meer de IR Mini Dome Network camera's van 4 MP en 8 MP. Deze laatste is vandalismebestendig. De IR Bullet Network Camera (4MP) is niet uitgerust met ingebouwde video-intelligentie (IVS) maar is wel varifocaal. Dezelfde BSA-camera met 8 MP is wel uitgerust met IVS. Hoe hoger de camera resolutie, hoe vaker voor de H.265/H.264 videocompres-

sie technologie wordt geopteerd, om niet in de problemen te komen met de bestaande bekabeling.

Videoparlofonie

De BSA-videoparlofonie zal eveneens compatibel zijn met het HOME ANYWHERE-platform van AnB-Rimex. Naast videobewaking zijn er indoor en outdoor videofoniekits (IP of tweedraads) met verschillende modellen van touchscreens. "Het voornaamste pluspunt is het brede scala aan uitbreidingsmogelijkheden dat AnB-Rimex biedt. Een videofonie-oplossing en – in een latere fase – een camera IP-oplossing kunnen geïntegreerd worden. Eventueel kan er nog een anti-inbraak of toegangscontrolesysteem worden aan toegevoegd. Bedoeling is om zoveel mogelijk technieken in een geïntegreerde beveiligingsoplossing met het HOME ANYWHERE-platform onder te brengen", aldus Philippe Stas, general manager van AnB-Rimex.

Projecten

Inmiddels realiseren klanten-installateurs van AnB-Rimex reeds enkele mooie BSA-projecten. Zo werd in het Pass, een wetenschappelijk avonturenpark in Frameries (Mons), een 50-tal camera's van 3 MP aangesloten op 10 over de site verspreide NVR-recorders, beheerd door een softwareoplossing voor de volledige site. Ook op het Domein van Wégimont (Provincie Luik) werd een aantal ANPR-camera's (2 MP) van BSA geïnstalleerd. Op de sites van 2 Volvo-concessionarissen (Herstal en Namen) werd voor speed dome camera's (2 MP) van BSA geopteerd. Net als op het bedrijfsterein van Abelag in Zaventem waar een twaalfstal vandalismebestendige camera's (6 en 12 MP) werden geïnstalleerd.

Door Philip Declercq

Foto's: AnB-Rimex

www.anb-sa.be



Schema met de mogelijke functies van het BSA-Dahua Intelligent Video System

KX15DT



Beproefde indoor detectie!

Betrouwbare dualtech beveiliging.

Installeer de bedrade KX15DT en u kunt erop vertrouwen dat de gebruiker beschikt over een uitstekende beveiliging van zijn eigendommen. De KX15DT omvat diverse functies om zich aan zijn omgeving aan te passen en biedt superieure indoor detectie die ideaal is voor particuliere en commerciële toepassingen.

www.facebook.com/pyronix

[@pyronix](https://twitter.com/pyronix)

[Volg ons op LinkedIn](https://www.linkedin.com/company/pyronix)

Hikvision Europe, Dirk Storklaan 3, 2132 PX Hoofddorp, The Netherlands
Tel: +31-23-5542770 E-Mail: sales.eu@hikvision.com Website: www.pyronix.com

Paxton on tour met software-update en nieuw paneel

De toegangssystemen van specialist Paxton zijn ondertussen goed ingeburgerd. Onlangs ging het bedrijf op tournee door de lage landen om enkele nieuwigheden voor te stellen, waaronder de update van de Net2 software. Ook Opensource platform Milestone was van de partij en toonde hoe de oplossingen van Paxton geïntegreerd kunnen worden. Top Security ging langs op de voorstelling in Lokeren.

Net2 software update v5.04

Software updates zijn veel meer dan een noodzakelijk kwaad. Eindklanten zijn steeds vragende partij om meer functionaliteiten toe te voegen aan hun toestellen. Paxton luisterde naar de diverse vragen van die klanten en komt daarom met een belangrijke update van haar Net2 software. Er kwamen onder andere uitgebreide functies voor rapportage en datumbeheer, triggers en acties per paneel, uitgebreide deuralarm gebeurtenissen en meer aandacht voor datasecurity. De nieuwe update is beschikbaar voor de Lite en Prosoftware. **Uitgebreide rapportagefuncties**

Er wordt steeds vaker gevraagd naar grotere rapportagemogelijkheden. Er was al de mogelijkheid tot het monitoren van gebruikersgebeurtenissen, maar in de update is de nieuwe functie om ook systeemgebeurtenissen te loggen. Ook de mogelijkheid om een datum- en tijdsselectie te creëren is uitgebreid, waardoor een fijnere afstemming mogelijk is. De functie 'specifieke dagen' is tevens uitgebreid waardoor eindklanten bijvoorbeeld een vakantiesluiting in één keer kunnen toevoegen.

Autorisatieprofielen

Een zeer belangrijke aanvulling zijn de autorisatieprofielen. Zo kunnen bijvoorbeeld lijsten getrokken worden van de locaties waar een bepaalde gebruiker toegang tot heeft, of een lijst per toegangspunt met wie er binnen kan. Een voorbeeld hiervan is om een lijst te verkrijgen van iedereen die toegang heeft tot een magazijnruimte. **Deuralarm gebeurtenissen**

Wie met deurcontacten werkt kent de situatie waarbij er alarmen worden gegenereerd bij ongebruikte contacten. Het is nu mogelijk om de alarmmeldingen uit te zetten, zoals alarmen uit bij deur geforceerd en alarmen uit bij deur te lang open.

Ongebruikte tags

Deze functie was al aanwezig in de vorige versie, maar is uitgebreid. Er kan nu aangegeven worden hoelang ongebruikte kaarten en tags niet gebruikt werden.

Actie per paneel

Het is nu mogelijk om een trigger- en actie-regel te maken per paneel, zo kunt u dus een actie starten afhankelijk van de locatie waar de gebruiker een oproep doet.

De belangrijke update van de Net2 software geeft de eindklant meer opties.

Dataprotectie

In 2018 wordt de General Data Protection Regulation van kracht, een regeling over de bescherming van persoonsgegevens. Wanneer persoonlijke gegevens worden verzameld, moeten partijen die deze data verzamelen, zowel binnen als buiten de EU, zich aan bepaalde regels houden. Ook daar werd rekening mee gehouden bij de

update door het instelbaar maken van het bewaren van gebruikersgebeurtenissen. Daarnaast kan er ingesteld worden dat de Net2 softwarebeheerder automatisch uitgelogd wordt en kunnen bepaalde eisen opgelegd worden aan de sterkte van het wachtwoord.

Net 2 Entry Touchpaneel

Een tweede nieuwheid is het nieuwe Net 2 Entry Touchpaneel. De belangrijkste nieuwe functies zijn de dynamische zoekfunctie, het gebruik van profielfoto's en logo's om het scherm te personaliseren en zo gebruikers eenvoudig terug te vinden. Dat kan bijvoorbeeld handig zijn om in een bedrijvencentrum snel het juiste bedrijf en de contactpersoon terug te vinden. Het touchpaneel is eenvoudig bedienbaar en is standaard uitgerust met ingebouwde kaartlezer en keypad. De Net 2 Entry is ook volledig compatibel met het huidige Net2 systeem. Het esthetische ontwerp wordt sterk gewaardeerd, getuige daarvan de twee awards die het touchpaneel binnenhaalde: de IF Design award 2017 in



Roy Band (solution engineer Benelux region Milestone Systems) kwam de koppeling tussen Paxton en Milestone toelichten.

de categorie Building Technology Products en de Red Dot Award 2017 in de categorie Communication Technology.

Update catalogus

Het aangepaste Touchpaneel krijgt ook een plaatsje in de update in 2017 van de catalogus, net zoals de HID activatiekaarten (maakt van een Paxton lezer een HID 125 kHz Prox lezer), de lezerfunctie kaar-



Stefan van der Velden (regional sales director Benelux, Paxton) toont het nieuwe Net 2 Entry Touchpaneel.

ten (zoals stille kaarten en led dimmen) en de halogeenvrije lezerkabel (voldoet aan CPR-brandclassificatie).

Koppeling met Milestone

Via een plug-in in Net2 kan Paxton direct geïntegreerd worden met Milestone zodat de gebruiker deuren en camera's kan monitoren vanaf 1 interface. Zo kan de gebruiker bijvoorbeeld de status van deuren in real-

time volgen en verifiëren of iemand die de deur opent met zijn pasje, daadwerkelijk de juiste persoon is. Ook kunnen deurstatus en gebeurtenissen op plattegrond gezien en van daaruit bediend worden.

Door Sammy Soetaert

www.paxton-nl.com

Terreinbeveiliging, natuurlijk de beste bescherming



Goede terreinbeveiliging is een combinatie van én de juiste kennis én uitstekende producten. Effectieve beveiliging vraagt om een professionele, liefst onzichtbare en natuurlijke installatie. Met onze systemen houdt u ongenode gasten letterlijk buiten de deur. En hoe sneller we een inbraak detecteren, hoe minder schade er wordt aangericht.



GPS Perimeter Systems bv
Postbus 50, 1740 Ternat
info@gps-perimeter.be
T +32 (0)2 569 77 34

GPS denkt niet in beperkingen, maar in oplossingen

Specialisten in terreinbeveiliging door bundeling van kennis en ervaring

www.externalsecurity.com

Geïntegreerde veiligheids- & audiovisuele systemen



TOEGANGS-
CONTROLE



CAMERA-
BEWAKING



INBRAAK



BRAND



AUDIOVISUEEL

Onze oplossingen

- > Toegangscontrole
- > Technische alarmen
- > Camerabewaking
- > Inbraakdetectie
- > Biometrische systemen
- > Branddetectie
- > Mobiele beveiligingssystemen
- > Perimeterbewaking
- > Video Content Analysis (VCA)
- > Gezichtsherkenning / identificatie
- > Nummerplaattherkenning (ANPR)
- > Overkoepelende beheersystemen
- > Videoplatformen
- > Software-integratie
- > Installatie en implementatie
- > Helpdesk en 24/7 Bijstand



B-1650/a



B-9070-FD-2



ENGIE FABRICOM
DEPARTMENT SECURITY & AUDIOVISUAL
Kontichsesteenweg 25
2630 Aartselaar - BELGIË
tel. +32 3 871 15 00 - fax +32 3 870 12 69
secr.security@engie.com



Hikshow toont toekomst vol innovatie

Als journalist zijn we voortdurend te gast op bedrijfsevenementen en vakbeurzen. Zo bezochten we onlangs Infopol. Op de stand van Hikvision werden we getriggerd door het enthousiasme waarmee de innovaties van de marktleider in videobewaking getoond werden. Een uitnodiging voor de Hikshow, waar de oplossingen van het bedrijf uitgebreider aan bod kwamen, sloegen we dan ook niet af.

