

TOP SECURITY

SECURITY, BUILDING & RISK MANAGEMENT

143 | JUI/AOÛT/SEP 2017

avec la
participation d'

alia



**Biométrie : les veines de la paume
de la main ne mentent pas**

Wisenet X series



La gamme Wisenet X de Hanwha Techwin (anciennement Samsung) a le plus puissant processeur jamais intégré à une gamme complète de caméras. Le processeur Wisenet 5 utilise une toute nouvelle architecture qui lui permet de traiter plus rapidement les données, et de vous assurer les meilleures performances vidéo quand vous en avez besoin. L'énorme puissance de traitement du processeur Wisenet X donne aux utilisateurs la possibilité d'exécuter plusieurs applications tierces d'analyse spécialisée. Wisenet 5 offre une qualité d'image élevée sans précédent avec des caractéristiques uniques.

150dB WDR en full HD • Nombreuses fonctions analytiques
Sensibilité supérieure à la lumière

 Hanwha Techwin | **SAMSUNG**

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

 **smartSD**
Smart Security Distribution

Colofon

TOP Security. Revue spécialisée destinée au secteur de sécurité. Envoyé gratuitement aux responsables chefs de sécurité dans les entreprises, les commerces, les banques; entreprises d'installations de systèmes de sécurité, télésurveilleurs; fabricants/distributeurs; sociétés de gardiennage; Facility Managers, gestionnaires de building; prescripteurs assureurs, architectes, bureaux d'étude et autorités officielles.

PERIODICITE
Trimestrielle

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

EQUIPE REDACTIONNELLE
Philip Declercq
Philip Vandenbon
Sammy Soetaert

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

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

EDITEUR RESPONSABLE
Filip Cossement
Boulevard des Canadiens 118
7711 Dottignies

CHANGEMENT D'ADRESSE
info@topsecurity.be

Version française: sur simple demande

Rien de cette édition ne peut être reproduit ou/et publié par impression, photocopie, microfilm ou tout autre moyen sans accord écrit préalable de l'éditeur. Les articles sont publiés sous la responsabilité de l'auteur.



MEMBRE DE L'UNION DES EDITEURS
DE LA PRESSE PERIODIQUE

www.topsecurity.be

04 NEWS

VLAAMSE SLOTENMAKERSUNIE

12 Rejet de l'autorisation du serrurier : OVLD, enfin l'explication

INTERVIEW OLIVIER DEMOULIN – NOUVEAU PRÉSIDENT D'ALIA SECURITY

17 « Notre profession va complètement changer dans les cinq prochaines années »

POINT DE VUE

21 Planification dynamique de la sécurité : avant tout, du bon sens

REPORTAGE

24 AnB-Rimex élargit sa gamme de solutions de sécurité intégrées

26 Paxton en tournée avec un logiciel mis à jour et un nouveau panneau

29 Hikshow : un avenir qui fait la part belle à l'innovation

33 Biométrie : les veines de la paume de la main ne mentent pas

36 Bosch Talks 2017 met principalement l'accent sur la sécurité

41 Attention, les voisins regardent (peut-être)

EVENT

44 SST2017 : Solutions de sécurité avancées dans l'Onderzeebootloods

47 Un demi-siècle de prévention incendie

50 PRODUCT NEWS

Paxton remporte l'IF Design award avec son écran tactile Net2 Entry Touch

Le nouvel écran tactile Net2 Entry Touch Paneel est mis à l'honneur cette année dans la catégorie product design. Cet écran a remporté le design award pour ses techniques et ses matériaux novateurs. Le design a aussi été très apprécié. Le jury fut éloquent sur les matériaux comme l'écran, la commande et l'installation aisée.

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



Le salon professionnel New Security désormais également aux Pays-Bas !

Suite au succès de New Security cette année à Louvain, il a été décidé d'organiser également cet événement aux Pays-Bas. C'est le site Expo Houten, près de Utrecht, qui a été choisi pour accueillir la foire. Houten est facilement accessible et possède toutes les facilités. La formule sera identique à la version belge de New Security. Le salon durera deux jours et se déroulera aussi tous les deux ans. Les exposants sont des importateurs, des fabricants et des grossistes. Les visiteurs sont des installateurs et des clients finaux professionnels. New Security NL se tiendra les 5 et 6 avril 2018. New Security BE est de son côté planifié les 14 et 15 février 2019. New Security devient ainsi une organisation Benelux alternant entre la Belgique et les Pays-Bas. Par ce biais, nous espérons répondre aux souhaits des exposants et des visiteurs. Pour toutes les informations pratiques, prière de se rendre sur

🔗 www.new-security.nl

Dahua Europe propose de l'information produit gratuitement via Icecat

Une large sélection de produits de Dahua est dès à présent reprise dans le catalogue Open Icecat. Suite à la collaboration avec Icecat, Dahua rend ses données de produits disponibles en ligne pour tous les channel partners qui peuvent ainsi facilement et rapidement intégrer cette information dans leurs plateformes e-commerce. Cette solution est gratuite pour les channel partners qui peuvent ainsi garder leurs gammes de produits Dahua à jour, y compris les numéros d'article, les spécifications, les textes de marketing et les illustrations. L'investissement dans Icecat offre aux channel partners divers avantages comme une plus grande efficacité, un gain de temps, une meilleure visibilité en ligne et des ventes meilleures. Le contenu est multilingue et optimisé pour une comparaison aisée des produits. « Grâce à la connexion avec Icecat, nous pouvons offrir un service encore meilleur à nos clients et leur proposer à tout moment de la journée des données digitales les plus actuelles et complètes de tous nos produits. Nous sommes convaincus que cette collaboration va nous aider et aider nos channel partners à atteindre les objectifs commerciaux dans les prochaines années », a déclaré Martijn Peeters (marketing manager Dahua Benelux).

🔗 www.dahuabenelux.com/nl/

Nextel remporte le Belgian HR Award

Lors de la remise des Belgian HR Awards par Trends et Kanaal Z, Nextel a remporté le HR Award for Internal Communication. À l'unanimité, le jury a désigné la campagne « NForce Eachother » comme gagnante de ce titre très convoité. L'Award est assorti d'un chèque de 33.500 euros. La campagne lauréate « NForce Eachother » s'inscrit dans le cadre du plan NForce 2020, avec lequel Nextel concrétisera, d'ici 2020, un certain nombre d'objectifs ambitieux. La fluidité de la collaboration interne est essentielle dans ce processus. C'est pourquoi entre 2016 et 2018, chaque département de Nextel a l'opportunité de se mettre en avant, pendant une semaine, au sein de l'entreprise. Les équipes apprennent ainsi à mieux se connaître : qui sont-elles et qu'attendent-elles des autres départements ? Tout cela de manière ludique, car il est plus agréable de collaborer dans une ambiance agréable. L'intégralité de la campagne est une initiative de, pour et par les collègues de Nextel, ce qui a impressionné le jury.

🔗 www.nextel.be



HIKVISION



H.265+ EFFICACITÉ ÉPOUSTOUFLANTE

FAIBLE BANDE PASSANTE

Hikvision hisse le monde de la vidéosurveillance à un niveau sans précédent avec son codec H.265+ En mode Full HD, le H.265+ utilise moins de 20% de bande passante que le H.264, permettant ainsi des flux en direct avec une qualité inégalée.

CAPACITÉ MINIMALE DE STOCKAGE

H.265+ est également largement supérieur à celui de ces prédécesseurs en termes de stockage. Quelque soit l'environnement réseau ou les applications spécifiques, H.265+ réduit l'espace de stockage requis de plus de 80%.

Pour résumé, Le H.265+ vous permet de commencer à voir les choses en grand : vous pouvez maintenant enregistrer des images avec des résolutions incroyablement élevées tout en minimisant la capacité de stockage requise, ce qui fait du codec H.265+ la solution parfaite pour votre système de surveillance 24/24.

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

www.hikvision.com

Hikvision lance la solution Access Control en Europe

Hikvision a lancé sa nouvelle solution Access Control sur le marché européen. Cette solution offre aux clients un environnement sûr via un accès sécurisé, grâce à une solution complète de bout en bout – des caméras aux contrôleurs, des relais d'alarme à l'architecture IP, des serrures de porte aux DVR's. Cette solution assure une intégration complète avec les interphones et classes d'intrusion Hikvision via le logiciel iVMS. Cela permet aux clients de commander les produits à distance via l'appli mobile Hik-Connect. Avec cette solution, les clients ont un contrôle total de l'accès au bâtiment, aux pièces et aux endroits sensibles. Cela leur permet de garder une présence, tandis que les actifs sont protégés. La solution et ses nombreuses options est très flexible. Plusieurs lecteurs de cartes sont par exemple disponibles. Il y a aussi les fonctions à mot de passe multi-door interlock, multi-card, anti-pass back et super card/super, et jusqu'à 100.000 cartes et 30.000 événements peuvent être traités.

🌐 www.hikvision.com/europe



La VEB fête ses 30 ans d'existence

La Vereniging Erkende Beveiligingsbedrijven est en fête. L'association sectorielle existe depuis 30 ans et a inauguré un bureau flambant neuf à Woerden le 8 juin dernier. C'est donc depuis le 6 août 1987 que la VEB défend les intérêts de ses membres dans le sens le plus large du terme. Avec ses quelques 600 membres, l'association est un partenaire important au sein du secteur néerlandais de la sécurité. La mission consiste à garantir la sécurité de manière optimale aux Pays-Bas, notamment en harmonisant toutes les mesures qui s'imposent. Plusieurs entreprises de sécurité aux disciplines diverses ont rejoint la VEB. La VEB estime qu'il est important que les particuliers et les entrepreneurs sachent en quoi consiste la qualité et la sécurité. Une campagne de promotion à grande échelle a dès lors été lancée. Celle-ci souligne l'intérêt d'une fiabilité éprouvée, de la garantie de qualité et des connaissances professionnelles. Par cette forme de sensibilisation, l'association aide les citoyens à se défendre et à lutter contre la criminalité.

🌐 www.veb.nl

La Commission vie privée publie sa brochure et son rapport d'activités numérique 2016

La Commission vie privée publie son rapport annuel pour l'exercice 2016. Au cours de l'année écoulée, le fonctionnement journalier de la Commission vie privée a été marqué par les travaux préparatoires relatifs au RGPD. Mais l'ordre du jour comportait également de gros dossiers d'avis sur des thèmes d'actualité comme le cloud computing, les mesures antiterroristes et la zone de basses émissions de la Ville d'Anvers. La victoire en référé contre Facebook a été annulée en degré d'appel en 2016. En raison notamment du RGPD, la Commission vie privée voit à nouveau le nombre de dossiers de fond augmenter. La plate-forme pour les jeunes "Je décide" a fait peau neuve et a remporté le tout premier M-Award de Mediawijis pour sa campagne sur le "Droit à l'image".

🌐 www.privacycommission.be

Eric Vermaas, nouveau directeur de Trigion Brand en Beveiligingstechniek

Erik Vermaas est depuis ce 5 juin le nouveau directeur de Trigion Brand en Beveiligingstechniek. Cette business unit dispose désormais d'un directeur qui, par ses connaissances et son expérience, va contribuer à la composante technologique au sein de l'offre intégrée de Trigion. Après avoir terminé avec succès ses études en Electrical Engineering (BSc) et Business Administration (MBA), Eric Vermaas a acquis une large expérience chez Siemens. Après y avoir occupé divers postes, il était ces dernières années responsable de la gestion et de la transformation de plusieurs domaines d'activités de l'entreprise dans les domaines des télécoms, la prévention incendie, la sécurité et le confort. Ce bagage constitue une base idéale pour la poursuite du déploiement de l'offre intégrée avec laquelle Trigion réalise la sécurité. L'organisation propose des solutions intégrées où la prestation de service physique est combinée à la technique et à l'intelligence (données), autant de domaines familiers pour le nouveau directeur.

🌐 www.trigion.nl



dahua
TECHNOLOGY

Environ **1.25** millions de personnes meurent chaque année des suites d'un accident de la route. Les accidents de la route sont la principale cause de décès chez les jeunes âgés de **15 à 29** ans. Si on ne réagit pas, les accidents de la route risquent de devenir la 7ème cause de mortalité d'ici **2030**.

— Source Organisation Mondiale de la Santé

Derrière les efforts mondiaux visant à générer un trafic plus sûr, Dahua fournit une gamme exhaustive de solutions permettant de prévenir les tragédies sur la route..

UN MONDE MEILLEUR ET PLUS SÛR

Dahua Intelligent Transportation Solution (ITS)



ANPR

Enregistre l'image du véhicule et reconnaît le numéro de plaque de l'événement à la vitesse de 180 km/h



Mesure de la vitesse

Détecte et enregistre le véhicule en excès de vitesse avec la classification du véhicule correspondante et le n° de voie par l'intégration d'un radar et d'une caméra



Application de la lumière rouge

Détecte et enregistre le piéton rouge avec le tracking ou la camera ITS et le radar 3D



Surveillance mobile

Veille à la sécurité de conduite, simplifie et gère le travail de répartition des véhicules

CE FC CCC UL ROHS ISO 9001:2000



DAHUA TECHNOLOGY EUROPE B.V.