Steile groei

We moeten toegeven dat het bezoek aan Hikvision niet helemaal ongepland was. We volgen het bedrijf al langer met argusogen. De snelle groei is ook bij ons niet onopgemerkt gebleven. Onderweg naar Infopol hadden we ons reeds verdiept in die steile opgang, want ondanks de nog zeer recente oprichting in 2001, groeide Hikvision in no time uit tot wereldmarktleider in CCTV en videobewakingsapparatuur. De motor van die steile groei? De enorme investeringen in de R&D-afdeling. Liefst 9.000 ingenieurs, waaronder 2.000 software ingenieurs, gaan dagelijks aan de slag om tegemoet te komen aan de wereldwijde noden en evoluties. Maar vooral: 8 % van de inkomsten van het bedrijf wordt opnieuw geïnvesteerd

in nieuwe ontwikkelingen. Het resultaat mag er zijn, want ondertussen is Hikvision uitgegroeid tot een wereldwijde technologie gigant actieve mastodont met meer dan 20.000 werknemers, een omzet van 4,67 miljard \$ in 2016 en aanwezigheid in meer dan 100 landen.

Hikvision op Infopol

Die R&D-inspanningen leveren boeiende oplossingen op, waarvan we een deel konden zien op Infopol, waar we de enthousiaste Roeland De Cauwer en Manuel Lambrechts ontmoetten. Roeland is key account manager, Manuel is pre sales engineer bij Hikvision Europe. We vroegen hen toen hoe het is om te werken voor een dergelijk bedrijf. Roeland De Cauwer: "Het is



Roeland De Cauwer (key accountmanager) stelde de innovaties van Hikvision voor. Liefst 9.000 ingenieurs, waaronder 2.000 software ingenieurs, gaan dagelijks aan de slag om tegemoet te komen aan de wereldwijde noden en evoluties.

enorm stimulerend om deel te kunnen uitmaken van het groeiverhaal van Hikvision. De snelheid waarmee het bedrijf innovaties op ons loslaat is enorm. Het is alsof we op een TGV gestapt zijn die bij elke tussenstop weer vernieuwende producten presenteert. Zo kunt u hier onze PanoVu camera's zien, maar ook oplossingen voor verkeersmonitoring en onze Drone UAV Jammer, een systeem om drones onschadelijk te maken. Maar dit zijn natuurlijk toepassingen specifiek voor deze beurs." Manuel Lambrechts: "We hebben een veel breder gamma dat we kunnen aanbieden, van een eenvoudige wifi-deurbel tot hoogtechnologische bewakingsoplossingen die aan de allerhoogste



Tijdens de voorstelling van de Darkfighter X werd het werkingsprincipe met twee sensoren toegelicht.



Op Infopol kon men onder meer kennismaken met de PanoVu camera's, oplossingen voor verkeersmonitoring en de Drone UAV Jammer, een systeem om drones onschadelijk te maken.

veiligheidseisen moeten voldoen. Binnenkort zullen we een aantal innovaties tonen aan onze Belgische klanten tijdens de Hikshow in Antwerpen."

Innovatie in het DNA

En dus begaven we ons richting de Antwerpse Rijnkaai, waar de Bocadero dienst deed als locatie voor het aangekondigde innovatieve geweld. Het belang van de Hikshow bleek onder meer uit de aanwezigheid van Derek Yang, general manager Europe van het bedrijf. Hij nam het welkomwoord op zich en had het onder meer over het groeiend belang van artificiële intelligentie en welk enorm potentieel deze tak heeft voor een bedrijf als Hikvision. En daarvan kregen we meteen bevestiging in de eerste presentatie.

Deep learning

De enorme investeringen van Hikvision in R&D leveren zeer boeiende inzichten op over de toekomst van video in bewaking. Een zeer interessant aspect hierin is Deep Learning. Artificiële intelligentie zit nog lang niet aan zijn limieten, iets wat Shirley You, front-end developer samen met product manager Arno Tromp kwam toelichten. Hikvision zet hiervoor twee concepten in: DeepInmind netwerk video recorders (NVR) en de daarmee compatibele DeepInview camera's. De DeepInmind NVR's kunnen ingezet worden in bestaande installaties ter bevordering voor perimeterbewaking (96% nauwkeurig) of gezichtsherkenning. De zeer intelligente en performante DeepInview camera's kunnen zichzelf dan weer zaken als lichaamsvormen, gezicht- en 3D-personentellingen via zelflerende algoritmes snel eigen maken. Zij wer-

ken op basis van twee processoren. Eén voor de werking van de camera zelf, en één Movidius processor van de nieuwste generatie die voor het Deep Learning gedeelte gebruikt wordt. Bij DeepInmind wordt gewerkt met Nvidia processoren, die enorm snel grote hoeveelheden data (big data) kunnen verwerken. Zeker nu terrorisme helaas hoog op de veiligheidslijst staat, wordt dit soort detectie en de snelheid waarmee alles verwerkt wordt nog belangrijker.

H.265+ en Turbo HD 4.0

Manuel Lambrechts toonde de voordelen van de door Hikvision gepatenteerde H.265+ compressietechnologie. Deze compressie zorgt ervoor dat er veel meer beelden kunnen opgeslagen worden, minder bandbreedte wordt verbruikt en dat ook de beeldkwaliteit nog eens beter is. Zo wordt de markt klaargestoomd voor 4K. Die 4K heeft heel wat meer bandbreedte en (dure) stockageruimte nodig, maar met de compressiemogelijkheden van H.265+ wordt dit haalbaar én betaalbaar.

Bewaking met drones

Bewaking met drones is al langer de kinderschoenen ontgroeid. Daar waar dit tot voor kort voornamelijk bestond uit een drone met een erop gemonteerde camera, worden nu allerlei functionaliteiten toegevoegd aan de besturing van de drone, terwijl de camera's performanter worden en geavanceerde opdrachten kunnen uitvoeren. We keken dan ook uit naar de aangekondigde demonstratie met een lichtgewicht hoogtechnologische Falcon Drone. Vincent Hong toonde zich een volerde piloot en de weergoden waren ons

goed gezind. We kregen een prachtige vliegdemostratie boven de Schelde. De live-beelden op het grote scherm van de Rijnkaai en omgeving waren indrukwekkend en zeer gedetailleerd. Jerry Wang lichtte ondertussen de mogelijkheden toe van deze klasse C drone, met onder andere de mogelijkheid om het 'flight path' vooraf in te stellen. Maar ook de stabiliteit van de camerabeelden die onmiddellijk aangepast wordt aan de beweging van de drone is ronduit indrukwekkend. De directe reactie op besturings-

acties levert dan weer meer besturingscomfort op. De drones van Hikvision zitten onder de vleugels van Hikrobotics, een aparte divisie waar alles wat Robotica en Machine Vision behelst, is ondergebracht.

Darkfighter X

Was de drone de visuele blikvanger van de avond, dan schoot op technologiegebied Darkfighter X de spreekwoordelijke hoofdvogel af. Videotechnologie werkt tot nog toe quasi altijd op basis van één lens en één sensor. De ene sensor moet dus zowel licht detecteren om kleur te genereren als infraroodlicht opvangen om helderheid van het beeld te vrijwaren. Er moet dus steeds een compromis gezocht worden tussen kleur en helderheid. De Darkfighter X heeft 2 sensoren, één specifiek voor kleur en één voor infraroodlicht. Die 100% toewijding op één aspect zorgt voor een veel preciezer beeld met een perfecte kleurechtheid en een geweldige helderheid. Dit heeft uiteraard een enorme impact op de beeldverwerking in het donker, die daardoor veel soepeler verloopt. In de opzet met één sensor moet de sluitertijd te hoog ingesteld staan om voldoende licht te ontvangen, waardoor de beelden vegen kunnen vertonen. Ook ruis is een groot probleem, omdat de camera ondanks de duisternis toch licht moet creëren. Met de Darkfighter X en zijn twee sensoren zijn deze problemen van de baan. Meteen ook een zeer geslaagde afsluiter van een avond waar innovatie de rode draad bleek.

Door Sammy Soetaert

www.hikvision.com

PROFESSIONAL SECURITY EXHIBITION NEW SECURITY

➤ INTRUSION
➤ FIRE
➤ ACCESS CONTROL
➤ CCTV
➤ MONITORING

www.new-security.be
www.new-security.nl

New Security is de tweejaarlijkse vakbeurs gericht op installateurs security en professionele eindklanten. Distributeurs en fabrikanten stellen de recentste producten en systemen voor en geven doelgerichte informatie.

New Security is een Benelux-event en gaat afwisselend door in België en Nederland.

05+06.04.2018
WWW.NEW-SECURITY.NL
EXPO HOUTEN

13+14.02.2019
WWW.NEW-SECURITY.BE
BRABANTHAL LEUVEN



The New Camera Line Mx6 Creates More Possibilities. More Images, in All Light Conditions, in Every Standard.



More Intelligence Is on the Way.