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

Crowd Monitoring

License plate Recognition

Face Recognition

People Counting

Suspect search

Abandoned Object Detection

Loud sound Detection

Heat map

Tracking

CamTech VMS

Donnez de l'intelligence à n'importe quelle caméra avec CamTech VMS

La nouvelle plateforme CamTech VMS d'ARAS Security rend plus de 4.000 caméras de 130 marques plus intelligentes. Chaque image, même prise avec des caméras anciennes, est utilisable pour une analyse approfondie des images prises et celles en temps réel, et pour de nombreuses autres possibilités comme la reconnaissance faciale et de signes particuliers. Profitez des possibilités, de la stabilité, de la force et de la convivialité d'un leader de marché et de coûts de licence uniques.

Les avantages de CamTech VMS

- Investissement unique en licences, donc pas de coûts supplémentaires annuels cachés.
- D'énormes quantités de données sont filtrées pour obtenir un résultat clair.
- Gestion efficace et conviviale des images prises et celles en temps réel
- Intégration sélectionnée de CamTech NXT et des enregistreurs UNV
- Support ARAS garanti

CamTech VMS est une marque de ARAS Security.

Allez sur www.aras.be ou appelez le 03 825 16 26 pour obtenir de la documentation et de l'information sur CamTech VMS

Une démonstration ?

Nous viendrons chez vous avec notre démo bus et nous vous accueillerons avec plaisir dans notre showroom.



Axis commercialise sa première solution ouverte de contrôle d'accès mobile IP en partenariat avec HID Global

Axis Communications a présenté une nouveauté au salon IFSEC International 2017 du 20 au 22 juin au London ExCeL : l'intégration de Mobile Access de HID Global à son contrôleur de porte réseau AXIS A1001 et à son logiciel AXIS Entry Manager. Concrétisant les attentes des entreprises, cette solution de contrôle d'accès mobile d'Axis et HID simplifie les modalités d'accès des effectifs, dont l'appareil mobile sert d'identifiant pour accéder aux bâtiments, locaux et autres espaces à accès restreint.

www.axis.com



Securitas est prêt à appliquer la nouvelle loi

Securitas réagit positivement à l'approbation finale de la nouvelle loi sur la sécurité privée, au Parlement Fédéral. « La nouvelle législation démontre comment le secteur de la sécurité privée a évolué ces dernières années pour devenir un partenaire à part entière et apprécié de la police. Cela est possible notamment grâce à nos connaissances technologiques. La nouvelle loi représente une étape importante pour une collaboration visant une sécurité intégrale dans toute la société », déclare Koen Colpaert, porte-parole de Securitas. « Nous sommes très satisfaits de la façon dont la législation a été adaptée. Les possibilités dont disposent des sociétés telles que Securitas – la technologie, les compétences de nos collaborateurs et nos connaissances – ont tellement évolué qu'il fallait impérativement moderniser la législation. »

www.securitas.be



INTERNATIONAL TRADE FAIR
WITH CONGRESS

- SAFETY
- SECURITY
- HEALTH AT WORK

17 - 20 OCTOBER 2017
DÜSSELDORF, GERMANY

**PEOPLE
MATTER.**

LES DEFIS NE DISPARAISSENT PAS. ILS CHANGENT.

Le monde du travail est en pleine mutation. Et c'est l'homme au travail qui le ressent le plus: numérisation, nouvelles technologies, flexibilité accrue, énorme intensification au travail. Tenez vous prêts à affronter les nouveaux défis: grâce au salon numéro 1 et ses 1.900 exposants du monde entier.

www.AplusA-online.com

Plus d'informations :
Fairwise BVBA
Hubert Frère-Orbanlaan 213 _ B-9000 Gent
T: 09 245 01 68 _ F: 09 245 01 69
info@fairwise.be





Les effets des attentats: le secteur du gardiennage a enregistré 9,7 % de croissance en 2016

L'Association Professionnelle des Entreprises de Gardiennage (APEG) a enregistré une croissance de 9,7 % en 2016 par rapport à 2015. Il s'agit de la conséquence des attentats qui ont touché la France et la Belgique fin 2015 et en 2016. Le bénéfice opérationnel a légèrement baissé, passant à 3,4 % du chiffre d'affaires, contre 3,5 % en 2015. La demande en surveillance des marchandises et en contrôle des personnes a augmenté. D'autre part, les banques ont moins fait appel aux entreprises de gardiennage. L'effectif des entreprises de gardiennage a augmenté de 10,2 % ou 1297 ETP. Fait remarquable : 31 % des personnes employées en 2016 avaient plus de 45 ans. Effectivement, le secteur du gardiennage est un important employeur et recruteur de travailleurs de plus de 45 ans, dont de nombreuses personnes peu qualifiées. Pour finir, le secteur du gardiennage a activement investi dans de nouvelles technologies, afin de pouvoir employer les personnes de façon plus ciblée.

2016 est l'année au cours de laquelle, d'une part, les activités des entreprises de gardiennage ont été respectées sur une base beaucoup plus large et, d'autre part, le secteur a été reconnu comme partenaire à part entière par les différentes parties de la chaîne de sécurité. «L'an dernier, nous nous sommes rapidement adaptés aux conditions changeantes du marché et de la sécurité», explique Danny Vandormael, Président de l'APEG. «Nos agents se sont montrés très flexibles. Nous avons convaincu par notre professionnalisme et avons bien collaboré avec les services publics de sécurité. Cela a largement profité à notre image. Nous en sommes contents, car nous avons consenti de très importants investissements en maté-

riel et en formation au cours des dernières années. Pour l'Europe, c'est d'ailleurs en Belgique que le profil des agents de gardiennage est le plus soigneusement vérifié», ajoute encore Danny Vandormael.

Chiffre d'affaires + 9,7%, bénéfice en baisse par rapport à 2015

Avec un chiffre d'affaires de 726,6 M€ le secteur a connu, comme l'on s'y attendait, une belle croissance en 2016: +9,7% par rapport aux 662M€ de 2015. Le résultat d'exploitation a évolué un peu moins que proportionnellement dans le même sens, et a atteint +3,4 % du chiffre d'affaires, contre 3,5% en 2015. En 2016, les institutions de formation des

membres de l'APEG ont donné pas moins de 656054 heures de formation, soit 13,7 % de plus qu'en 2015. Cela revient, sur une base annuelle, à 374,9 ETP ou 2,6% de l'effectif total. Cette hausse est due aux pics soudains dans la demande de services de gardiennage après les attentats.

«La hausse inattendue de la demande après le 22 mars a entraîné des frais plus que proportionnels», souligne Danny Vandormael. «Il faut miser davantage sur le recrutement, la formation et l'achat de matériel supplémentaire; les heures de travail irrégulières et supplémentaires coûtent plus cher; etc. C'est pourquoi le bénéfice a évolué moins que proportionnellement. À l'automne 2016, malgré le niveau de menace persis-

tant à 3, la demande a de nouveau baissé. Il y a probablement eu une certaine accoutumance au niveau de menace, qui était pourtant toujours de 3», conclut Danny Vandormael.

En recourant temporairement à du personnel de gardiennage supplémentaire, les organisations ont clairement voulu donner un sentiment de sécurité accru par le biais de mesures 'visibles'. À plus long terme, une approche plus structurelle sera opportune, comme des agents de gardiennage supplémentaires combinés à plus de ressources et de technologie. L'APEG stimule ses membres à opter pleinement pour de nouvelles technologies innovantes et à les proposer en combinaison avec des agents de gardiennage. La mise à disposition de drones avec opérateurs, par exemple pour des manifestations sportives, en est un exemple.

Hausse inégale par secteur

Le nombre de clients a légèrement augmenté. Ce sont surtout les clients existants qui ont acheté plus de services. Le chiffre d'affaires moyen par client s'élevait à 51 478€ en 2016, contre 48,076€ en 2015. La demande a par exemple connu une hausse significative dans le secteur du transport. Les services fournis aux aéroports, aux ports et aux gares ferroviaires ont augmenté de 43,8%. Ce secteur est désormais le troisième acheteur des membres de l'APEG, après les services publics et l'industrie, avec 16% du chiffre d'affaires total. Cette demande a augmenté en réaction aux attentats qui ont touché la France et la Belgique. Les banques ont acheté 1,1% de services en moins, à cause du nombre d'agences bancaires classiques qui continue à baisser et de la diminution des transports de fonds. La part des banques dans le chiffre d'affaires des membres de l'APEG est passée de 12,4% en 2015 à 11,2% en 2016. Elles sont désormais le quatrième secteur le plus important pour les membres de l'APEG. La distribution (grossistes) est un autre secteur important. La demande y a augmenté de 8,7%, pour atteindre 9,8% du chiffre d'affaires dans le secteur. Il est intéressant de constater que la demande d'agents de gardiennage lors d'événements a augmenté de 30,8 %, pour atteindre 1,8% du chiffre d'affaires total.

En termes d'activités, la majeure partie du chiffre d'affaires vient de la surveillance de marchandises (68,6%). La surveillance et le contrôle de personnes arrivent en deuxième position (18,5%). Il s'agit de la surveillance du comportement des personnes, par exemple pour l'accès à un endroit. Les transports de fonds ferment le trio de tête avec 11,6%.

Le secteur mise activement sur des technologies innovantes combinées à des personnes.

Outre l'engagement de nombreuses personnes supplémentaires, le secteur du gardiennage investit aussi activement dans les nouvelles technologies, afin de pouvoir employer les personnes de façon plus ciblée.

La technologie permettant de travailler avec des opérateurs à distance via des caméras par exemple pour constater le vol en magasin et guider l'agent de gardiennage vers le voleur dans le magasin plutôt que de prévoir la présence physique d'inspecteurs de magasin (agents de gardiennage) en nombre suffisant pour observer le comportement de tous les clients, illustre ce type d'application. D'autres exemples sont les rondes virtuelles à l'aide de caméras, réalisées par des opérateurs dans les centrales de surveillance, ou encore l'ouverture et la fermeture de portes ainsi que l'activation et la désactivation de systèmes d'alarme à distance.

L'utilisation des rayons X pour contrôler les sacs des visiteurs est une autre application. Jusqu'il y a peu, cette technologie était uniquement utilisée dans les aéroports. Aujourd'hui, elle est de plus en plus courante, par exemple dans les tribunaux. Le secteur du gardiennage fournit une solution complète, comprenant la technologie et les personnes.

Activement à la recherche des plus de 50 ans

Le secteur du gardiennage est un secteur axé sur l'humain. Pas moins de 1297 ETP, soit 10,2%, sont venus renforcer les rangs des membres de l'APEG en 2016. En ce qui concerne l'emploi en 2016, 16,8% des collaborateurs sont dans la catégorie d'âge 18-25 ans, 52% avaient entre 26 et 45 ans, et 31,1% plus de 45 ans. En partant du principe que les membres de l'APEG représentent plus de 90% de

l'emploi dans le secteur, cela signifie qu'au moins 1441 ETP sont venus grossir les rangs de tout le secteur du gardiennage.

«Nous nous mettons activement en quête de personnes de plus de 45 et 50 ans, que nous occupons en combinaison avec des plus jeunes», explique encore Danny Vandormael. «Le but est toujours d'employer des gens rapides et bons dans l'action physique avec d'autres personnes plus posées. Nous nous efforçons d'atteindre un bon équilibre entre les groupes d'âge et entre rapidité et maturité. Les plus de 50 ans qui ne peuvent par exemple plus exercer leur métier en raison de problèmes physiques trouvent ainsi une deuxième opportunité de carrière chez nous.»

Autre fait intéressant: 83% des personnes employées ont uniquement un diplôme de l'enseignement secondaire. 10,1% des personnes n'ont qu'un diplôme issu de l'école primaire. Il y a une légère hausse du nombre de travailleurs avec au moins un diplôme de l'enseignement secondaire (89,9%) par rapport aux travailleurs ayant uniquement un diplôme de l'enseignement primaire.

En 2016, 15,3% des personnes occupées par les membres de l'APEG étaient des femmes, soit 0,3 % de plus que l'année précédente.

www.apeg-bvbo.be



Danny Vandormael (Président de l'APEG) : « Nous avons convaincu par notre professionnalisme et avons bien collaboré avec les services publics de sécurité. »



Rejet de l'autorisation du serrurier : OVLD, enfin l'explication

Le mystère du Open VLD : pourquoi ne souhaite-t-il pas protéger les citoyens contre les serruriers-escrocs, en introduisant une autorisation dans la Loi sur la sécurité privée ? Chapeau au « Meldpunt Malafide Slotenmakers » (le Point de contact Serruriers Malhonnêtes néerlandophone): il est parvenu à recevoir la position du Open VLD... une heure après l'approbation définitive de la loi. (Mail de Diederik Pauwelyn (Coordination des Matières, Management opérationnel du Open VLD) du 8 juin 2017, à relire sur la page Facebook du point de contact.) De fait, la loi a été approuvée ce 8 juin sans cette autorisation, le CD&V ayant laissé s'étioiler discrètement son projet de loi avec ce même objet à la Commission de l'Intérieur. Un amendement ultime par lequel le sp.a, le PS et le cdH, avec l'appui de l'opposition tout entière, avaient récupéré le projet CD&V, a été rejeté sans pitié par les partis au gouvernement, CD&V inclus. Le Open VLD a réussi son coup avec ses arguments. Qu'est-ce qu'ils étaient ?