The new Mx6 6MP camera system from MOBOTIX offers increased performance. A frame rate that is up to twice as fast than that of other cameras allows it to capture quick movements even better and simultaneously deliver sharp images in MxPEG, MJPEG and, for the first time in H.264, the industry standard. The innovative Mx6 camera line is faster, more flexible and higher-performing, opening up new application and integration opportunities for to you to meet all requirements.

**MOBOTIX**

Biometrie: de aders in onze handpalm liegen niet

Op Fujitsu World Tour in Brussel was er ruime aandacht voor de recente ontwikkelingen op het vlak van biometrische beveiliging. Digital Co-Creation tussen Fujitsu en het Hongaarse bedrijf BioSec leidde tot de ontwikkeling van StadiumGuard, een waterdichte oplossing voor identificatie bij toegang tot data en gebouwen. Dankzij nieuwe biometrische technologie kan onder meer het hooliganisme in de kiem gesmoord worden.

Biometrie wordt al enige tijd gebruikt als authenticatiemethode voor zowel toegang tot data als fysieke toegang tot gebouwen en domeinen. Toch blijken technieken zoals het scannen van vingerafdrukken, iris-, gelaats- en stemherkenning niet waterdicht. De gangbare systemen hebben hun zwakke plekken in de vorm van mogelijke vervalsing, oneigenlijk gebruik van een kaart, fraude, hacking etc. In de Spaanse Primera Divison werd een experiment met vingerafdruktechnologie bij toegangscontrole tot voetbalwedstrijden weer afgevoerd omdat de herkenningstijd te hoog lag.

Tot 15 miljoen referentiepunten

Handpalmtechnologie opent nieuwe perspectieven. Gezien de patronen die onze aders in onze handpalm vormen voor iedereen uniek zijn, vormt het scannen hiervan een afdoende oplossing om de identiteit van iemand met bijna 100% zekerheid te achterhalen. De patronen van aders kunnen zelfs vanop minimale

afstand gescreend worden (het toestel moet niet aangeraakt worden), waardoor besmetting (denk bv. aan ziekenhuisomgevingen) voorkomen wordt. “Waar bij vingerafdruktechnologie gebruik wordt gemaakt van 20 tot 120 referentiepunten, spreken we bij handpalmtechnologie van tot wel 15 miljoen referentiepunten onder de huid. Op het ogenblik dat de informatie wordt opgeslagen wordt deze, door middel van een speciale sensor (uitgerust met een PCB) AES256 geëncrypteerd”, aldus Oliver Reyers (business development manager PalmSecure Solutions bij Fujitsu Technology Solutions). “Bij de nieuwe PalmSecure-applicatie maken hackers geen schijn van kans. Met deze oplossing wordt het hooliganisme in de kiem gesmoord, en behoren aan de clubs opgelegde boetes voor het wangedrag van een aantal van hun fans tot het verleden.” Ook in voetbalstadions is de kans op aanslagen niet denkbeeldig, denk aan het recente incident met de spelersbus van Borussia Dortmund.

Waar bij vingerafdruktechnologie gebruik wordt gemaakt van 20 tot 120 referentiepunten, spreken we bij handpalmtechnologie van tot wel 15 miljoen referentiepunten onder de huid.

5 politiemensen voor 11.000 bezoekers

De oplossing kan onder meer efficiënt worden toegepast bij identiteitscontrole bij grote sportevenementen. Specifiek voor de beveiliging van stadia, is de oplossing geïntegreerd met het elektronische ticketing systeem, online betalen en camera-beveiliging. “De StadiumGuard oplossing – geënt op de PalmSecure-technologie – werd een drietal jaar geleden voor het eerst geïmplementeerd in het stadion van de Hongaarse voetbalploeg Ferencváros Boedapest. Het land kampt met zware problemen op het vlak van hooliganisme. In de bewuste Groupama Arena in Boedapest, waar deze ploeg haar thuiswedstrijden afwerkt, doen zich alvast geen ernstige ongeregelheden tussen home en away



Digital Co-Creation tussen Fujitsu en het Hongaarse bedrijf BioSec. Met StadiumGuard neemt de toegang tot een voetbalstadion per persoon amper 1 seconde in beslag.

fans meer voor”, aldus Oliver Reyers. “Voor een niet risicovolle wedstrijd eind vorig jaar, waarbij zo’n 10.000 bezoekers aanwezig waren, volstond de aanwezigheid van vijf politiemensen. De maatschappelijke kost ligt dus een stuk lager. Het systeem kan stapsgewijze worden uitgebouwd, bijvoorbeeld door te starten met de toegangscontrole voor VIP’s, en het geleidelijk uit te breiden.”

Vanaf de leeftijd van 16 jaar veranderen de patronen die de aders in onze handpalm vormen niet meer. Onder deze leeftijd laat de Europese wetgeving het opslaan van biometrische gegevens niet toe.

Aanzienlijk potentieel

Elke stadionbezoeker moet eenmaal door het systeem geregistreerd worden. De oplossing kan zowel in bestaande als in nieuwe stadions worden geïmplementeerd. Vanaf de leeftijd van 16 jaar veranderen de patronen die de aders in onze handpalm vormen niet meer. Onder deze leeftijd laat de Europese wetgeving het opslaan van biometrische gegevens niet toe. Daarom voorziet het concept dat kinderen (min zestienjarigen) via speciale gates, in de directe nabijheid van de met StadiumGuard beveiligde ingangen, het stadion worden binnengelaten. De oplossing vraagt een grotere investering dan andere biometrische oplossingen zoals vingerafdruktechnologie, maar heeft ook een groot potentieel buiten het stadionegebeuren. Zo kan het gebruik van de kaart gekoppeld worden aan shoppen in bepaalde retailzaken in het kader van een loyaliteitspartnership met de voetbalclub in kwestie. De software biedt ook de mogelijkheid om de stadionuitbater bijkomende informatie te geven, bijvoorbeeld met betrekking tot de mate van bezetting van de diverse delen van het stadion (crowd controlling). “Binnen de internationale voetbalwereld voeren we gesprekken met alle bij de stadionveiligheid betrokken partijen. En dat



De StadiumGuard-oplossing werd een drietal jaar geleden voor het eerst geïmplementeerd in het stadion van de Hongaarse voetbalploeg Ferencváros Boedapest.

zijn er nogal wat: de nationale voetbalbonden, de voetbalploegen uit eerste (en soms tweede) klasse, veiligheidsbedrijven, de eigenaars van de stadions (niet altijd de clubs), de politiediensten, de interne veiligheidsdiensten van de stadions,... Elke partij moet overtuigd worden en akkoord gaan. En dat is vaak een werk van lange adem. Maar in eerste instantie gaat het er om de voetbalbond van het land in kwestie over de streep te halen”, aldus Reyers.

Ook medische sector en bankwereld

De PalmSecure technologie kan ook gebruikt worden om de toegang tot datacenters of tot medicijnenkasten in ziekenhuizen te beveiligen, of in het kader van terrorismebestrijding. Het gebruik van paswoorden kan straks definitief tot het verleden behoren. Voor kantoorgebouwen kan het systeem en de software beperkt worden tot het aspect toegangscontrole. “Inmiddels zijn er wereldwijd meer dan 2 miljoen mensen vertrouwd met deze technologie, ook in diverse, andere toepassingen: loonadministratie, kiosk-systemen... Op de Belgische markt zijn er inmiddels reeds applicaties in de medische sector en in de financiële wereld. Voor deze laatste sector kunnen we onze technologie ook enten op een bestaande informatie-omgeving. Terwijl andere oplossingen op de markt hier-

voor een volledig nieuwe IT-configuratie vragen”, aldus Reyers.

Digital Co-Creation

Bij deze Digital Co-Creation voorziet Fujitsu de basistechnologie van de handpalm authenticatie (PalmSecure). BioSec, als één van de strategische partners van Fujitsu, biedt de kennis en de expertise van de bijhorende infrastructuur: de fysieke toegangscontrole, de camerabewaking en de beveiliging van de organisatie van het wedstrijdgebeuren. BioSec is een sterk innovatie- en technologiegedreven Hongaars bedrijf, opgericht in 2012. Een flexibele KMO met een 25-tal medewerkers, waaronder vooral softwareontwikkelaars. “Momenteel focussen we vooral op de voetbalsport, de IT-wereld en de beveiligingsbranche. Fujitsu zorgt voor technical support en maintenance, en voorziet in hoofdzaak in IT-ondersteuning en storage”, aldus Peter Györgydeák (CEO BioSec). “We verkopen geen producten, wel een concept. Wij zijn sterk in ontwikkeling, terwijl Fujitsu voor ons een sterke partner is op het vlak van sales en marketing, en zeer goed geïntroduceerd op de Belgische markt.”