Voici un an, un parlementaire du CD&V défendait notre projet encore avec beaucoup de conviction, introduisant même un projet de loi. Une indisposition lors des réunions cruciales de la commission l'a empêché de défendre son projet, et malgré la confirmation que ses collègues du CD&V allaient faire le nécessaire, ils ont quand-même perdu de vue et laissé expirer le projet. Le jeudi 8 juin, en séance plénière, c'est tout son groupe CD&V qui a purement et simplement voté *contre* les amendements qui réintroduisaient au débat les propos de son texte. Mais pourquoi la N-VA et le MR se sont-ils joints au CD&V ? Ils n'avaient pourtant rien contre notre proposition ? C'est tout simplement que le Open VLD, qui siège lui aussi au gouvernement, s'est opposé à une autorisation pour les serruriers. Par conséquent, le gouvernement n'a évidemment

pas pu inclure cette autorisation dans la proposition de loi. Pourtant, les parties au gouvernement avaient aussi convenu de soumettre la question à la discussion au parlement. Il n'est pas normal, alors, que tous ces partis au gouvernement, y compris ceux qui nous soutenaient initialement – enterrent l'affaire au parlement et décident d'exclure toute discussion à ce sujet. Parlons dès lors de la motivation du Open VLD. Lorsque celle-ci a été la seule motivation pour faire rejeter par le gouvernement notre autorisation, elle doit être, sans doute, assez pertinente.

1) Selon le Open VLD, les « serruriers malhonnêtes font naître des risques pour la sécurité et une concurrence déloyale ».

Des propos étranges pour le Open VLD, puisque aucun de ces raisons est réellement important. Les escrocs ne créent pas vraiment des risques pour la sécurité. Ces

risques constituent plutôt, en revanche, une raison d'adopter l'autorisation des serruriers, qui permet de mieux garantir la confidentialité. Il n'y a pas non plus question d'une concurrence déloyale parce que les serruriers malhonnêtes ne suivraient pas les mêmes règles. En effet, il n'existe pas de règles pour les serruriers en général, tout simplement. Et à supposer qu'il y en ait, les escrocs ne les respecteraient pas, en l'absence de contrôles. Apparemment, le Open VLD tente ici de détourner l'attention vers des problèmes dont il prétend avoir la solution. Mais il refuse de voir l'évidence : il s'agit tout simplement de pratiques criminelles, où des victimes sont menés jusqu'à ces exploiters par le biais de sites Internet. Cela ne peut être toléré; la seule solution efficace consiste en une autorisation obligatoire avec contrôles et sanctions à la clé, et qui s'étende égale-

ment aux intermédiaires comme les sites en question.

2) « Oui, mais une autorisation obligatoire entraîne des complications : prime de lancement, rétributions... » objecte le OVLD

Voilà un bien curieux argument – il n'y a pas de problèmes pour les installateurs de systèmes d'alarme, de vidéosurveillance, ou pour les nombreuses petites et grandes entreprises de gardiennage, services de gardiennage interne et consultants en sécurité qui représentent quelque 2000 entreprises et plus de 20.000 emplois. Par la prime de lancement, on entend les frais uniques de dossier (1000 euros pour les installateurs de systèmes d'alarme), et par les rétributions, le montant annuel qu'une entreprise autorisée est tenue de verser (forfait de 500 euros par autorisation, plus 135 euros par travailleur). Mais pour le screening de sécurité que le Open VLD propose, il faut également verser tous les 5 ans une rétribution, qui monte jusqu'à 250 euros (et qui n'a pas été revue depuis des années). Rien n'empêche d'ailleurs que le gouvernement adapte ces coûts à la capacité des entreprises. Il existe d'autres charges dont l'on ne parle pas, et qui sont précisément indispensables. Ce n'est pas un luxe que les serruriers conservent les dossiers de leurs clients, les clés et les doubles d'une manière sécurisée et sous l'anonymat. D'autres charges, comme la mention du numéro d'autorisation sur tous les documents et sur le véhicule, font simplement partie d'une activité autorisée. Il est d'autant plus étonnant que le Open VLD soulève le problème de ces charges, puisque c'est elle qui propose d'introduire un screening de sécurité plus lourd et chronophage pour le serrurier. Quel est le véritable objectif du Open VLD ?

3) « Nous risquons l'engrenage après l'intégration dans la loi, et d'en arriver à demander des contrôles d'identité, la détention d'armes, l'assistance de la police », affirme le Open VLD.

Il est extraordinaire de voir comment le Open VLD recycle le risque d'engrenage, risque pour lequel il doit lui-même se démenier comme un beau diable à chaque élargissement des tâches du secteur du gardiennage. Les serruriers demandent le strict nécessaire, pas plus. Dans notre proposition, nous ne faisons pas mystère du fait que des bonnes raisons justifient au bout du compte, *qu'il faut* permettre – et obliger – les serruriers à contrôler l'identité

et les droits d'accès des personnes qui leur demandent d'urgence d'ouvrir une porte. À défaut, ils continuerons à ouvrir la porte pour des cambrioleurs, des ex-partenaires ou des harceleurs. L'assistance de la police n'est nécessaire que dans des interventions à risque, alors que la détention d'armes est totalement *hors question*.

4) « Il ne faut pas négliger le risque de retombées négatives, par exemple pour les installateurs de portes », poursuit le Open VLD.

C'est précisément ce qu'excluait notre proposition. Elle prévoyait que les menuisiers ou les placeurs de portes peuvent continuer à installer des serrures normales (comme tout un chacun). En plus, tout fabricant ou menuisier qui réalise des portes ou des fenêtres pourrait continuer à livrer ses produits avec des serrures de sécurité déjà placées, comme cela se passe déjà régulièrement aujourd'hui. Aucun des arguments du Open VLD ne résiste, dès lors, à la critique.

Quelle alternative le Open VLD propose-t-il ?

Le Open VLD veut « élargir la loi sur les screenings de sécurité aux serruriers. » Comme on l'a vu, ces screenings sont plus stricts que les contrôles prévus dans la Loi sur la sécurité privée, alors qu'ils n'examinent ni les connaissances professionnelles ni le respect des bonnes pratiques commerciales.

Cette loi ne précise pas non plus dans quels cas les screenings seront obligatoires. Une réglementation supplémentaire est donc toujours nécessaire. Enfin, cette réglementation devrait aussi préciser comment le caractère obligatoire du screening doit être respecté, et comment les défaillances sont sanctionnées. Le Open VLD ne présuppose tout de même pas que le couple âgé qui a eu affaire à des escrocs et a dû déboursier 865 euros va demander à ces messieurs leur screening pour les livrer ensuite à la police ? Pour qu'il y ait contrôle, il faut des mécanismes de contrôle, et qu'on le veuille ou non, ceux-ci verront plus facilement le jour dans un contexte existant prévoyant déjà un contrôle et des sanctions. Dans la Loi sur la sécurité privée, ce système est complètement établi et opérationnel. Mais l'avantage d'un screening de sécurité est bien entendu qu'il ne s'agit justement pas d'une *autorisation*. C'est ce que le Open VLD souhaitait. C'est aussi la raison pour

laquelle il se refusait à expliquer ses motivations (sauf une heure après l'approbation définitive de la loi), et n'a jamais été disposé à envisager des alternatives. Ce n'est pas ce qu'on appelle être 'Open'.

La motivation réelle du Open VLD

Le fait qu'un seul parti du gouvernement obtienne, sur la base d'une argumentation si maigre, que tous les autres oublient leurs principes et leurs points de vue suscite bien des questions. En effet, le Open VLD avait d'autres intérêts à défendre, intérêts que l'autorisation des serruriers aurait contrariés. Quand un huissier doit faire ouvrir une porte, par un serrurier bien entendu, un policier doit veiller au bon déroulement de l'opération. Le Open VLD plaide depuis des années pour qu'un agent de gardiennage puisse remplacer le policier dans ce type de situation. Il faut savoir que c'est en principe le policier qui choisit le serrurier. Toutefois, une fois qu'il sera remplacé par un agent de gardiennage, ce dernier tentera d'ouvrir lui-même la porte. Et la nouvelle Loi sur la sécurité privée l'y autorise... *pour autant que ce travail ne soit pas soumis à une autorisation*. Autrement dit : s'il faut une autorisation pour le travail de serrurier, les agents de gardiennage ne pourront pas le reprendre à leur compte. Lorsque les agents de gardiennage pourront intervenir à la place des policiers, les serruriers perdront du travail au profit de personnes dénuées de compétences professionnelles. Cette intervention fera disparaître 100 emplois dans notre secteur.

Épilogue

Il est incompréhensible qu'un parti libéral ouvert même une telle politique, et encore plus que les autres partis au gouvernement l'y aident. Mais pour les serruriers, les choses n'en resteront pas là. L'autorisation reste indispensable, plus que jamais.

Geert Herbots, Conseiller juridique VSU et FNS.

📧 www.vsu.be

📧 www.serrurier.be



**Vlaamse
Slotenmakers
Unie**





ALARM INDUSTRIES ASSOCIATION

Les importateurs et fabricants, membres de ALIA sont à votre disposition pour vos études et approvisionnements en matériel d'alarme, CCTV et contrôle d'accès. Les installateurs de systèmes de sécurité trouvent chez les distributeurs de matériel d'alarme membres de ALIA., les conditions d'une parfaite collaboration: service, dépannage, approvisionnement nouveaux produits, formation, documentation.

Consultez-les.

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

DES DISTRIBUTEURS ET FABRICANTS À VOTRE SERVICE

> 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

Lobeco
FIRE + SECURITY
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

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

RAS
 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
 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

SABELCO
 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
 SMART PEOPLE. IT. SOLUTIONS.
 Boulevard de l'Humanité 233
 B-1620 Drogenbos - Belgium
 T: +32 (0)2 522 76 22
 F: +32 (0)2 524 49 29
 www.milestone.be

IDIS
 One Solution. One Company.
 Boulevard de l'Humanité 233
 B-1620 Drogenbos - Belgium
 T: +32 (0)2 522 76 22
 F: +32 (0)2 524 49 29
 www.idis.be



Olivier Demoulin (53, CEO d'ETAC Alarme Service): « Dans l'avenir, nous vendrons moins de hardware et les solutions de type 'product as a service' vont se généraliser, ce qui va entraîner un changement dans la manière de travailler du vendeur. »

« Notre profession va complètement changer dans les cinq prochaines années »

Olivier Demoulin – Nouveau président d'ALIA Security

Après trois années de présidence à la tête d'ALIA Security, Roger De Grave a passé le flambeau à Olivier Demoulin (53, CEO d'ETAC Alarme Service). Pour le nouveau président, la profession va complètement changer dans les cinq prochaines années. La qualité sera plus que jamais le mot-clé pour relever les défis. Un entretien sur les opportunités et les dangers, ainsi que sur le rôle de l'association professionnelle.

Olivier Demoulin est à la barre d'ETAC Alarme Service, une société active depuis 1949 dans le secteur et membre de Connex Group leader sur le marché de la protection électronique. L'entreprise est spécialisée dans la conception, l'installation, la maintenance et le service après-vente de systèmes de sécurité électronique contre le vol (détection d'intrusion et d'incendie, vidéo-surveillance, contrôle des accès etc...). Jusqu'à présent, plus de 15.000 installations ont été réalisées dans tous les segments du marché (particuliers, entreprises, institutions, ...) et toutes les régions du pays. ETAC ALARME SERVICE emploie une cinquantaine de collaborateurs dont une trentaine techniciens spécialisés. L'entreprise est détentrice du certificat ISO 9001-2015, est Fournisseur breveté de la Cour de Belgique et a réalisé en 2016 un chiffre d'affaires de 7.700.000,00 euros. Olivier Demoulin est engagé dans la vie associative depuis plus de vingt ans. Ces dernières années, il est membre du Comité de Direction d'INCERT et de divers comités au sein d'ALIA Security où sa vision technique et stratégique est très appréciée. D'où vient cet engagement ? « J'estime qu'il est important de défendre les intérêts des petites PME et d'avoir de bons contacts avec les différents acteurs du secteur comme le SPF Intérieur, les compagnies

d'assurances, les organismes de contrôle etc.... Une association professionnelle est une aide au déploiement d'un réseau et c'est une manière de se tenir au courant de ce qu'il se passe dans le secteur. C'est d'ailleurs dans ce contexte que nous sommes actuellement en train de revoir le contenu de notre site web. »