Door Philip Declercq

🌐 www.fujitsu.com/be

VEILIG, FLEXIBEL EN EFFICIËNT

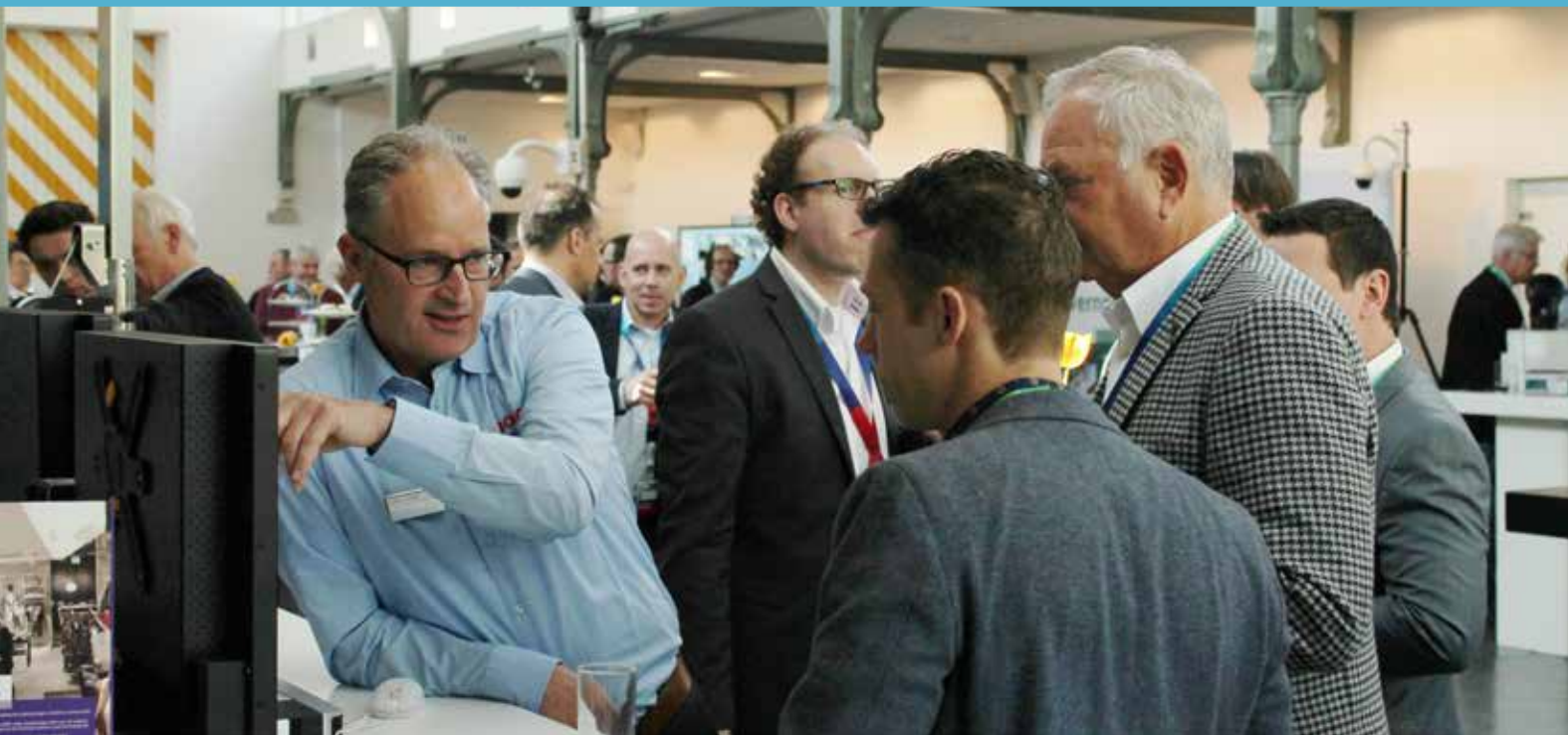
Dát, is toegangscontrole van SALTO Systems.



Het SALTO XS4 platform combineert elektronische deursloten, randapparatuur en software in een op maat gemaakte oplossing van elektronische toegangscontrole, eenvoudig in een netwerk zonder kabels.

- ❑ **VEILIG:** Bepaal wie waar naar binnen mag en wanneer.
- ❑ **TOEGANGSBEHEER:** Krijg inzicht in alle toegangsactiviteiten vanuit één platform.
- ❑ **GEBRUIKSGEMAK:** Pas toegangsrechten aan wanneer nodig en integreer uw bestaande systemen.
- ❑ **MOBIELE TOEGANG:** Gebruik uw smartphone met JustIN Mobile voor toegangscontrole en ontvang toegangsrechten in real-time.
- ❑ **EFFICIËNT:** In plaats van sleutels of sloten te vervangen wijzigt u toegangsrechten in de software zonder extra kosten.





Bosch Talks 2017 stelt focus op veiligheid scherp

Tientallen klanten en relaties van Bosch Security Systems konden tijdens een gesmaakt evenement in Hilvarenbeek kennismaken met de nieuwe oplossingen en applicaties van het bedrijf. De genodigden konden tussendoor genieten van productdemonstraties en interessante presentaties, met onder meer een toelichting door Kris De Gendt over de innoverende technieken toegepast in het simulatiecentrum voor de politie in Zedelgem.

Bosch Security maakt er ondertussen een jaarlijkse gewoonte van om haar klanten uit te nodigen. Na de Franstalige editie van vorig jaar, was het deze keer de beurt aan de Nederlandse en Vlaamse klanten. Saske Rodenburg (marketing & communication manager van het bedrijf) licht toe: "Het evenement is opgedeeld in drie pijlers. We hebben demo's door onze eigen productspecialisten, er komen enkele externe specialisten sessies geven rond thema's als communicatie en hacken en er is een marktplaats waar we onze innovaties voorstellen in applicatiegerichte onderwerpen. De deelnemers zijn klanten van ons: systeemintegratoren, groothandels, studiebuureaus en een aantal grote eindklanten."

Simulatiecentrum voor politie

Vijf jaar geleden werd beslist om een simulatiecentrum op te richten waar de Belgische politiediensten in een realistische omgeving levensechte situaties zoals bankovervallen, arrestaties en slechtnieuwsmeldingen kunnen simuleren. In de oude

militaire school in Zedelgem werd daarom een echte setting nagebouwd om deze situaties zo goed als mogelijk na te bootsen. Onder andere een onthaalruimte, een kantoor, een politiecel, een café, een sanitair blok, een appartement, verschillende

soorten trappen, een Salduz-verhoorlokaal, een bankautomaat, een incheckbalie, een winkel, een leslokaal en een volwaardige realistische buitenomgeving werden aangelegd. Kris De Gendt (zaakvoerder van de betrokken groothandel Security Projects):



Vijf jaar geleden werd beslist om een simulatiecentrum op te richten waar de Belgische politiediensten in een realistische omgeving levensechte situaties zoals bankovervallen, arrestaties en slechtnieuwsmeldingen kunnen simuleren.

"Camera's zijn voor cybercriminelen bijzonder interessant om te hacken, omdat ze grote hoeveelheden data kunnen verwerken. Ze zijn dus interessant om in te zetten in een cyberaanval."

Gerard Otterspeer, sales manager
Nederland Bosch Security Systems

"Om de lesgevers de kans te geven om de opleiding te evalueren en begeleiden, werden een aantal Bosch camera's geplaatst. In elke ruimte werden er twee diagonaal tegenover elkaar geplaatst zodat de ruimte volledig in beeld kan gebracht worden en men de situatie vanuit twee verschillende gezichtspunten kan bekijken. De camera's zijn ook uitgerust met nachtzicht dankzij de ingebouwde infraroodverlichting. Zo kunnen ook oefeningen zoals een inval in volledige duisternis plaatsvinden. Verder werden de camera's uitgerust met microfoons en luidsprekers zodat een lesgever vanuit de regiekamer in real-time kan meevolgen en bijsturen. Het beeld en geluid wordt ook continue opgenomen zodat de oefening opnieuw kan bekeken worden samen met de cursist."

Er waren ook enkele specifieke vereisten voor het systeem. Kris De Gendt: "Klopt, voor de opdrachtgever is het zeer belangrijk dat de camera's zeer snel reageren op wisselende lichtomstandigheden. Zo krijg je bij het binnen gooien van een flash bang een luide knal in combinatie met een helle lichtflits. Men wilde niet dat de beelden hierdoor een paar seconden verblind waren, de opname moest dus continu van hoge kwaliteit zijn. Voor verhoren en slechtnieuwsmeldingen is het dan weer belangrijk dat het beeld en geluid lipsynchroon worden opgenomen, omdat de gelaatsuitdrukkingen hierbij van enorm belang zijn. Dit kan met het Bosch Video Management Systeem."

Ook andere hulpdiensten als brandweer en ambulanciers komen ondertussen oefenen in het simulatiecentrum. Er zijn plannen om het centrum verder te verhuuren aan specifieke doelgroepen zoals dokters, apothekers en winkeliers. Zij kunnen opleidingstrajecten volgen zoals het leren omgaan met agressie.



Op de marktplaats werden enkele innovaties voorgesteld per applicatie.



Hacken: met de neus op de feiten

Ethisch hacker Edwin van Andel van het bedrijf Zerocopter gaf in een aantal markante voorbeelden inzicht in wat hacken inhoudt en waar de voornaamste zwakke plekken liggen. Ze illustreren het belang van bescherming tegen crimineel hacken. De hypermoderne Amerikaanse straaljager F35 had al meteen een quasi exacte Chinese kopie dankzij een datahack bij fabrikant Lockheed. Een belangrijk Nederlands energiebedrijf beschermt haar servers met paswoorden die nog op de default setting staan. Een goedkope camera van de doe-

het-zelfzaak die na welgeteld 98 seconden gehackt is. Ook in eigen land is hacken alom tegenwoordig. Een netwerkprinter die in de Antwerpse haven vrachtbrieven afdruckt, bleek plots verbonden te zijn met een vreemde verdeelstekker. Nader onderzoek wees uit dat deze een Raspberry Pi bevatte die de gegevens van de vrachtbrieven rechtstreeks doorstuurde naar een criminele organisatie, kwestie van de boot met de meest waardevolle lading te kunnen traceren. Het zijn vier angstaanjagende voorbeelden van waar lekken in databescherming kunnen toe leiden. Maar



Ethical hacker Edwin van Andel stond onder meer stil bij het gevaar van een USB-stick.



Gerard Otterspeer (Bosch) lichtte de maatregelen toe die Bosch toepast om de veiligheid van haar producten te waarborgen.