Aiguiser la réflexion stratégique

La Belgique compte environ 950 entreprises de sécurité agréées dont quelques 350 sont certifiées INCERT. Olivier Demoulin : « Au moins la moitié de nos membres sont certifiés. A l'instar de mon prédécesseur Roger De Grave, je veux m'investir dans la qualité. Notre profession va complètement changer dans les cinq prochaines années. Les installateurs ne s'en rendent pas toujours compte. De nombreuses petites PME n'ont pas assez de temps pour se livrer à une réflexion stratégique. C'est à ce niveau que l'association professionnelle peut jouer un rôle. Je perçois aujourd'hui divers mouvements. Il y a la tendance 'Provider to consumer'. Les fabricants proposent de plus en plus leurs solutions directement au client final, ce qui peut représenter un danger pour le distributeur comme pour l'installateur. A côté de cela, il y a l'e-commerce. Deux autres défis sont l'Internet of Things (IoT)

et la manière d'appréhender cela, ainsi que la dématérialisation des systèmes de gestion. Dans l'avenir, nous vendrons moins de hardware et les solutions de type 'product as a service' vont se généraliser, ce qui va entraîner un changement dans la manière de travailler du vendeur. Il y a aussi les aspects juridiques. Le secteur ne s'occupe pas assez de cela. Ce peut être une opportunité mais aussi une menace. Nous voulons donc informer les entreprises via des réunions d'information et des workshops. La formation est aussi à l'agenda. On recherche de plus en plus de techniciens qui ont des compétences IT et il faut investir dans la formation continuée. Dans ce domaine, nous voulons approfondir nos bonnes relations avec les cabinets ministériel et les centres de formations. »

La nouvelle certification INCERT Video

ALIA Security a organisé en juin deux séances d'information sur la nouvelle certification INCERT Video, désormais aussi disponible pour les professionnels de la sécurité. L'association professionnelle est consciente de l'importance de cette certification car elle complète un cadre référentiel qui est vide aujourd'hui, et veut éviter les installations qui ne répondent pas aux attentes souhaitées. Olivier Demoulin : « Nous travaillons là-dessus depuis plus

de quatre ans. La vidéosurveillance est en pleine évolution. A l'heure actuelle, il y a un grand nombre d'acteurs sur le marché dont l'installation de caméras n'est pas l'activité principale. Je pense par exemple aux entreprises informatiques. Certaines solutions semblent peut-être intéressantes sur le plan financier mais le résultat final n'est pas conforme aux attentes des clients. Nous recommandons dès lors aux installateurs professionnels de faire certifier leur entreprise. Tout comme la certification pour l'intrusion, INCERT Video est un excellent label de qualité qui sera de plus en plus demandé. Nous avons remarqué un grand intérêt lors des soirées d'information où quelques 150 inscriptions ont été enregistrées. Notre objectif est qu'une trentaine d'entreprises « early adopters » soient cer-

tifiées d'ici la fin de l'année. Nous sommes conscients du fait que les caméras vont influencer tous les segments de notre profession. Je pense notamment au contrôle d'accès et à la détection d'incendie. »

Nouvelle Loi sécurité privée

La nouvelle Loi sécurité privée a été approuvée le 8 juin et remplace la loi Tobback. Olivier Demoulin : « La collaboration avec les cabinets fut franche et constructive et nous sommes particulièrement satisfaits de la nouvelle loi. Il y a le renforcement du droit à la sous-traitance des services de gardiennage, ce qui permet aux entreprises qui ne sont pas agréées « gardiennage » de pouvoir continuer à proposer ces services en sous-traitance à leurs clients. Nous sommes aussi contents du nouvel agrément

caméra obligatoire ainsi que de l'interdiction de la vente de systèmes d'alarme de porte-à-porte. »

ALIA Security a rencontré les inspecteurs du SPF Intérieur le 18 avril. Le ministère a engagé 25 inspecteurs à des fins de contrôle. Plusieurs points ont été discutés dans un dialogue constructif : la tolérance zéro pour les entreprises qui ne sont pas agréées, ainsi que le contexte et les problématiques typiques du secteur. Olivier Demoulin : « Nous avons informé ces inspecteurs des spécifications de notre secteur et leur avons transmis le message qu'il est important qu'il y ait une force de frappe mais aussi de la compréhension pour la réalité du secteur. »

Par Tilly Baekelandt

www.aliasecurity.be

ALIA Security

ALIA Security est l'association professionnelle belge de l'industrie de la sécurité électronique. Elle représente les installateurs, les fabricants et les distributeurs en matière de détection intrusion, de détection incendie, de contrôle d'accès et de vidéosurveillance. Les membres d'une des associations d'installateurs ELOYA, FEDELEC ou NELECTRA ainsi que les membres de la FEE, la fédération regroupant les fabricants, les importateurs et les distributeurs d'appareils de sécurité électronique sont automatiquement membres d'ALIA Security. ALIA compte environ 600 membres qui, en nombre, forment les deux-tiers des entreprises de sécurité agréées, et représente environ 80% du chiffre d'affaires global sur le marché.

AFIDIS devient FEE Security

Fin de l'année dernière, AFIDIS et FEE ont décidé d'unir leurs forces et de fusionner. Le 14 avril, la FEE est officiellement devenue membre du conseil d'administration d'ALIA et AFIDIS en tant qu'association a été dissoute. Eric Piers a été nommé directeur de la FEE. Les ex-membres d'AFIDIS font désormais partie intégrante de FEE Security, une division spécifiquement fondée suite à la restructuration et qui défend les intérêts des distributeurs et des fabricants au sein d'ALIA. Christophe Depuydt (CEO RAS) est le porte-parole de FEE Security. Il a suivi par le passé les dossiers ALIA pour les distributeurs et les fabricants.

Départ de Yves Ryckaert

Au nom d'ALIA Security, Olivier Demoulin souhaite vivement remercier Yves Ryckaert parti en pension pour ses plus de 25 ans de dévouement envers l'association professionnelle.

Yves Ryckaert a décidé de se retirer de la vie associative. Tout au long de ces années, il a su défendre les intérêts d'ALIA avec beaucoup de conviction et de passion. C'est notamment au niveau des négociations intenses sur l'évolution du cadre légal que son apport a été crucial pour le secteur.



Votre croissance, avec la dernière génération sur ip!



- Exclusivement disponible chez: -

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





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

secure your powerbusiness

Un système UPS sécurise votre système d'alarme à 100%

MCE est votre fournisseur pour systèmes UPS, batteries et systèmes DC. Nous pouvons résoudre vos problèmes rencontrés lors des chutes de courant, des variations de tension ou les protections contre la foudre. Nous disposons également d'une gamme d'alimentations en courant continu ainsi que de transformateurs, adaptés aux exigences des processus d'automatisation dans l'industrie et la construction de machines.

Pour plus d'informations sur nos produits, visitez notre site web www.mce-ups.com ou contactez-nous par e-mail : sales@mce-ups.com



salicru



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

www.mce-ups.com



LA VALEUR AJOUTÉE



- **Intégration**
Home Anywhere - BiBus - MiniDo
- **100% Compatible Dahua**

IVS (Intelligent Video Systems)

NEW!!!



Franchissement de ligne



Disparition /
apparition d'objet



Intrusion dans une zone
délimitée

PRODUCT OF 

Pour plus d'informations: www.anb-rimex.be



Z
chimie & pharma

Chaque année, la chimie et le secteur des sciences de la vie représentent un chiffre d'affaires de près de 63 milliards d'euros, 90.000 emplois, et 3 milliards d'euros d'investissement pour la recherche et le développement. Un tiers de nos exportations proviennent d'entreprises de ces secteurs.

Dans Z Chimie & Pharma, Canal Z présente un acteur capital de l'économie belge.



Z Chimie & Pharma

A partir du 26 février, chaque jeudi
sur Canal Z et sur www.canalz.be

canal Z
POWERED BY 

Planification dynamique de la sécurité : avant tout, du bon sens

Aucun directeur de la sécurité n'ignore l'existence de ces « directives sectorielles » qu'il vaut mieux mettre en oeuvre au plus vite dans les processus d'entreprise. À côté des normes de qualité ISO et des exigences légales, on peut notamment citer la réglementation TAPA¹ pour les entrepôts de stockage, les dispositions FSR² pour la logistique, le code ISPS³ pour les infrastructures portuaires, les directives AEO⁴ pour le commerce international, la norme LME⁵ pour le traitement industriel du métal ou encore le label INCERT⁶ pour les entreprises sensibles aux effractions. Et il y a fort à parier qu'une nouvelle « règle du jeu » viendra s'y ajouter bientôt.

Anticiper de manière dynamique

Sachant que les restrictions et les exigences du prochain certificat indispensable ne sont pas toujours évidentes, le responsable de la sécurité est obligé de faire appel à un consultant en sécurité. Ce spécialiste l'aidera à garantir la conformité de l'entreprise par rapport à la nouvelle norme. Toutefois, comme un bon plan de sécurité n'est jamais qu'un instantané et requiert par conséquent des ajustements empiriques, peut-être quelques mesures supplémentaires suffisent-elles pour satisfaire l'auditeur.

Contrôle direct du risque

Une bonne manière de s'assurer que le plan de sécurité est à jour consiste à dresser l'inventaire des nouveaux risques qui touchent l'entreprise. Et comme la créativité et les ressources des agresseurs évoluent avec la technologie, vous avez tout intérêt à adapter en permanence votre plan de sécurité. Suivre l'actualité consacrée aux incidents de sécurité et aux (ingénieuses) techniques inédites d'effraction permet déjà d'éviter bien des déboires. Cela présuppose toutefois que chaque risque supplémentaire, ou chaque nouvelle directive, se traduise par une solution satisfaisante dans le plan de sécurité.

Identification et évaluation des risques

Pour identifier les risques, on commencera donc par se poser la question suivante : « Qu'est-ce qui doit être protégé contre quoi/qui ? » Après avoir énuméré les risques, on les classera par ordre d'importance. Le risque d'incendie, par

exemple, est plus important que celui de voir un avion s'écraser sur les bâtiments de l'entreprise. Les deux risques existent, et sans doute provoqueraient-ils les mêmes dégâts, mais il est évident que l'incendie pose un risque plus important.

Quantification des risques

Pour subdiviser les risques, les universitaires et les spécialistes ont mis quantité de techniques au point, dont les plus connues sont la Méthode de KINNEY et celle de HAAGSE. En gros, on peut dire que l'importance d'un risque est définie par trois facteurs principaux, à savoir : (1) la probabilité que le risque se concrétise, (2) l'exposition au risque, et (3) la gravité ou les dégâts si le risque vient à se concrétiser.

Risque = impact x fréquence

Une bonne évaluation approximative du risque consiste à multiplier la perte potentielle (impact) par la fréquence du risque. Le résultat fournit une indication objective de l'importance du risque. La quantification est alors un modèle simplifié de chaque risque en soi. Les risques résiduels – il est illusoire de vouloir prévoir tous les risques – peuvent au besoin être assurés. Le meilleur système de détection d'incendie n'exclut pas qu'un incendie puisse se déclarer, pas plus qu'une installation anti-effraction de pointe n'empêchera un travailleur malintentionné de saboter une machine coûteuse. À moins qu'une cyberattaque ne paralyse le réseau de votre entreprise au moyen d'un ransomware. Sans parler d'une fuite de gaz ou d'un incident AMOK. Allez-vous autoriser ces

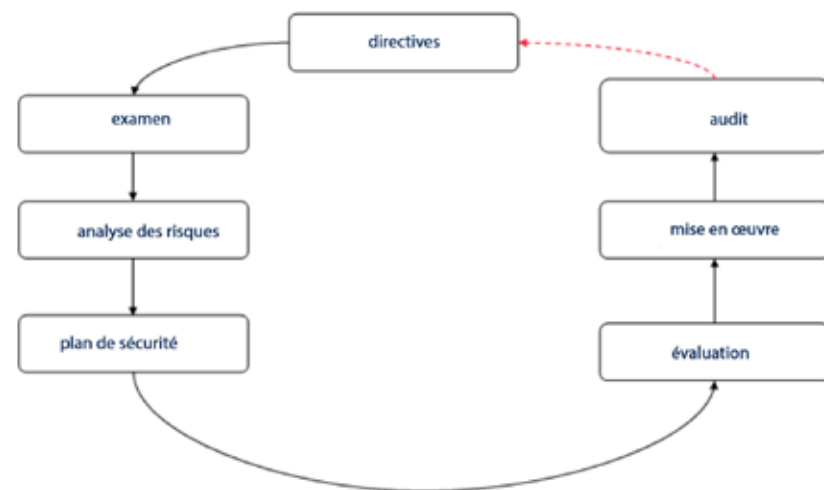
risques, ou faire appel à un assureur pour vous en protéger ?

Plan d'action pour la protection : partir de l'incident

Après avoir évalué la sécurité et dressé l'inventaire des risques, la troisième étape consiste à établir un plan de sécurité. Ce plan décrit en détail les mesures à prendre par le personnel de sécurité. En cas d'incident de sécurité, ce plan sera logiquement relié aux procédures d'urgence et d'évacuation. Le plan d'action définit deux situations : (1) l'incident n'est pas encore survenu, et il convient alors de tout mettre en oeuvre pour l'éviter, ou (2) l'incident est survenu ou est en cours, et il faut prendre les mesures adéquates pour éviter toute aggravation de la situation. Dans les deux cas, cela revient à concevoir des contre-mesures efficaces en imaginant à l'avance ce que pourrait être la situation. Pour cela, on utilisera de préférence la méthode des scénarios.

La méthode des scénarios : que se passerait-il si... ?

La méthode des scénarios a été mise au point par des stratégies militaires ainsi que par Shell, dans le but de pouvoir envisager plusieurs futurs possibles. Cet instrument didactique permet une gestion efficace des risques, et d'aboutir de manière simple à un large éventail de conclusions. La méthode des scénarios part toujours de la question « que se passerait-il si... ? », et donne le coup d'envoi du véritable brainstorming. Pas de formules alambiquées, juste du bon sens.



Comme un bon plan de sécurité n'est jamais qu'un instantané et requiert des ajustements empiriques, peut-être quelques mesures supplémentaires suffisent-elles pour satisfaire l'auditeur.

La méthode des scénarios dans la pratique

La question posée distingue trois groupes cibles : les personnes, les ressources de l'entreprise et l'infrastructure. C'est à ces « cibles » que la méthode est appliquée. Pour info, le système de gestion des risques certifié (ISO-31000) suit dans une large mesure cette piste de réflexion. Voici quelques exemples de méthode des scénarios appliquée à un terminal portuaire de type Seveso⁷.

• Que se passerait-il... Si le local informatique prenait feu ?

• ... Si la canalisation de gaz se rompait accidentellement, en libérant un nuage toxique ?

• ... Si la radio du local de garde était volée ?

• ... Si un visiteur pénétrait dans une zone interdite ?

• ... Si un marin tentait d'introduire en fraude de la drogue à terre ?

• ... Si un membre du personnel était menacé par un visiteur armé d'un couteau ?

• ... Si des bagages non accompagnés étaient retrouvés dans le bâtiment administratif ?

• ... Si une installation de chargement était sabotée, faisant tomber un conteneur ?

• ... Si quelqu'un escaladait la grille et s'enchaînait à un conteneur nucléaire ?

• ... Si un remorqueur éperonnait intentionnellement un navire à quai ?

• ... Si un gazier détourné par des pirates entraînait dans le port et faisait exploser sa cargaison ?

Standard Operating Procedures (SOP) et contre-mesures spéciales

La réponse à toutes ces questions décrit les mesures organisationnelles, architecturales, électroniques et sur le plan des communications nécessaires pour juguler au maximum le risque correspondant. On met au point un plan d'action proactif qui se déploie dès qu'un risque donné se transforme ou pourrait se transformer en incident. Sachant que certains risques requièrent une réaction identique, les contre-mesures peuvent être consignées dans une sorte de memorandum des SOP connu du personnel et des intérimaires. Le plan d'action des procédures et instructions de sécurité spéciale sera de préférence établi par une task force spécialisée

Impact	Déastreux	5	10	15	20	25
	Grave	4	8	12	16	20
	Fort	3	6	9	12	15
	Modéré	2	4	6	8	10
	Petit	1	2	3	4	5
		Très peu probable	Peu probable	Possible	Probable	Très probable

Une bonne évaluation approximative du risque consiste à multiplier la perte potentielle (impact) par la fréquence du risque.

en sécurité... et mis à jour régulièrement. Cette approche est la meilleure garantie pour que votre entreprise obtienne ou conserve le certificat de sécurité lors du prochain audit.

Conscientiser le personnel à la sécurité

Rester conscient en permanence de l'éventualité d'actions malveillantes ou criminelles est une bonne façon de prévenir les incidents. C'est donc la vigilance qui est de rigueur. Un danger imminent ou des agissements suspects doivent être signalés immédiatement puis abordés avec la prudence qui s'impose. Conseil : apprenez aux membres du personnel à identifier et à communiquer (efficacement) un maximum d'informations pertinentes lorsqu'ils repèrent un individu, un véhicule ou un chargement suspect. Il s'agit d'anticiper collectivement les incidents en misant sur les actions proactives (prévention) plutôt que réactives (gestion de crise). Soyez particulièrement attentif à l'éventualité d'embuscades ou de manœuvres de diversion.

Par Philip Vandenberg

1. TAPA : Transported Asset Protection Association
2. FSR : Freight Security Requirements
3. Code ISPS : International Ship and Port facility Security Code (Europe : CE/725/2004)
4. AEO : Authorized Economic Operator
5. LME : London Metal Exchange
6. INCERT : Intrusion Certification
7. SEVESO : évoque la catastrophe industrielle survenue en Italie (1976) et suite à laquelle des directives européennes ont été prises.

IDIS ANPR

Révolution et précision dans la reconnaissance des plaques d'immatriculation

- avec une vue multi-voies
- pour une large gamme de conditions météorologiques
- même lors d'un éclairage limité de la plaque d'immatriculation

IDIS ANPR

la nouvelle norme premium

IDIS ANPR est une nouvelle innovation révolutionnaire d>IDIS.

Cette technologie innovante permet la reconnaissance précise de plaques d'immatriculation sur plusieurs voies. IDIS ANPR offre une implémentation simple et rapide, une facilité d'utilisation, des économies mesurables et encore bien d'autres performances par rapport aux technologies ANPR traditionnelles. C'est le complément parfait de la gamme de produits IDIS.

Principales caractéristiques

- Fiabilité et excellent niveau dans le domaine de la précision dans n'importe quelles conditions
- Véritable vue multi-voies possible
- Large champ de vision et qualité supérieure de l'image
- technologie plug-and-play simple
- Flexibilité dans le positionnement de la caméra et de l'appareillage
- moins complexe, commande et maintenance simples
- intégration transparente avec les plateformes de surveillance IDIS

Principaux avantages

- Technologie tournée vers l'avenir, compatibilité avec la future génération des caméras et des enregistreurs IDIS
- Coût de propriété économique et bas
- Sécurité et protection améliorées
- Surveillance améliorée, images de persuasion de grande qualité
- Efficience opérationnelle par l'automatisation des tâches manuelles
- Plus de rendement des activités commerciales
- Meilleur rapportage et suivi
- Retour sur investissement rapide

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

KX15DT

AnB-Rimex élargit sa gamme de solutions de sécurité intégrées

Lors du salon New Security, l'entreprise AnB-Rimex spécialisée en solutions intégrées dans le domaine de la sécurité intrusion, la domotique, la communication, les systèmes vidéo et le contrôle d'accès, a présenté sa nouvelle gamme Belgian Security Articles (BSA). Avec ces caméras de vidéosurveillance et les accessoires dédiés au marché belge, l'entreprise de Herstal se diversifie dans les solutions de sécurité intégrées.

En ce qui concerne les enregistreurs NVR de la gamme BSA, il y a notamment les séries BSA4 et BSA5 suivant le nombre de caméras à raccorder. La première dispose de la technologie de compression vidéo H.265/H.264, de 200 Mbps de bande passante entrante et d'une résolution de 8 MP pour les caméras IP. La seconde offre une bande passante entrante de 320 Mbps maximum et une résolution de 12 MP pour les caméras IP. Avec le format de compression H265, il est donc possible d'acquérir de la bande passante pour raccorder plus de caméras au réseau et occuper moins d'espace sur le disque dur. « L'enregistreur hybride BSA pour les installations existantes – qui combine plusieurs technologies – est un produit particulier. L'atout est de pouvoir entièrement récupérer le câblage coaxial », explique Ibrahim Tiryaki, Product Manager CCTV d'AnB-Rimex. Tous les enregistreurs NVR sont équipés supportent des caméras IP intégrant l'analyse intelligente de la vidéo (IVC) (IVS).

Un large spectre de caméras

La gamme des caméras BSA comprend un vaste assortiment de systèmes de caméras avec des résolutions variant entre 3 et 12 MP. Il y a notamment les caméras IR Mini Dome Network de 4 MP et 8 MP. Cette dernière est résistante au vandalisme. Le modèle IR Bullet Network Camera (4MP) n'est pas équipé du système de vidéosurveillance intelligent (IVS) mais il s'agit d'une caméra varifocale. La caméra BSA avec 8 MP est quant à elle équipée du système IVS. Au plus la résolution de la caméra est élevée, au plus on opte pour la technologie de compression

vidéo H.265/H.264 afin d'éviter les problèmes avec le câblage existant.

Vidéoparaphonie

Le système de vidéoparaphonie BSA sera également compatible avec la solution plateforme HOME ANYWHERE d'AnB-Rimex. Outre la vidéosurveillance, il y a les kits de vidéophonie (IP ou à 2 fils) avec divers modèles et écrans tactiles. « Le principal avantage est la palette de possibilités d'extension proposées par AnB-Rimex. Une solution de vidéophonie et une solution de caméra IP peuvent être intégrées dans une phase ultérieure, et un système de contrôle d'accès anti-intrusion peut être ajouté. L'objectif est de rassembler le plus de techniques possibles dans une solution de protection intégrée avec la plateforme HOME ANYWHERE », souligne Philippe Stas, General Manager d'AnB-Rimex.

Projets

Les clients-installateurs d'AnB-Rimex ont entretemps réalisé quelques beaux projets

BSA. Ainsi au Pass, le parc d'aventures scientifiques à Frameries (Mons), une cinquantaine de caméras de 3MP ont été connectées aux 10 enregistreurs NVR dispersés sur le site, lesquelles sont gérées par une solution logicielle pour l'ensemble du site. Au Domaine de Wégimont (Province de Liège), plusieurs caméras ANPR (2 MP) de BSA ont été installées. Pour les sites de 2 concessionnaires de Volvo Trucks (Herstal et Namur), le choix s'est porté sur des caméras speed dôme (2 MP) de BSA. Idem pour le terrain de l'entreprise Abelag à Zaventem où douze caméras résistantes au vandalisme (12M & 6 MP) ont été installées.

Par Philip Declercq

Photos : AnB-Rimex

🌐 www.anb-sa.be



Schéma avec les fonctionnalités possibles du système de vidéosurveillance intelligent Dahua-BSA.



Détection intérieure prouvée!

Tranquillité garantie avec sa double technologie.

Installez le KX15DT et vous êtes assurés que l'utilisateur possède la protection parfaite pour son intérieur. Avec une multitude de fonctionnalités lui permettant de s'adapter à son environnement, le KX15DT offre une détection d'intérieure supérieure, idéale pour les installations résidentielles mais aussi commerciales.

f www.facebook.com/pyronix

t @pyronix

in Suivez-nous sur LinkedIn

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 en tournée avec un logiciel mis à jour et un nouveau panneau

Les systèmes de contrôle d'accès du spécialiste Paxton sont entre-temps bien intégrés. Récemment l'entreprise est partie en tournée à travers la Belgique et les Pays-Bas, afin de présenter quelques nouveautés, dont une mise à jour du logiciel Net2. La plate-forme Open source Milestone était également de la partie et montrait comment les solutions Paxton pouvaient y être intégrées. Top Security accompagnait la présentation à Lokeren.

Mise à jour du logiciel Net2 v5.04

Les mises à jour de logiciels sont bien plus qu'un mal nécessaire. Les clients finals sont sans cesse en demande de davantage de fonctionnalités de leurs appareils. Paxton a pris en compte les diverses demandes de ces clients et présente, en conséquence, une importante mise à jour de son logiciel Net2. S'y sont ajoutées, entre autres, des fonctions étendues d'établissement de rapports et de gestion de dates, des déclencheurs et des actions par panneau, des événements d'alarme de porte étendus, et davantage d'accent mis sur la sécurité des données. La nouvelle mise à jour est disponible pour les logiciels Lite et Pro.

Fonctions d'établissement de rapports étendues

La demande des utilisateurs porte sans cesse sur des possibilités plus étendues d'établissement de rapports. Il y avait déjà la possibilité de surveiller des événements chez les utilisateurs, mais cette mise à jour comporte une nouvelle fonction permettant également d'enregistrer au fil de l'eau les événements 'système'. La possibilité de sélectionner une date et une heure est également étendue, permettant ainsi un réglage plus fin. La fonction 'jours spécifiques' a été en outre étendue, et permet par exemple aux clients finals d'ajouter une fermeture pour vacances en une seule fois.

Profil d'autorisation

Un complément très important est constitué par les profils d'autorisation. On peut ainsi, par exemple, dresser des listes des endroits auxquels un certain utilisateur a accès, ou encore, une liste, par point d'accès, avec les personnes autorisées à y

accéder. On peut donner comme exemple l'obtention d'une liste de tous ceux qui ont accès à un local d'entrepôt.

Événements d'alarme de porte

Ceux qui travaillent sur les contacts de porte connaissent la situation dans laquelle des alarmes sont générées par des contacts non utilisés. Il est à présent possible de désactiver des messages d'alarme, comme ceux venant d'une porte forcée ou d'une porte restée trop longtemps ouverte.

Étiquettes non utilisées

Cette fonction existait déjà dans la version précédente, mais a été étendue. On peut à présent indiquer, pour des cartes ou des étiquettes non utilisées, pendant combien de temps elles n'ont pas été utilisées.

Action par panneau

Il est à présent possible de paramétrer un déclenchement et une action par panneau ; on peut donc démarrer une action en fonction de l'endroit d'où l'utilisateur appelle.