Ken Anthonissen (key accountmanager Bosch Security Systems)

hoe bescherm je je daartegen? Het al te naïef omgaan met onbekende USB-sticks is een bekend pijnpunt, maar wist u dat men op internet een gerichte DDoS-aanval eenvoudig kan bestellen voor de ronde som van 10 euro? Ook een gepersonaliseerd malwarevirus is in enkele klikken eenvoudig te bestellen, net zoals goedkope RFID-lezers die de frequenties van toegangsbadges kunnen scannen. Ook een te lakse toegangsbeveiliging van bedrijfsgebouwen is een probleem. Beschermen tegen hacking is dus niet evident, maar enkele eenvoudige maatregelen zoals verantwoord USB-gebruik, het niet klikken op links en het vermijden van naïviteit bij het gebruik van wachtwoorden zijn er daar enkele van. Van Andel besloot met een oproep om hackers niet als criminelen maar als medestanders te beschouwen. In deze optiek wees hij de toehoorders ook op de term 'responsible disclosure', wat betekent dat bedrijven een beleid uitstippelen waarbij ze beloven om geen strafvervolg in te zullen stellen tegen hackers, maar hen wel zullen belonen als zij een zwakke plek vinden in hun systeem. Op die manier krijgen hackers meer juridische zekerheid dat hun activiteiten niet als crimineel zullen beschouwd worden.

Gerard Otterspeer (sales manager Nederland Bosch Security Systems) pikte in zijn presentatie in op de boeiende wereld van het hacken met het voorbeeld van een

niet nader genoemde Amerikaanse universiteit die via haar snoepautomaten en verlichtingssysteem het slachtoffer werd van een DDoS-aanval. Camera's zijn voor cybercriminelen bijzonder interessant om te hacken, omdat ze grote hoeveelheden data kunnen verwerken. Ze zijn dus interessant om in te zetten in een cyberaanval. IP-netwerken zijn dus kwetsbaar maar de producten van Bosch zijn standaard verbonden via https en werken niet op basis met default wachtwoorden. Er zit ook geen extern operating system in de camera's. Ook toepassingen als conferencing zijn kwetsbaar. Bosch maakt hier gebruik van de WPA2-standaard. Bij de installatie wordt er niet gewerkt met een pin, en er zit ook geen toetsenbord meer op. De aanmelding op het netwerk gebeurt via een knop die een encryptieverbinding start. Brandmeldcentrales zijn dan weer via gateway verbonden. Die bezit de meest up-to-date certificaten.

Om de gevaren van het Internet of Things te counteren, nam Bosch Security recent ook een bedrijf gespecialiseerd in encryptie over.

Door Sammy Soetaert

🌐 www.boschsecurity.nl

Demosessies: personendetectie en rookdetectie

Naast de eerder theoretische presentaties, waren er ook demonstraties. Zo stond er buiten een intelligente camera opgesteld die in dit geval een weiland bewaakte. Personen werden feilloos gedetecteerd tot op meer dan 100 meter afstand. De camera kan ook geleerd worden om dieren en voertuigen te onderscheiden van mensen.

Ken Anthonissen (key accountmanager Bosch Security Systems) trok de toehoorders dan weer mee in een demonstratie rond rook- en branddetectie door camera's: "In toepassingen met hoge plafonds, zoals bij opslagmagazijnen, voldoet traditionele puntdetectie met rookmelders niet. In de zomer bijvoorbeeld, kan zich een 'warmtedeken' vormen net onder het plafond, waarin rook minder snel infiltreert. Het duurt dan te lang voor rook het plafond bereikt, waardoor te laat ingegrepen wordt. Ook valse alarmen komen bij dit type detectie te vaak voor. Bij videodetectie wordt rook direct aan de bron gedetecteerd, waardoor het slechts enkele seconden duurt voor er een alarm gegeven wordt. Er wordt gedetecteerd op kleur van de brand in combinatie met het flikkeren van de vlam en de driehoekige vorm van een brand."

Er zijn wel enkele voorwaarden verbonden aan een feilloze detectie, een lichtsterkte van minimaal 7 lux bijvoorbeeld. Ook als de kleur van de rook te weinig contrast heeft met de achtergrond, wordt de detectie bemoeilijkt.



Missie

De A.C.A. groepeert telebewakingsondernemingen en stelt zich onafhankelijk op van alle andere beroepsverenigingen voor elektronische beveiliging en fysieke bewaking en verleent haar medewerking aan initiatieven tot verbetering van de veiligheid van de klant. Zij werpt zich op als enige erkende gesprekspartner van de overheid en de internationale organisaties, voor wat betreft de specifieke bijdrage van zijn leden: de telebewaking.

De A.C.A. staat open voor een nieuwe samenwerking met zowel de elektronische beveiligingsbedrijven als met de fysieke bewakingsbedrijven en hun respectievelijke organisaties en ondersteunt alle initiatieven die leiden tot verbetering en verduidelijking van deze samenwerking, o.a. met betrekking tot de onderaanneming.

Activiteiten

Opvolging van alarmen bij particulieren, bedrijven, administraties:

- binnendringing, agressie
- brand
- technisch
- medisch

Bewaken via high-tech oplossingen:

- video-bewaking
- tracking & tracing (volgen van wagens)
- toegangscontrole

Service naar partners en derden:

- telepermanentie

Opstellen van interventieprocedures in samenwerking met politie, brandweer, technici, hulpverleners,...

Doelstellingen - Acties

- De evolutie van de wetgeving, waarbij meer en meer operationele verantwoordelijkheid toegekend wordt aan de alarmcentrales, dwingt ons tot een gezamenlijke aanpak rond thema's als aansprakelijkheid, procedures, de fiscale wetgeving, ...
- Een antwoord bieden naar de eindgebruikers toe in de vorm van een positieve en gezamenlijk geformuleerde communicatiestrategie, met als doel de regressie van de beveiligingsmarkt in ons land in te passen in de hogere groeicurves die door onze buurlanden worden gehaald.
- Wij wensen, door gezamenlijke actie met alle spelers op de elektronische beveiligings- en fysieke bewakingsmarkt, een positieve boodschap uit te dragen over de werking van onze sector en de ontwikkeling ervan te stimuleren

Professionalisme

De leden van A.C.A. beantwoorden aan de eisen van kwaliteitsprestaties:

Infrastructuur

- erkende software voor tele- en alarmbewaking, videobewaking, telepermanentie
- ontvangst van verscheidene protocols
- IP-netwerk
- vergevorderde signaalfiltratie ter ondersteuning van de overheidsdiensten
- betrouwbare informaticasystemen

Omkadering

- gekwalificeerd personeel volgens de in voege zijnde normen en wetten, meertalig en permanent gevormd om adequaat te handelen in dagdagelijkse en crisis-situaties

Partnership

De A.C.A. is het bevoorrechte aanspreekpunt van verschillende partners om een optimale beveiliging van goederen en personen te waarborgen zoals:

- de installateurs van beveiligingssysteem (inbraak, brand, agressie, hulpverlening)
- de interventie-eenheden (bewakers, politie, brandweer, technici, burgerbescherming,...)
- de service managers
- de verzekeraars, studie burelen, consultants

A.C.A.: Alarm Centrale Associatie v.z.w. (Ondernemingsnummer : 867744974)

Sint-Lendriksborre 3 – 1120 Brussel

Tel +32 2 639 39 71

Fax: + 32 2 639 39 79

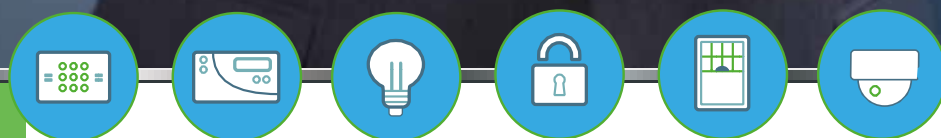
Email: info@a-c-a.be

www.a-c-a.be



In de wereld van de Internet of Things maakt betrouwbaarheid het verschil

UltraSync™ Secure Connectivity Solution



Veilige connectiviteit in No Time

Bekijk operationele status

- Verbindingsstatus
- Overzicht apparaten
- Filteroptie
- Rapporten

Diagnostiek verstrekken

- Connectiviteit
- Gebeurtenissenlogboek
- Mobiele RSSI
- Firmware-updates op afstand

Extern verbinden

Apparaten/services registreren

Geen configuratie vereist voor randapparatuur

UltraSync maakt het mogelijk dat u eenvoudig en snel M2M-verbindingen tot stand brengt voor intelligente randapparatuur zodat de verbindingen vooraf geconfigureerd zijn voordat de technicus aankomt op locatie.

Bijna real-time datacommunicatie

De snelheid van de data-overdracht van één punt in een netwerk naar een ander is cruciaal. UltraSync biedt bijna real-time datacommunicatie dankzij een hoog-presterend netwerk met lage latentie.

Veilige connectiviteit

Hoewel het belang van een veilige connectiviteit over het internet algemeen begrepen en erkend wordt, is de werkelijkheid vaak anders. UltraSync zorgt ervoor dat de connectiviteit te allen tijde is verzekerd.

UltraSync wordt ondersteund door Advisor Advanced.

We listened to you

Gluren bij de burens Digitale inbraken voorkomen

Hackers en cybercriminelen worden almaar driester en inventiever, zelfs voor het capteren van digitale videostreamen draaien ze al lang hun hand niet meer om. Waarom is dit voor hen een lucratieve 'markt' en wat kunt u er tegen doen?

Het lijkt wel het scenario van een slechte sciencefiction film, maar het is ondertussen al harde realiteit: hackers die zich toegang weten te verschaffen tot de beelden van IP-camera's en die, vanuit hun luie zetel, rustig alles kunnen bekijken wat die camera's capteren. De camera's kunnen bovendien ook een toegangspunt vormen waarlangs de cyberboeven diep in de computernetwerken van bedrijven en organisaties kunnen doordringen. De Britse geheime dienst MI6 noemde het probleem eind vorig jaar nog zelfs een 'bedreiging voor de nationale veiligheid' nadat bekend werd dat een van de grootste leveranciers van CCTV-materiaal in het V.K. een Chinees bedrijf is met banden tot in de hoogste regeringskringen. De camera's staan geïnstalleerd in onder meer luchthavens, overheidsgebouwen en de Londense metro.

Ook bij particulieren zijn er al heel wat gevallen aan het licht gekomen waarbij het een fluitje van een cent was om via een beveiligingscamera mee te kijken in de babykamer of de slaapkamer van de ouders. Vaak zijn niet alleen de beelden te bekijken, maar kunnen de camera's ook van op afstand bediend worden, of zelfs uitgeschakeld. De Russische site Insecam.org verzamelt honderden van die videostreams van onbeveiligde camera's, zodat ze voor de hele wereld te aanschouwen zijn. Op de beelden zijn nietsvermoedende mensen te zien in huizen, winkels en restaurants die zich er niet van bewust zijn dat het hele internet hen kan bekijken.

Afpersing en chantage

Het is ontegensprekelijk een feit dat videostreams van veiligheidscamera's een zeer interessant doelwit vormen voor cybercriminelen. Met de beelden kunnen mensen

in de gaten gehouden worden en kunnen hun gewoontes en patronen worden bestudeerd, de beelden kunnen eventueel gebruikt worden voor afpersing en chantage, uit puur vandalisme kan men de camera's uitschakelen, men kan bijvoorbeeld productiesites bespioneren, ... er zijn heel wat lucratieve scenario's te bedenken.

De meeste digitale inbraken kunnen alleen maar gebeuren door menselijk falen, nalatigheid, een slechte configuratie en/of gebrekkig onderhoud.

Bescherming: aandachtspunten en tips

Om u adequaat tegen dit soort praktijken te beschermen, is het belangrijk dat IP-camera's voldoende aandacht krijgen in de IT-veiligheidspolicy die elk bedrijf (hopelijk) heeft opgesteld. Net zoals als alle andere netwerkapparaten, clients en servers maken de camera's deel uit van het bedrijfsnetwerk en moeten ze ook op die manier beschermd worden. De meeste digitale inbraken kunnen alleen maar gebeuren door menselijk falen, nalatigheid, een slechte configuratie en/of gebrekkig onderhoud. Die bescherming begint dus al bij de keuze van de juiste betrouwbare fabrikant, de kunde van de installateur en de kennis van de werknemers die er mee om moet gaan. Zo is bijvoorbeeld belangrijk

dat de apparaten uitgerold en geïnstalleerd worden op een veilige manier. Als bepaalde services niet gebruikt worden, zoals bijvoorbeeld FTP (file transfer protocol), dan is het zeker raadzaam om die meteen ook uit te schakelen. Via FTP kan een hacker zonder veel problemen kwaadaardige code en scripts in een netwerk injecteren om zo de controle over te nemen. Ook niet-technische zaken moeten hier in overweging genomen worden. Bij het plaatsen van de camera is het bijvoorbeeld niet alleen belangrijk dat de juiste beeldhoek op het scherm komt, maar ook dat de camera hoog genoeg hangt om hem niet te kunnen beschadigen.

Het is ook absoluut noodzakelijk dat alle apparatuur in het netwerk, inclusief camera's, servers, printers en werkstations van de laatste firmware voorzien worden. Heel vaak voorziet die firmware immers in oplossingen voor recent ontdekte beveiligingsgaten. Dat is meteen ook de reden waarom een onderhoudsplan en -cyclus zo belang-



Het is aangeraden om duidelijke verantwoordelijkheden en 'ownerships' bij de werknemers te leggen. In veel organisaties gaat het fout met cyberveiligheid omdat het niet duidelijk is welke mensen nu precies welke toegangsrechten hebben.



rijk is: alleen zo weten bedrijven nog welke apparaten nog niet geüpdatet zijn. Als u de camera heeft uitgepakt en van de laatste firmware heeft voorzien, moet u meteen ook het standaardwachtwoord veranderen. Die standaardwachtwoorden zijn voor bijna alle fabrikanten immers probleemloos te achterhalen met een simpele zoekactie op Google. Zo maakt u

het de hackers dus wel héél gemakkelijk. Kies daarbij natuurlijk ook een wachtwoord dat niet makkelijk te raden valt. Uw geboortedatum, de naam van uw hond, of nog erger, "123456" of "wachtwoord" zijn uiteraard totaal uit den boze. Verander deze wachtwoorden ook regelmatig.

Natuurlijk is een netwerk ook maar zo veilig als zijn zwakste schakel. Zorg daarom dat de juiste firewalls zijn geïnstalleerd en correct werken en gebruik steeds beveiligde connecties (http digest authentication en HTTPS). Op die manier bent u zeker dat alle informatie die over het netwerk loopt versleuteld is.

Tot slot is het ook aangeraden om duide-

lijke verantwoordelijkheden en 'ownerships' bij de werknemers te leggen. In veel organisaties gaat het fout met cyberveiligheid omdat het niet duidelijk is welke mensen nu precies welke toegangsrechten hebben. Probeer daarbij te werken volgens het principe van 'least privileged accounts'. Dat betekent dat werknemers enkel toegang krijgen tot die infrastructuur die strikt noodzakelijk is voor hun job. Specifiek bij het gebruik van IP-camera's is het ook raadzaam om geen enkel apparaat rechtstreekse toegang tot de camera's te geven, tenzij echt noodzakelijk. Gebruik beter een tussenstation als een Video Management Systeem of een media proxy.

Door Edwin Roobol, regional director Middle Europe bij Axis Communications

🌐 www.axis.com



ATRIUM

plug en play
ingebouwde webserver
eenvoudig beheer

Atrium behoort tot de nieuwste generatie toegangscontrolesystemen. Deze bieden een extra voordeel in gebruiksgemak door de toevoeging van een webinterface.

Zo kan je vanuit je luie zetel of vanop het strand heel eenvoudig uw systeem beheren via je tablet of smartphone. Door deze voordelen in een compact modulair systeem te verwerken biedt Atrium een oplossing voor één deur tot systemen met honderden deuren.

Contacteer ons voor een uitgebreide demo of vraag gratis uw opleiding aan via (0)56 73 93 00

"Eén oplossing van één leverancier, perfect!"

...dat betekent minder werk."

Dankzij de AXIS Companion Line ben ik in staat de wensen van mijn klanten te vervullen met een kwalitatief hoogwaardige oplossing.

Heeft u interesse om **AXIS Companion Line Specialist** te worden? Bezoek onze website www.axiscompanion.com/apply of bel ons op +31 10 750 46 00



In de Rotterdamse Onderzeebootloods verzamelde een 1000-tal beveiligingsinstallateurs, waaronder heel wat bezoekers uit België.

SST2017: geavanceerde security-oplossingen in Onderzeebootloods

De vierde editie van de Smart Security Technology (SST) ging door in de RDM Onderzeebootloods in het oude havengebied van Rotterdam. Tijdens het event op deze schitterende locatie toonde SmartSD samen met haar leveranciers de nieuwste technieken en ontwikkelingen uit de elektronische beveiligingswereld. In de openingsshow was er, naast aandacht voor face matching en inbraakdetectie, ook een spectaculaire camera shootout.

Na de geslaagde SST-editie vorig jaar in de Gentse Eskimofabriek had SmartSD er ook nu alles aan gedaan om spectaculair uit te pakken. In de mooi gerenoveerde Rotterdamse loods waar vroeger onderzeeërs van de helling liepen, verzamelde een 1000-tal beveiligingsinstallateurs, waaronder ook ditmaal heel wat bezoekers uit België. "SmartSD wil verder doorgroeien, zowel op de Belgische als de Nederlandse markt. Daarvoor blijven we investeren in technische mensen en in support naar onze klanten toe. Een en ander heeft ervoor gezorgd dat we onze te krap geworden locatie in Gilze straks inruilen voor een ruimer en comfortabeler pand, en dit (opnieuw) in Breda. Onze Belgische klanten blijven welkom in ons filiaal in Wilrijk. Beveiliging is een hightech sector. Innovatie is uiteraard zeer belangrijk maar de relaties met onze klanten en leveranciers zijn dat evenzeer, vandaar ook dit jaarlijks evenement,

dat afwisselend in België en in Nederland plaats vindt", aldus Rik van Aken (marcom specialist SmartSD). Volgend jaar viert de prominente distributeur van oplossingen voor camerabeveiliging, toegangscontrole en inbraak- en branddetectie zijn 10-jarig bestaan.

Face matching

Naast de 43 exposanten op de beursvloer en de tal van (drukbeklante) Belgische keukentjes, was er ook een uitgebreid seminar-programma. Kers op de taart was de openingsshow gepresenteerd door de product managers van SmartSD. Met het thema face matching

mocht Bruno Taymans, business development manager CCTV & Integrated Systems, de spits afbijten: "De technologie rond gezichtsherkenning heeft de voorbije jaren grote stappen vooruit gezet. Gezien de recente golf van aanslagen en de toegenomen veiligheidsproblematiek neemt het belang van face matching steeds meer



"De technologie rond gezichtsherkenning heeft de voorbije jaren grote stappen vooruit gezet", aldus Bruno Taymans van SmartSD. (Foto: SmartSD)



Gezien het toenemende belang van face matching ging SmartSD in zee met Herta, een Spaanse fabrikant gespecialiseerd in het ontwikkelen van software voor gezichtsherkenning.



De cameratechnologie ontwikkelt zich steeds sneller en op meerdere vlakken: hogere sensorgevoeligheid, hogere resolutie, kortere sluitertijd...

toe. Daarom is SmartSD in zee gegaan met Herta, de Spaanse fabrikant gespecialiseerd in het ontwikkelen van software voor gezichtsherkenning. Hierbij worden resolutiefoto's, verzameld in een database, gematcht met live videostreamen. Speciale software zorgt ervoor dat er vanuit 1 enkele fotohoek verschillende biometrische referentiefoto's van één of meerdere personen worden genomen, en daarna in 3D omgezet. Op die manier kunnen 1 (of meerdere) perso(n)en worden gedetecteerd. Per seconde kunnen er tot 115 frames worden geanalyseerd, terwijl er bijvoorbeeld slechts 25 beelden werden opgenomen. De enige beperking bij deze manier van gezichtsherkenning is dat er – per gezicht – een minimum van 100 pixels noodzakelijk is. Bij elke gedetecteerde persoon kan je zien met welke referentiefoto er een match is. Deze foto's worden opgeslagen in het videomanagementsysteem. Het Herta-systeem biedt ook de mogelijkheid om een alarm te versturen."