Protection des données

En 2018 entrera en vigueur la « General Data Protection Regulation », une réglementation concernant la protection des données personnelles. Lorsque des données personnelles sont collectées, les parties qui rassemblent celles-ci, tant à l'intérieur qu'à l'extérieur de l'UE, doivent observer certaines règles. Il en a été tenu compte également dans cette mise à jour, en rendant paramétrable la conservation des événements liés aux

utilisateurs. En outre il peut être paramétré que la session du gestionnaire du logiciel Net2 soit automatiquement fermée, et certaines exigences peuvent être imposées quant à la force du mot de passe.

Panneau tactile Net 2 Entry

Deuxième nouveauté, le nouveau Panneau tactile Net 2 Entry. Les nouvelles fonctions les plus importantes sont la fonction de recherche dynamique, l'utilisation de photos de profils et de logos pour personnaliser l'écran et pouvoir ainsi retrouver facilement des utilisateurs. Ceci peut s'avérer pratique pour retrouver rapidement une entreprise et une personne donnée, dans un centre d'entreprises. L'utilisation du panneau tactile est simple, et il est équipé d'une usine d'un lecteur de carte et d'un clavier intégrés. Le panneau Net 2 Entry est également entièrement compatible avec le système Net2 actuel. Son esthétique est très appréciée ; en témoignent les deux awards que le panneau tactile a emportés : l'IF Design award 2017 dans la catégorie Building Technology Products et le Red Dot Award 2017 dans la catégorie Communication Technology.



Roy Band (Ingénieur solutions région Benelux Milestone Systems) est venu expliquer le couplage entre Paxton et Milestone.



Stefan van der Velden (directeur régional des ventes Benelux, Paxton) présente le nouveau panneau tactile Net 2 Entry.

Mise à jour du catalogue

Le panneau tactile modifié reçoit également une petite place dans la mise à jour de 2017 du catalogue, tout comme les cartes d'activation HID (transformant un lecteur Paxton en un lecteur HID 125 kHz Prox), les cartes de fonction lecteur (telles que les cartes muettes et la gradation de leds) et le câble de lecteur sans halogène (répondant à la classification au feu CPR).

Couplage avec Milestone

Un module d'extension (plug-in) dans Net2 permet d'intégrer directement Paxton à Milestone, qui donne la possibilité à l'utilisateur de surveiller les portes et les caméras depuis une même interface. L'utilisateur peut ainsi suivre en temps réel l'état des portes et vérifier si une personne qui ouvre une porte avec son badge est réellement la bonne. Les états des portes

et les événements peuvent également être observés sur le plan correspondant et être commandés depuis ce dernier.

Par Sammy Soetaert

www.paxton-nl.com

La protection de terrain, la sécurité naturellement supérieure



Une protection de terrain supérieure résulte de compétences alliées à d'excellents produits. Une sécurité efficace exige une installation professionnelle, de préférence invisible et naturelle. Avec nos systèmes, vous gardez les intrus littéralement à l'extérieur. Et plus vite une intrusion est détectée, plus les dégâts sont limités.



GPS ne pense pas en restrictions, mais en solutions

Spécialistes dans la protection de terrains, alliant connaissance et expérience

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

www.externalsecurity.com

Systemes de sécurité et audiovisuels intégrés



CONTRÔLE
D'ACCÈS



VIDÉO-
SURVEILLANCE



INTRUSION



INCENDIE



AUDIOVISUEL

Nos solutions

- > Contrôle d'accès
- > Alarmes techniques
- > Vidéosurveillance
- > Détection d'intrusion
- > Systèmes biométriques
- > Détection incendie
- > Systèmes de sécurité mobiles
- > Surveillance de périmètre
- > Video Content Analysis (VCA)
- > Reconnaissance faciale / identification
- > Reconnaissance de plaques d'immatriculation (ANPR)
- > Systèmes de gestion globale
- > Plateformes vidéo
- > Intégration logicielle
- > Installation et mise en service
- > Helpdesk et Assistance 24/7



B-1650/a



B-9070-FD-2



ENGIE FABRICOM DEPARTMENT SECURITY & AUDIOVISUAL

Chaussée de Tubize 489
1420 Braine-l'Alleud - BELGIQUE
tel. +32 2 389 22 11 - fax +32 2 389 23 00
secr.security@engie.com



Hikshow : un avenir qui fait la part belle à l'innovation

En tant que journalistes, nous assistons fréquemment à des événements d'entreprise et à des salons professionnels. C'est ainsi que nous nous sommes récemment rendus à Infopol. Sur le stand de Hikvision, nous avons été frappés par l'enthousiasme avec lequel étaient présentées les innovations du leader du marché de la vidéosurveillance. C'est pourquoi nous n'avons pas décliné l'invitation pour le Hikshow, où l'entreprise a présenté ses solutions dans les détails.

Croissance soutenue

Avouons-le, notre visite de Hikvision n'était pas entièrement imprévue. Nous suivons depuis longtemps l'entreprise, et sa croissance rapide ne nous avait pas échappé. En nous rendant à Infopol, nous avions déjà étudié son évolution en flèche, car bien que relativement jeune (2001), Hikvision n'a pas tardé à devenir le chef de file du marché de la vidéosurveillance et des appareillages qui s'y rapportent. Le moteur de cette croissance ? Les investissements gigantesques du département R&D. Pas moins de 9000 ingénieurs, dont 2000 informaticiens, travaillent chaque jour pour aller au-devant des innovations et besoins à l'échelle mondiale. Mais surtout, 8% des revenus de l'entreprise sont réinjectés dans de nouveaux développements. Le résultat est à la hauteur, car Hikvision est aujourd'hui un géant technologique mondial employant plus de 20.000 personnes, avec un chiffre d'affaires de 4,67 milliards de dollars en 2016, et implanté dans plus de 100 pays.

Hikvision à Infopol

Ces efforts donnent naissance à des solutions captivantes, dont nous avons pu

découvrir une partie à Infopol où nous avons rencontré les enthousiastes Roeland De Cauwer et Manuel Lambrechts, respectivement key account manager et pre sales engineer chez Hikvision Europe. Nous leur avons demandé ce que leur inspirait le fait de travailler pour une telle entreprise. Roeland De Cauwer : « Participer à la croissance de Hikvision est extraordinairement stimulant. Les innovations que l'entreprise nous transmet se succèdent à un rythme vertigineux. C'est comme de se trouver à bord d'un TGV qui présente des produits innovants à chaque arrêt. Par exemple, vous pouvez voir ici nos caméras PanoVu, mais aussi des solutions de surveillance du trafic et notre UAV Jammer, un système permettant de neutraliser les drones. Mais il s'agit bien entendu d'applications spécifiques à ce salon. » Manuel Lambrechts : « Notre gamme est beaucoup plus large que ce que nous pouvons proposer, depuis une simple sonnette wifi jusqu'à des solutions de surveillance de haute technologie qui doivent répondre aux exigences les plus strictes sur le plan de la sécurité. Bientôt, nous présenterons une série d'innovations à nos clients belges à l'occasion du Hikshow à Anvers. »



Roeland De Cauwer (key account manager) nous a présenté les innovations de Hikvision. Pas moins de 9000 ingénieurs, dont 2000 informaticiens, travaillent chaque jour pour aller au-devant des innovations et des besoins à l'échelle mondiale.

L'innovation inscrite dans les gènes

Nous avons donc rejoint le Rijnkaai, à Anvers, où le Bocadero accueillait l'événement en question. L'intérêt du Hikshow s'expliquait notamment par la présence de Derek Yang, General Manager Europe de l'entreprise. Dans son allocution de bienvenue, celui-ci a notamment évoqué l'importance de plus en plus marquée de l'intelligence artificielle, et son immense potentiel pour une entreprise comme Hikvision. Une importance qui nous a été confirmée dès la première présentation.



Infopol nous a notamment permis de découvrir les caméras PanoVu, les solutions de surveillance du trafic, ainsi que l'UAV Jammer, un système permettant de neutraliser les drones.

Deep learning

Les investissements colossaux de Hikvision en R&D donnent naissance à des perspectives passionnantes quant à l'avenir de la vidéo dans le domaine de la surveillance. Le Deep Learning, notamment, est un aspect fascinant. L'intelligence artificielle est bien loin d'avoir atteint ses limites, comme nous l'ont expliqué Shirley You, front-end developer, et Arno Tromp, product manager. Hikvision combine ici deux concepts : les enregistreurs vidéo en réseau (network video recorders ou NVR) DeepInMind et les caméras compatibles DeepInView. Les NVR peuvent se greffer sur des installations existantes pour améliorer la surveillance de périmètre (96% d'efficacité) ou la reconnaissance faciale. Les caméras DeepInView, à la fois très intelligentes et très performantes, sont capables de se remémorer des éléments tels que forme du corps, traits du visage et caractéristiques 3D, à l'aide d'algorithmes d'auto-apprentissage. Elles travaillent en combinant deux processeurs ; le premier contrôle le fonctionnement de la caméra proprement dite, tandis qu'un processeur Movidius de dernière génération est utilisé pour le Deep Learning. DeepInMind utilise des processeurs Nvidia capables de traiter d'énormes quantités de données (Big Data) très rapidement. À une époque où le terrorisme fait partie des priorités sur le plan de la sécurité, ce type de détection et la rapidité de traitement n'en sont que plus importants.

H.265+ et Turbo HD 4.0

Manuel Lambrechts nous a également présenté les avantages de la technologie de compression H.265+ brevetée par Hikvision. Elle permet de stocker des images beaucoup plus nombreuses, tout en consommant moins de bande passante et en améliorant la qualité de l'image. Le marché est ainsi prêt pour l'arrivée de la 4K, qui a besoin de beaucoup plus de bande passante et d'espace de stockage (coûteux) – deux éléments qui deviennent à la fois réalistes et abordables grâce à H.265+.

Surveillance par drones

Il y a longtemps que la surveillance par drones n'en est plus à ses balbutiements. Si, à l'origine, celle-ci consistait principalement à équiper un drone d'une caméra, le pilotage de l'engin s'est depuis lors enrichi de multiples fonctionnalités, tandis que les caméras se faisaient plus performantes et accédaient à des tâches plus avancées. Nous avons donc assisté à la démonstration annoncée utilisant un drone Falcon léger de haute technologie. Vincent Hong s'est avéré être un pilote confirmé, et la météo était de notre côté. Nous avons eu droit à une magnifique démonstration au-dessus de l'Escaut. Les images du Rijnkaai et des environs s'affichant en direct sur le grand écran installé étaient à la fois impressionnantes et très détaillées. Pendant ce temps, Jerry Wang nous expliquait les potentialités de ce drone de classe C, y compris la possibilité d'établir un plan de

vol à l'avance. Mais la stabilité des images, qui s'adaptent automatiquement aux mouvements du drone, est elle aussi franchement impressionnante. La réaction immédiate aux manœuvres améliore quant à elle le confort de pilotage. Les drones de Hikvision sont placés sous l'aile de Hikrobotics, une division spécifique qui gère tout ce qui a trait à la robotique et à la vision artificielle.

Darkfighter X

Si le drone était l'attraction visuelle de la soirée, c'est

Darkfighter X qui décroche la palme sur le plan de la technologie. Jusqu'à présent, la technologie vidéo continue à fonctionner presque systématiquement selon le principe « une lentille, un capteur ». Ce capteur doit donc à la fois détecter la lumière pour générer des couleurs, et les infrarouges qui garantiront la clarté de l'image. Il faut donc toujours chercher le compromis entre couleur et clarté.

Or, le Darkfighter X possède 2 capteurs, l'un pour la lumière et l'autre pour les infrarouges. En privilégiant ainsi un seul aspect par capteur, il parvient à générer des images beaucoup plus précises et des couleurs beaucoup plus fidèles tout en restant étonnamment lumineuses. Cette évolution a bien entendu un immense impact sur le traitement de l'image dans l'obscurité, qui en devient nettement plus souple. Dans une configuration monocapteur, la vitesse d'obturation doit être exagérée pour capter suffisamment de lumière, ce qui risque d'entraîner la présence de traînes sur les images. Le bruit est également un problème, car les caméras doivent créer de la lumière en dépit de l'obscurité. Avec le Darkfighter X et ses deux capteurs, ces problèmes appartiennent au passé. Une conclusion particulièrement réussie pour une soirée qui faisait la part belle à l'innovation.

Par 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 est un salon professionnel biennal orienté vers les installateurs de sécurité et des clients finals professionnels. Des distributeurs et fabricants proposent leurs produits et leurs systèmes les plus récents, et fournissent également des informations ciblées.

New Security est un événement du Benelux qui se déroule alternativement en Belgique et aux Pays-Bas.

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

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



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

Biométrie : les veines de la paume de la main ne mentent pas

Lors du Fujitsu World Tour à Bruxelles, une grande attention a été portée aux derniers développements dans le domaine de la sécurité biométrique. Une co-crédation digitale entre Fujitsu et l'entreprise hongroise BioSec a conduit au développement de StadiumGuard, une solution d'identification étanche pour l'accès aux données et aux bâtiments. Grâce à cette nouvelle technologie biométrique, l'hoooliganisme est étouffé dans l'œuf.