Meer cloudoplossingen

Met zijn nieuwe VuPoint camera's – die via P2P, plug & play gekoppeld kunnen worden aan de cloud – en de verdere uitbreiding van de Smart Home oplossingen blijft RISCO Group innoveren. Alle technologieën kunnen via dezelfde RISCO applicatie bediend worden. Inim Electronics introduceert de Inim Cloud. Deze oplossing maakt het mogelijk van om het even waar de Smart Living panelen te beheren. Op het gebied van branddetectie lanceert Inim het modulair op te bouwen Praesidia brandmeldsysteem. Vanderbilt focust op het ontwikkelen en leveren van geavanceerde toegangs- en inbraakdetectieproducten en -systemen zoals MAGIC, SPC, Seismisch... De uitbreiding van de SPC Connect cloud zorgt ervoor dat de installateur over een bijzondere tool beschikt voor een eenvoudig beheer en onderhoud van de SPC panelen. SPC Connect cloud maakt – via video-integratie – onder meer visualisatie met behulp van plattegronden mogelijk.

Vertrouw in de cloud

Zijn collega Jeroen Vons belichtte de technologische evoluties inzake inbraakmeldsystemen. "Inim Electronics, Vanderbilt en RISCO Group hebben mooie cloudoplossingen in petto die het de installateur gemakkelijk maken. De tijd van de detectiesystemen met een eenvoudig keypad, eventueel uitgerust met status LED's – die enkel konden aan- of uitschakelen – ligt achter ons. Nu is iedereen verk(n)ocht aan de smartphone, waarop je een app voor een inbraakpaneel kan downloaden. We hoeven ons geen zorgen te maken over – of bang te zijn van – de cloud verbinding als such. Deze is veilig zonder meer. Zaken als pushnotificatie, bijvoorbeeld, heeft men uiteindelijk zelf onder controle."

Camera shootout

Daarna nam zijn collega Bruno Taymans het opnieuw over voor de spectaculaire camera shootout. "Naast gevoeligheid van de sensor zijn ook de hogere resolutie, de kortere sluitertijd van de camera, en de sterkere zoomlens en de evolutie van het zoekbereik voorname ontwikkelingen in de cameratechnologie. Ditmaal worden er geen nieuwe cameramodellen van diverse leveranciers in de weegschaal gelegd. Wel worden – per fabrikant – de parameters van de cameramodellen van nu met deze van 2 of 3 jaar terug met mekaar vergeleken." Zo werden bij Mobotix het oudere M12-model (3MP) en de nieuwe M16 (6MP) met elkaar vergeleken. Beide werden getest, zoals ze uit de verpakking komen, op dezelfde locatie en in dezelfde omstandigheden (dag/nacht). Bij de nieuwe oplossing is een van de nieuwigheden een security-programma dat ervoor zorgt dat de camera geoptimaliseerd is voor... security-toepassingen. Dit levert een bruikbaar beeld op. Dankzij de zeer gevoelige sensor wordt de persoon herkenbaar in beeld gebracht.

Gesofistikeerde camera-oplossingen

Hikvision lanceert zijn nieuwe Turbo HD 4.0 producten die gebruik maken van de nieuwe H.265+ videokompressie technologie. De nieuwe Easy IP3.0 camera's zijn uitgerust met deze technologie en bereiken superieure videoprestaties. Ze zijn uitgerust met 120 dB True WDR en beschikken ook onder meer over Hikvision EXIR 2.0 met Smart IR verlichting, en de Darkfighter ultra-low-lighting technologie. Ook Samsung Hanwha en Dahua presenteren nieuwe oplossingen. Sony pakt uit met nieuwe zeer lichtgevoelige camera's uitgerust met Exmor R TM CMOS-sensoren. De G6-R camera's in full HD bieden geavanceerde beeldtechnologie met een minimumverlichting van 0,006 lux, inspelend op de vraag naar meer lichtgevoelige camera's binnen de videobewaking.

Door Philip Declercq

www.smartsd.com



Bien gardé à chaque seconde Elke seconde veilig bewaakt

Alarm Monitoring

Security View “Video Verification”

Security View “Video Access”

Security View “Video Guarding”

Security Track

Security Assistance “Never Alone”

Teleservices

Reporting

Certifications



16.1027.01
Service Public Fédéral de l'Intérieur
Federale Overheidsdienst Binnenlandse zaken



TB-0004
INCERT certification



Association des Centrales d'Alarmes
AlarmCentrales Associatie



ISO 9001:2008



ACE Property of UTC

Contact us

Security Monitoring Centre BVBA/SPRL

Keizer Karellaan / Avenue Charles Quint 345
B-1083 Brussel / Bruxelles
Tel. +32 2 646.08.42 Fax +32 2 646.28.13
RPR Brussel / PRM Bruxelles 0454.284.850

<http://www.smc-net.be>
info@smc-net.be

Een halve eeuw brandpreventie

Na de brand in de Innovation in Brussel op 22 mei 1967 – waarbij 251 mensen het leven lieten – werd, op initiatief van de Beroepsvereniging der Verzekeringsondernemingen (Assuralia), de vzw ANPI opgericht. Voluit ‘Association Nationale pour la Protection de l’Incendie et la Vol’ of ‘Nationale Vereniging voor brand- en diefstalbestrijding’. 50 jaar later is ANPI uitgegroeid tot de referentie die alle betrokken actoren bij brandpreventie in ons land verenigt. Naast Assuralia zijn dat onder meer FOD Binnenlandse Zaken, AFT Detectie, Agoria en ORI. Op 22 mei 2017 werd er herdacht en vooruitgeblikt.

Na een historische schets van ‘De brand in de Innovation’ door historicus Siegfried Evens had Alain Verhoyen (general manager ANPI) het over de houding van de Belg ten opzichte van brandrisico's. Hij stelde de resultaten van de laatste tweejaarlijkse monitoring voor, en sloot zich aan bij de boodschap rond brandveiligheid die Agoria recent lanceerde. Hieruit blijkt dat één op de twee ondernemingen, gespecialiseerd in brandveiligheid, van oordeel is dat gebouwen in ons land nog onvoldoende beschermd zijn inzake brandveiligheid. Recente gebouwen stellen doorgaans weinig problemen op dat vlak. Op oudere gebouwen is er evenwel nog te weinig controle. Nogal wat beheerders van gebouwen gaan er – verkeerdelijk – van uit dat het volstaat om sprinklers of een rookdetectiesysteem te installeren om de brandveiligheid te garanderen.

Van 53 tot 80.000 woorden

Jan De Saedeleer van de FOD Binnenlandse Zaken besprak de evolutie en het huidige wetgevende kader inzake brandpreventie. Op het ogenblik van de ramp in Brussel bestond de wetgeving ter zake uit één artikel dat welgeteld 53 woorden telde. Na de ramp werd het bewuste artikel herschreven en dit niet zozeer vanuit doelgericht, wel vanuit een meer restrictief oogpunt. Het KB van 7 juli 1994 en zijn Bijlagen specificeren vooral de brandvoorschriften voor onder meer industriële gebouwen en kantoorgebouwen. Nochtans vallen de meeste slachtoffers ingevolge brand vandaag vooral in woningen en appartementsgebouwen. Anno 2017 omvat dit KB – dat

inmiddels... 9 maal werd gewijzigd – meer dan 80.000 woorden. Bernard Desmet van Assuralia had het over de organisatie van de brandverzekering in ons land, en over wat de brandverzekering precies dekt. Daarna belichtte Benoit Stockbroeckx van ANPI op zijn beurt de diverse niveaus inzake normalisering.

“Branddetectie vandaag gaat niet enkel over technologie maar is ook een kwestie van risicoanalyse en operationele procedures.”
Marnix Steenbeke, voorzitter Agoria Fire Technologies (AFT) Detectie

Branddetectie

De eerste branddetectienorm NBN S21-100, gepubliceerd in 1986, beperkte zich in hoofdzaak tot temperatuur-, rook- en

vlammelders. In de praktijk waren ze vooral bedoeld voor kantooromgevingen. “Pluspunt was de accurate branddetectie. Nadeel was dat deze systemen in andere omgevingen onder invloed van factoren zoals vocht, wind en stof, vaak voor vals alarm zorgden”, aldus Marnix Steenbeke, voorzitter van Agoria Fire Technologies (AFT) Detectie. “Anno 2017 hebben branddetectoren een doorgedreven technologische evolutie doorgemaakt. Ze zijn adresseerbaar, hebben driftcompensatie om de gevoeligheid constant te houden. Door de aanwezigheid van kortsluitisolatoren hebben kabelonderbrekingen en kortsluitingen minder impact op de totaalinstallatie. Men kan eveneens de vervuilingsgraad vanop afstand consulteren. Nu zijn er ook multicriteria detectoren op de markt waarmee men het meten van rook, temperatuur, CO etc kan combineren.



Op het ogenblik van de ramp in Brussel (Innovation) bestond de wetgeving ter zake uit één artikel dat welgeteld 53 woorden telde. Na de ramp werd het bewuste artikel herschreven en dit niet zozeer vanuit doelgericht, wel vanuit een meer restrictief oogpunt. Foto: herdenkingsplechtigheid



François Asselman van Belgian Fire Sprinkler Network had het onder meer over de verfijning van componenten en systemen bij automatische blusinstallaties.



Jan De Saedeleer van FOD Binnenlandse Zaken: "De controle op branddetectie in woningen en appartementsgebouwen moet nog beter".



"Branddetectie vandaag is een kwestie van risicoanalyse, technologische oplossingen en operationele procedures", aldus Marnix Steenbeke van AFT Detectie.



Alain Verhoyen (general manager ANPI) stelde de resultaten van de laatste tweejaarlijkse monitoring voor.

Deze kunnen worden bekabeld met redundante peer-to-peer netwerken, zodat men grote aantallen detectoren kan uitrusten en beheren."

Air sampling systemen kwamen op de markt in de periode dat blusgassystemen verboden werden. "Ze bieden het voordeel dat men brand zeer snel kan detecteren, waardoor de interventietijd om manueel tussen te komen toeneemt. Deze systemen zijn in de klassen A, B en C beschikbaar en in alle maten, gewichten en afmetingen voorhanden. Een andere hedendaagse oplossing zijn de lineaire temperatuurdetectoren – van basic tot optic fiber –, vooral gebruikt in corrosiegevoelige omgevingen, of omgevingen waar een klassieke puntdetector geen oplossing biedt", aldus Steenbeke.

Draadloze detectie & cameradetectie

Rond een andere mogelijkheid, draadloze branddetectie, is er momenteel een werkgroep actief. "Draadloze branddetectie is geen mirakeloplossing. Draadloos werken impliceert onder meer radiofrequentie, golflengtes en bandbreedtes... Het is niet mogelijk om signalen over een onbeperkte afstand doorheen muren en obstakels te sturen. Draadloze detectie biedt enkel een oplossing in omgevingen waar klassieke bekabeling niet aan de orde is, bijvoorbeeld bij historisch waardevolle gebouwen. Last but not least is er cameradetectie, wellicht de toekomst voor branddetectie. Cameradetectie zorgt voor een perfect beeld van de in een grote ruimte aanwezige rookdeeltjes", aldus Steenbeke. De slotboodschap van de voorzitter van AFT Detectie was drieledig. "Een goede brandalarminstallateur is een gecertificeerde installateur die de vereiste knowhow in huis heeft, een problem solver die het juiste product goed toepast op de juiste plaats. Branddetectie vandaag gaat niet enkel over technologie maar is ook een kwestie van risicoanalyse en operationele procedures." Hij lanceerde ook een oproep aan de verzekeringswereld om bedrijven die branddetectiesystemen installeren op de werkvloer, op een of andere manier financieel te ondersteunen.

Verfijning van componenten en systemen

François Asselman van Belgian Fire Sprinkler Network, en administrateur van ANPI, had het over nieuwe, specifieke ontwikkelingen inzake automatische blusinstallaties. "In eerste instantie is er de verfijning van componenten en systemen. Denk bijvoorbeeld aan de differentiatie in functie van de te beveiligen risico's en brandbelasting, de reactietijd bij een sprinkler (68°C) die nu nog 7 (vroeger 32) seconden bedraagt, en de nieuwe generatie sprinklers, met onder meer intelligente sprinklersystemen en de combinatie van detectieprincipes en intelligente triggering. Ook op het vlak van engineering en realisatie zijn er nieuwe ontwikkelingen zoals CAD-design, prefabricage van buisleidingen in de fabriek, en het gebruik van klemkoppelingen bij de montage."

"Een Rook- en Warmte Afvoer(RWA)-installatie kan bijdragen tot het verbeteren en garanderen van het totale brandbeveiligingsniveau, met de nadruk op een veiliger evacuatie en ondersteuning tijdens de interventie van de brandweer", was de boodschap van Robby De Roeck (fire safety engineer bij Brakel Aero nv en bestuurslid van FiroProNet vzw).

Door Philip Declercq

www.anpi.be

DAITEM DRAADLOZE ALARMSYSTEMEN

100 % DRAADLOOS

INCERT

VOCAL CENTRALE

5 JAAR AUTONOMIE (BATTERIJEN)

BEVEILIGDE COMMUNICATIE

AANSTUURBAAR VIA DE APP e-DAITEM

5 JAAR GARANTIE



Dahua Technology introduceert thermische camera voor de commerciële markt

Tot nu toe zijn de meeste thermische camera's in de industriële markt nog steeds erg omvangrijk en boven de betaalbare grens van de meeste commerciële projecten. Dahua lanceert een intuïtieve thermische mini-hybride bullet camera – DH-TPC-BF2120. Dit met mini-grootte, dual-channel spectrum, intelligente functies en betaalbare prijs.

<http://www.dahuasecurity.com>



Panasonic stelt nieuw IP-gebaseerd video-intercomsysteem voor

Panasonic introduceert een nieuw, volledig IP-gebaseerd video-intercomsysteem dat inspeelt op de toenemende integratie van toepassingen in gebouw-beheersystemen. Op het nieuwe systeem, de VL-VN1900, kan een groot aantal apparaten zoals CCTV-camera's, SIP-telefoons en netwerkvideorecorders aangesloten worden. Via Power over Ethernet kan het systeem met één kabel worden aangesloten om zo installaties eenvoudiger en goedkoper te maken. Met een extra controlbox ondersteunt het systeem tot 2000 SIP-apparaten met standaard-PoE.

<http://nl.business.panasonic.be>



Axis verbetert Zipstream en omarmt daarmee nieuwe 360° camera's en 4K-resolutie

Axis maakt bekend dat het zijn Zipstream-compressietechnologie heeft verbeterd als antwoord op de hogere eisen die gesteld worden aan gegevensstreaming en -opslag bij 360 graden panoramische camera's en camera's met 4K-resolutie. Zipstream zorgt ervoor dat belangrijke forensische details in het beeldmateriaal bewaard blijven, terwijl er gemiddeld 50 procent of meer aan bandbreedte en opslagruimte bespaard wordt. Axis introduceert ook twee nieuwe domes met de verbeterde Zipstream-technologie en levert daarmee op kosteneffectieve wijze camerabeelden van 360 graden in hoge resolutie.

www.axis.com

ARAS Security breidt CamTech assortiment uit met VMS

ARAS introduceert het CamTech VMS, dat vanwege de modulaire opbouw perfect meegaat in de filosofie 'altijd een oplossing op maat'. Van PTZ-sturing tot fisheye-dewarping en van gezicht- tot kentekenherkenning, het nieuwe CamTech VMS is een schaalbaar, betrouwbaar, krachtig en flexibel Video Management Systeem. Door toepassing van geavanceerde Video Analytics bespaart u op beheerkosten. Naast videobeelden is het namelijk ook mogelijk om op basis van meta-data te zoeken: de juiste beelden nog sneller vinden maakt adequaat opvolgen efficiënter en waardevoller. Daarnaast is het dankzij het open karakter mogelijk om 4.000 verschillende IP-camera's aan te sluiten van meer dan 130 merken.

www.aras.nl



Full HD surveillance oplossing over coax

De vraag naar een analoge camera-observatie oplossing blijft nog steeds bestaan. IDIS biedt met DirectCX™ een geavanceerde analoge FULL HD oplossing gebaseerd op HD-TVI technologie. De voordelen van DirectCX™: een ideale oplossing voor de vervangingsmarkt met behoud van bestaande coaxbekabeling, alleen uitwisselen van camera's en hard-diskrecorder; real-time Full HD beeldkwaliteit (30ips@1080p) zonder kwaliteitsverlies en vertraging, OSD camera menu-instellingen via de coax; kabelafstanden tot 500 mtr.

www.idisglobal.com

2de generatie Paxton lezers met Genuine HID Technology

In 2017 heeft Paxton de Genuine HID Technology™ aan de meerderheid van de Proximity lezers toegevoegd. Vanaf nu kunt u de HID functionaliteit inschakelen door het gebruik van de HID Proximity Licentie kaart. Via de los verkrijgbare HID licentiekaart is het mogelijk om HID™ te activeren op Paxton Proximity lezers. De licentie kaarten zijn beschikbaar met 1, 5 of 10 licenties. Wanneer de licentiekaart aangeboden wordt op compatibele lezers wordt de HID™ Prox® 125 kHz functionaliteit geactiveerd, naast de geactiveerde HID™ Prox® 125 kHz functionaliteit, behoudt de lezer de mogelijkheid om Paxton en EM kaarten en tags te lezen.

<http://bit.ly/2sRSBWY>



DE NIEUWE, STILLE RECORDERS VAN SEFICA

Onvif-compatibel en nummerplaatherkenning



Sefica streeft de ontwikkeling van zijn eigen gamma NVR's na met de introductie van het gamma Imagebox. Deze recorders zonder ventilator (Passive Cooling Technology) en met Onvif-compatibiliteit zijn beschikbaar in 2 versies:

IBX-09: een 9-kanaals NVR met IP, compatibel met Windows en MAC. De geïntegreerde bewegingsdetectie en Smart Motion Search kunnen geconfigureerd worden op elk type camera.

IBX-02-ANPR: een NVR voor 2 camera's met geïntegreerde nummerplaatherkenning (ANPR). Met de automatische synchronisatie tussen de ANPR en de ImageBox softwares, vindt u snel de gewenste nummerplaat terug.

Sefica.
secure. protect. prevent.

Sefica is een exclusief kwaliteitsmerk van



RAS bvba
Brugsesteenweg 257, 8500 Kortrijk
T +32(0)56 36 37 40
contact@sefica.be
www.sefica.be



OKTOPUS WAAKT OVER UW VEILIGHEID

PERSONEN • GEBOUWEN • INDUSTRIËLE PROCESSEN • LOKALISEREN VAN VOERTUIGEN EN ANDERE MOBIELE OBJECTEN



TELEBEWAKING: UW VEILIGHEIDSGARANTIE

- Streng geselecteerde medewerkers
- Hoogtechnologische infrastructuur
- Op maat ontwikkelde procedures
- Soepele administratieve en operationele diensten
- Morele, technische en functionele garanties
- Diensten 24u/24 operationeel



Erkend door de Federale overheidsdienst Binnenlandse Zaken
en de verzekeringsmaatschappijen (ASSURALIA).
Certificatie: ISO 9001-2000

Louizalaan 331
1050 Brussel
Tel.: 32-2-542 05 42
Fax: 32-2-542 05 43
contact@oktopus.com

www.oktopus.com