La biométrie est utilisée depuis un certain temps déjà comme méthode d'authentification, tant pour l'accès aux données que l'accès physique aux bâtiments et aux domaines. Cependant, des techniques comme le scannage des empreintes digitales, la reconnaissance de l'iris, du visage et de la voix ne sont pas infaillibles. Les systèmes actuels ont leurs points faibles et génèrent une contrefaçon potentielle, un usage détourné d'une carte, de la fraude, du piratage, etc. Au sein de la Primera Division espagnole, une expérience de contrôle d'accès lors de compétitions de football à l'aide d'une technologie basée sur les empreintes digitales a été écartée car le temps de reconnaissance était trop long.

Jusqu'à 15 millions de points de référence

La technologie utilisant la paume de la main ouvre de nouvelles perspectives. Comme les motifs des veines de la paume de main sont uniques à chaque individu, son

scannage constitue une solution adéquate pour connaître l'identité d'une personne selon une certitude de presque 100%. Les motifs des veines peuvent être scannés à une distance minimale (l'appareil ne doit pas être touché), ce qui permet de prévenir toute contamination (pensez aux milieux hospitaliers). « Si la technologie des empreintes digitales utilise 20 à 120 points de référence, la technologie de la paume de la main peut se fonder sur 15 millions de points de référence sous la peau. Au moment où l'information est sauvegardée, celle-ci est cryptée au moyen d'un capteur spécial AES256 (équipé d'un PCB) », explique Oliver Reyers (business development manager PalmSecure Solutions chez Fujitsu Technology Solutions). « Avec la nouvelle application PalmSecure, il en est fini des hackers. Cette solution permet de tuer l'hoooliganisme dans l'œuf, et les amendes octroyées aux clubs pour le comportement inapproprié d'un certain nombre de leurs fans font partie du passé ». Et dans

les stades de football, le risque d'attentats est bien réel, voyez le récent incident avec le bus des joueurs de Borussia Dortmund.

Si la technologie des empreintes digitales utilise 20 à 120 points de référence, la technologie de la paume de la main peut se fonder sur 15 millions de points de référence sous la peau.

5 agents de police pour 11.000 visiteurs

La solution peut être efficacement appliquée notamment pour le contrôle d'identité lors de grands événements sportifs. Pour la sécurisation spécifique des stades, la solution est intégrée au système de ticket électronique, au paiement en ligne et à la vidéosurveillance. « La solution StadiumGuard – greffée sur la technologie PalmSecure – a été implémentée pour la première fois il y a trois ans au stade de l'équipe



Co-crédation digitale entre Fujitsu et l'entreprise hongroise BioSec. Avec StadiumGuard, l'accès au stade de football ne prend qu'une seconde par personne.

de football hongroise Ferencvaros Budapest. Le pays était alors confronté au hooliganisme. Au fameux Groupama Arena à Budapest, là où l'équipe joue les compétitions à domicile, aucun incident grave n'a été répertorié entre les fans de l'équipe et ceux de l'équipe adverse », poursuit Oliver Reyers. « Lors d'un match à risque l'année dernière, où 10.000 visiteurs étaient présents, la présence de cinq agents de police a suffi. Le coût sociétal a donc sérieusement diminué. Le système peut être déployé par étapes, en commençant par exemple par un contrôle d'accès pour les VIP puis en l'étendant progressivement. »

Un potentiel considérable

Chaque visiteur du stade doit être enregistré une seule fois par le système. La solution peut être implémentée dans les stades existants et nouveaux. A partir de l'âge de 16 ans, les motifs des veines de la paume de la main ne changent plus. Avant cet âge, la législation européenne n'autorise pas la sauvegarde de données biométriques. Aussi, le concept prévoit de faire entrer les enfants (ayant moins de seize ans) dans le stade via des entrées spéciales situées à proximité des entrées sécurisées avec StadiumGuard. La solution demande un investissement plus important que les autres solutions biométriques comme la technologie des empreintes digitales, mais elle a un plus grand potentiel hors du stade. L'usage d'une carte peut ainsi être couplé à un shopping dans certaines boutiques dans le cadre d'un partenariat de fidélité avec le club de football en question. Le logiciel offre aussi la possibilité à l'exploitant du stade de donner de l'information supplémentaire concernant par exemple le degré d'occupation des diverses parties du stade (contrôle de foules).

« Au sein du monde footballistique international, nous avons des discussions avec toutes les parties impliquées dans la sécurité des stades. Et elles sont nombreuses : il y a les fédérations de football nationales, les équipes de football de première (et parfois de seconde) classe, les entreprises de sécurité, les propriétaires des stades (pas toujours les clubs), les services de police, les services de sécurité internes des sta-



La solution StadiumGuard a été implémentée pour la première fois il y a trois ans au stade de l'équipe de football hongroise Ferencvaros Budapest.

des, ... Chaque partie doit être convaincue et marquer son accord. C'est souvent un travail de longue haleine. Mais il s'agit avant tout de persuader la fédération de football du pays en question », continue Reyers.

Aussi pour le monde médical et bancaire

La technologie PalmSecure peut aussi être utilisée pour sécuriser l'accès aux datacenters ou aux armoires de médicaments dans les hôpitaux, ou encore dans le cadre du terrorisme. L'usage de mots de passe fera bientôt définitivement partie du passé. Pour les immeubles de bureaux, le système et le logiciel peuvent être limités à l'aspect du contrôle d'accès. « Aujourd'hui, plus de 2 millions de personnes dans le monde sont familiarisées avec cette technologie, dans diverses autres applications : l'administration des salaires, les systèmes de kiosque, ... Sur le marché belge, il y a déjà des applications dans le secteur médical et le monde de la finance. Pour ce dernier secteur, nous pouvons greffer notre technologie à un environnement d'information existant, alors que d'autres solutions sur le marché demandent une toute nouvelle configuration IT », souligne Reyers.

Une co-crédation digitale

Dans le cadre de la co-crédation digitale,

Fujitsu propose la technologie de base de l'authentification de la paume de la main (PalmSecure). Biosec, en tant qu'un des partenaires stratégiques de Fujitsu, fournit les connaissances et l'expertise de l'infrastructure inhérente : le contrôle d'accès physique, la vidéosurveillance et la sécurisation de l'organisation des matchs de compétition. BioSec est une entreprise hongroise fondée en 2012, axée sur l'innovation et les technologies. Cette PME flexible emploie 25 collaborateurs dont de nombreux développeurs de logiciels. « Actuellement, nous nous focalisons sur le football, le monde IT et le secteur de la sécurité. Fujitsu se charge du support technique et de la maintenance, et prévoit principalement un support IT et de la capacité de stockage », explique Peter Györgydéak (CEO BioSec). « Nous ne vendons pas un produit mais un concept. Nous sommes très forts dans le développement, tandis que Fujitsu est un partenaire solide dans le domaine de la vente et du marketing, très bien introduit sur le marché belge. »

Par Philip Declercq

🌐 www.fujitsu.com/be

SÉCURITÉ, FLEXIBILITÉ ET EFFICACE

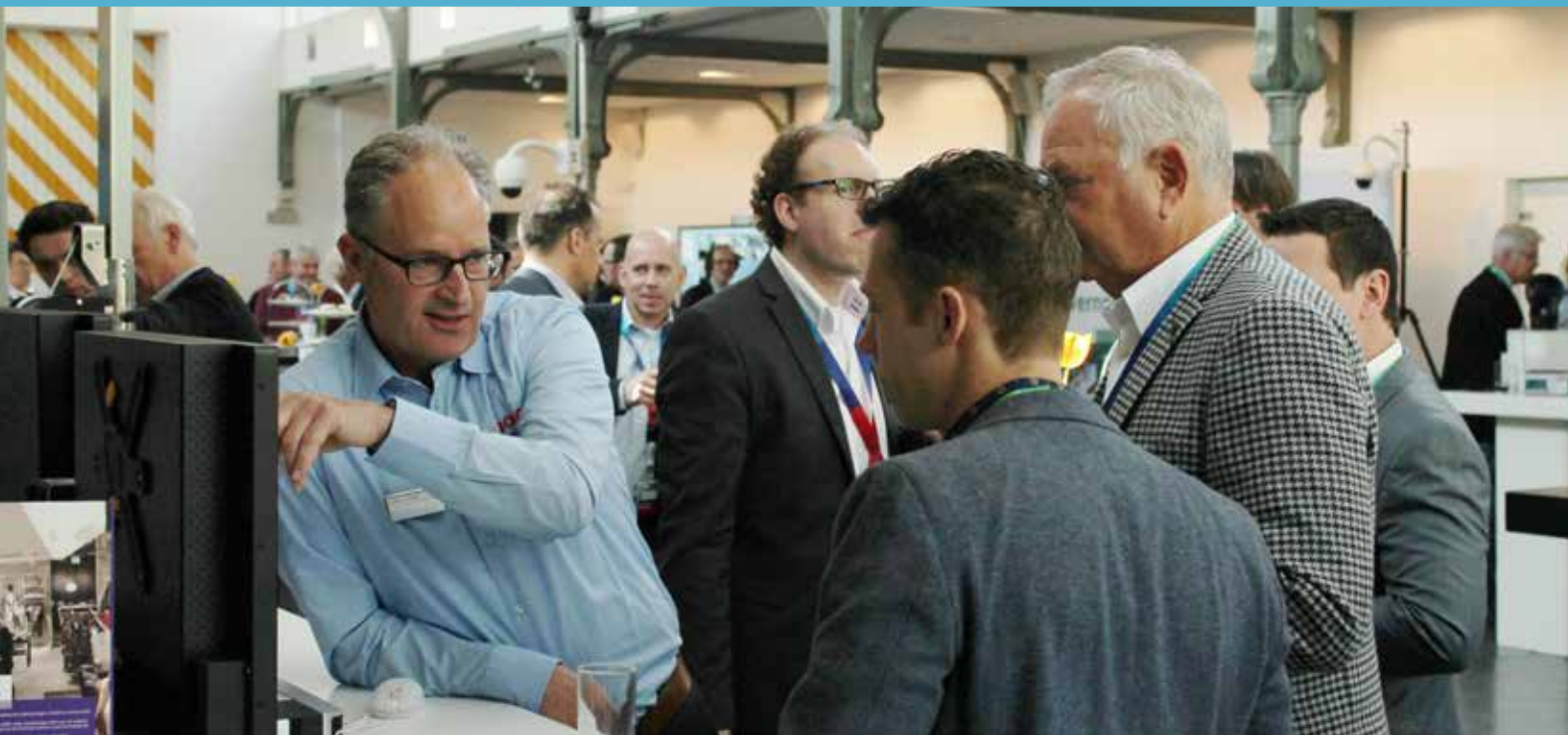
C'est le contrôle d'accès de SALTO Systems.



La plateforme SALTO XS4 peut combiner les ensembles plaques béquilles électroniques, les accessoires et les logiciels, ce qui lui permet de proposer des solutions de contrôle d'accès électroniques en réseau sans câblage.

- ❑ **FIABLE:** De déterminer qui peut entrer, où et quand.
- ❑ **GESTION DU BÂTIMENT:** Pour comprendre toutes les opérations d'accès à partir d'une plate-forme unique.
- ❑ **COMMODITÉ POUR L'UTILISATEUR:** Avec les droits d'accès que vous pouvez modifier selon les besoins et la capacité d'intégrer vos systèmes existants.
- ❑ **L'ACCÈS MOBILE:** Utilisez votre smartphone pour le contrôle d'accès par JustIN Mobile et recevez des droits d'accès en temps réel.
- ❑ **EFFICACE:** Au lieu de remplacer les clés et les serrures vous pouvez modifier les autorisations dans le logiciel, sans frais supplémentaires.





Bosch Talks 2017 met principalement l'accent sur la sécurité

Des dizaines de clients et relations de Bosch Security Systems ont pu, lors d'un événement très apprécié organisé à Hilvarenbeek, prendre connaissance des nouvelles solutions et applications de l'entreprise. Les invités ont pu également assister à des démonstrations de produits et des présentations intéressantes, avec, entre autres, un exposé par Kris De Gendt sur les techniques innovantes utilisées au centre de simulation pour la police, à Zedelgem.

Bosch Security a pris au fil du temps l'habitude d'inviter une fois par an ses clients. Après l'édition francophone de l'an dernier, c'était cette fois au tour des clients néerlandais et flamands. Saske Rodenburg (responsable marketing & communication de l'entreprise) nous explique : « L'événement s'articule autour de trois piliers. Nous avons des démonstrations de produits faites par nos propres spécialistes ; quelques spécialistes externes viennent également animer des sessions autour de thèmes comme la communication et le piratage, et il y a aussi un 'marché' où nous présentons nos innovations concernant des sujets d'application pratique. Les participants sont choisis parmi notre clientèle : intégrateurs système, grossistes, bureaux d'études et un certain nombre de clients finals importants. »

Centre de simulation pour la police

Il y a cinq ans, il a été décidé de créer un centre de simulation où les services de

police belges pourraient simuler, dans un environnement réaliste, des situations courantes telles que des attaques de banque, des arrestations et des communications de mauvaises nouvelles. C'est pourquoi

un décor en grandeur nature a été créé dans l'ancienne école militaire de Zedelgem, afin de simuler au mieux ces situations. Il y a été aménagé, entre autres, un espace d'accueil, un bureau, une cellule



Il y a de cela cinq ans, il a été décidé de créer un centre de simulation où les services de police belges pourraient simuler, dans un environnement réaliste, des situations courantes telles que des attaques de banque, des arrestations et des communications de mauvaises nouvelles.

de police, un café, un bloc sanitaire, un appartement, différents types d'escaliers, un local d'audition Salduz, un distributeur de billets, un comptoir d'enregistrement, un magasin, une salle de classe et un environnement extérieur réaliste complet. Kris De Gendt (directeur du magasin de gros concerné Security Projects) : « Afin de permettre aux enseignants d'évaluer et de suivre la formation, il a été installé un certain nombre de caméras Bosch. Chaque local est équipé de deux caméras installées en diagonale, de façon à couvrir convenablement les lieux et pouvoir observer la situation de deux points de vue différents. Les caméras sont également pourvues d'une vision nocturne, grâce à un éclairage infrarouge intégré. On peut ainsi y organiser des exercices tels qu'un assaut dans le noir complet. En outre, les caméras ont été équipées de micros et de haut-parleurs de sorte que l'enseignant puisse, depuis le local régie, suivre et corriger la formation en temps réel. L'image et le son sont également enregistrés en continu, de sorte que l'exercice puisse être visionné à nouveau avec l'élève. »

Il y avait également quelques exigences spécifiques concernant le système. Kris De Gendt : « C'est exact : le maître d'ouvrage a estimé qu'il était très important que les caméras puissent réagir rapidement à des conditions de luminosité changeantes. Ainsi, lors du jet dans le local d'un flash bang, on perçoit une forte détonation combinée à un flash lumineux intense. Il ne fallait pas que les images soient éclipsées de ce fait pendant quelques secondes ; l'enregistrement devait donc être continuellement de grande qualité. Pour les interrogatoires et la communication de mauvaises nouvelles, il est également important que l'image et le son enregistrés soient synchrones avec le mouvement des lèvres, parce que les expressions du visage sont dans ce cas d'une énorme importance. Ceci est possible avec le système Bosch Video Management. »

D'autres services d'intervention, comme les pompiers et les ambulanciers, viennent depuis s'entraîner dans le centre de simulation. Il est envisagé de continuer à louer le centre à des groupes cibles spécifiques comme les médecins, les pharmaciens et les commerçants. Ils peuvent y



suivre des stages de formation portant, par exemple, sur la manière de répondre à une agression.

« Les caméras sont particulièrement intéressantes à pirater pour les cybercriminels, car elles peuvent traiter de grandes quantités de données. Elles peuvent donc être utilisées efficacement pour une cyber-attaque. »

Gerard Otterspeer, directeur des ventes Bosch Security Systems Pays-Bas

Piratage : regarder la réalité en face

Le pirate éthique Edwin van Andel, de l'entreprise Zerocopter, a donné, grâce à un certain nombre d'exemples marquants, une idée de ce que comporte le piratage et où se trouvent les principaux points faibles. Ils illustrent l'importance de la protection contre la cybercriminalité. L'avion de chasse américain hypermoderne F35 a eu immédiatement une copie chinoise quasi parfaite grâce à un piratage de données chez le fabricant Lockheed. Une importante société néerlandaise du secteur de l'énergie protège ses serveurs par des mots de passe qui sont restés ceux du paramétrage par défaut. Une caméra bon marché achetée dans un magasin de bricolage qui est piratée au bout d'exactement 98 secondes. Chez nous aussi, le pira-

tage est présent partout. Une imprimante en réseau, du port d'Anvers et servant à imprimer des lettres de voiture, a semblé brusquement être reliée à un coupleur étranger. Une enquête approfondie a montré qu'elle comportait une carte Raspberry PI qui envoyait directement les données des lettres de voiture à une organisation criminelle, dans le but de repérer le bateau ayant la cargaison la plus précieuse. Voilà quatre exemples anxiogènes de ce que des fuites dans les protections de données peuvent entraîner comme conséquences. Mais comment s'en protéger ? L'utilisation trop naïve de clés USB inconnues est un point sensible bien connu, mais saviez-vous qu'on peut commander facilement sur Internet une attaque DDOS ciblée pour la modique somme de 10 euros ? On peut aussi commander en quelques clics un virus malveillant personnalisé, tout comme des lecteurs RFID bon marché capables de scanner les fréquences des badges d'accès. Un contrôle d'accès trop laxiste à des bâtiments d'entreprise est également un problème. La protection contre le piratage n'est donc pas évidente, mais quelques règles simples, telles que l'utilisation responsable des clés USB, le fait de ne pas cliquer à gauche et d'éviter d'être naïf lors de l'utilisation de mots de passe, constituent déjà une protection. Et Edwin van Andel conclut par un appel à ne pas considérer les pirates informatiques comme



Le pirate éthique Edwin van Andel s'est, entre autres, arrêté sur le danger d'une clé USB.



Gerard Otterspeer (Bosch) a exposé les mesures appliquées par Bosch pour garantir la sécurité de ses produits.



Ken Anthonissen (key accountmanager chez Bosch Security Systems)

des criminels mais comme des alliés. Dans cette optique il a également attiré l'attention des participants sur les termes 'responsable disclosure' (*divulgateur responsable*), qui signifient que les entreprises définissent une politique dans laquelle elles promettent de ne pas poursuivre les pirates informatiques mais au contraire de les rétribuer s'ils découvrent un point faible dans leur système. De cette manière les pirates auront moins de crainte, sur le plan juridique, que leurs activités soient jugées comme criminelles.

Gerard Otterspeer (directeur des ventes Bosch Security Systems pour les Pays-Bas) enchaîne dans sa présentation, avec le monde passionnant du piratage, avec l'exemple d'une université américaine, dont il ne cite pas le nom, qui via ses distributeurs de confiseries et son système d'éclairage, a été victime d'une attaque DDOS. Les caméras sont particulièrement intéressantes à pirater pour les cybercriminels, car elles peuvent traiter de grandes quantités de données. Elles peuvent donc être utilisées efficacement pour une cyber-attaque. Les réseaux IP sont donc vulnérables, mais les produits Bosch sont reliés, de série, via https et ne fonctionnent donc pas sur la base de mots de passe par défaut. Il n'y a pas non plus de système d'exploitation externe dans les caméras.

Les applications telles que les systèmes de téléconférence sont également expo-

sées. Bosch utilise dans ce cas la norme WPA2. Lors de l'installation, on n'utilise pas de code secret et il n'y a plus non plus de clavier. L'ouverture d'une session sur le réseau se fait à l'aide d'un bouton qui déclenche une liaison cryptée. Les centrales d'alarme incendie sont reliées quant à elles via une passerelle. Cette dernière possède les certificats les plus récents. Pour contrer les dangers de l'Internet des Objets, Bosch Security a également racheté récemment une entreprise spécialisée dans le cryptage.

Par Sammy Soetaert

➤ www.boschsecurity.nl

Sessions de démonstration : détection de personnes et de fumées

Outre les présentations plutôt théoriques, il y avait aussi des démonstrations pratiques. Il y avait ainsi à l'extérieur une caméra intelligente qui, dans le cas présent, surveillait une prairie. Les personnes étaient détectées sans erreur jusqu'à plus de 100 mètres de distance. La caméra peut aussi apprendre à distinguer les animaux et les véhicules, des personnes.

Ken Anthonissen (key accountmanager chez Bosch Security Systems) entraînait quant à lui les participants dans une démonstration concernant la détection de fumées et d'incendie par caméras : « Dans les applications à plafonds élevés, comme des magasins de stockage, la détection d'incendie ponctuelle à l'aide de détecteurs de fumée ne suffit pas. En été par exemple, il peut se former, juste sous le plafond, un matelas d'air chaud dans lequel la fumée s'infiltre rapidement. Cela prend alors trop de temps avant que la fumée n'atteigne le plafond, et l'intervention arrive alors trop tard. Les alarmes intempestives se produisent également trop souvent avec ce type de détecteurs. Avec la vidéo-détection, la fumée est détectée directement à la source, et il ne faut que quelques secondes avant que l'alarme ne retentisse. La détection se fait sur la base de la couleur des produits de combustion, en combinaison avec le scintillement de la flamme et la forme triangulaire d'un feu déclaré. »

Il y a toutefois quelques contraintes pour une détection sans faille, par exemple un éclairage d'au moins 7 lux. Lorsque la couleur de la fumée présente trop peu de contraste avec l'arrière-plan, la détection devient également difficile.



Mission

L'A.C.A. se positionne de façon indépendante des autres associations professionnelles pour la sécurité électronique et le gardiennage physique et accorde sa coopération aux initiatives qui ont comme but d'améliorer la sécurité du client et de ses partenaires. Elle se présente comme l'interlocuteur unique du gouvernement et des organisations nationales et internationales, dans le domaine de la télésurveillance qui est son métier.

L'A.C.A. est ouverte à une nouvelle coopération aussi bien avec les sociétés de sécurité électronique qu'avec les sociétés de gardiennage physique et leurs organisations respectives.

Activités

Le suivi des alarmes émanant de particuliers, entreprises, administrations:

- intrusion, agression
- incendie
- technique
- médicale

La surveillance par des solutions high-tech:

- surveillance par caméras
- tracking & tracing (le suivi des véhicules)
- contrôle d'accès

Le service pour les partenaires et les tiers:

- permanence téléphonique

La mise en oeuvre des procédures d'intervention en accord avec la police, les pompiers, les techniciens, les secours,...

Objectifs - Actions

- L'évolution de la législation attribue de plus en plus de responsabilité opérationnelle aux centrales d'alarmes, ce qui nous oblige à prendre des mesures communes concernant notre responsabilité et nos procédures, la législation fiscale, ...
- Nous voulons apporter une réponse aux utilisateurs grâce à une stratégie de communication positive et conjointe du secteur, afin d'aligner la régression du marché de la sécurité dans notre pays, aux courbes de croissance connues dans les pays qui nous entourent.
- Nous voulons, par une action commune avec l'ensemble des acteurs du marché de la sécurité électronique et du gardiennage physique, apporter un message positif sur le fonctionnement de notre secteur et en stimuler le développement.

Professionalisme

Les membres A.C.A. répondent aux exigences d'un prestation de qualité:

Infrastructure

- système informatique agréé pour la télésurveillance en général et plus particulièrement les alarmes intrusion, la vidéo-surveillance, la télé-permanence
- la réception de différents protocoles
- réseau IP
- système de filtrage des signaux élaborés pour soutenir les services gouvernementaux
- systèmes informatiques fiables

Encadrement

- personnel formé selon les obligations légales, polyglotte, entraîné et régulièrement formé pour réagir en situation normale comme de crise

Partnership

L'A.C.A. est le partenaire privilégié de différents acteurs pour assurer une protection optimale des biens et des personnes comme:

- les installateurs de systèmes de sécurité électronique (alarme intrusion, incendie, agression, secours)
- les groupes d'interventions (gardiens, police, pompiers, techniciens, protection civile)
- les service managers
- les assureurs, bureaux d'études, consultants

A.C.A.: Association des Centrales d'Alarmes a.s.b.l. (Numéro d'entreprise: 867744974)

Avenue des Saisons, 100-102 B30 - 1050 Bruxelles

Tél +32 2 639 39 71

Fax: + 32 2 639 39 79

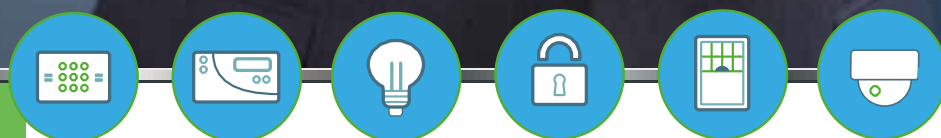
E-mail: info@a-c-a.be

www.a-c-a.be



Dans le monde Internet des objets, la fiabilité fait toute la différence

UltraSync™ Secure Connectivity Solution



Une connexion sécurisée en un rien de temps

Aucune configuration nécessaire pour périphériques

Équipé d'un numéro de série unique, l'Advisor Advanced, habilité par UltraSync, vous permet d'établir facilement et rapidement des connexions M2M à distance. Vous pouvez dorénavant la configurer et établir des diagnostics de n'importe où. La réduction du temps d'installation ainsi que celui des visites sur site entraînent une réduction significative des coûts.

Communication de données presque en temps réel

La vitesse de transfert des données d'un point à un autre dans un réseau est cruciale. Grâce à un réseau performant à faible latence, UltraSync fournit une communication de données en quasi temps réel.

Connectivité sécurisée et immédiate

Bien que l'importance de la connectivité Internet sécurisée soit présente dans l'esprit de tous, la réalité est souvent différente. UltraSync s'assure que votre connectivité soit sécurisée en tout temps.

L'Advisor Advanced intègre de nouvelles fonctionnalités essentielles comme le contrôle d'accès et bénéficie des services de la plateforme Cloud, **UltraSync**.

Etat de fonctionnement

- État de la connexion
- Présentation de l'appareil
- Option de filtre
- Rapports

Diagnostics

- Connectivité
- Journal des événements
- RSSI mobiles
- Mises à jour du Firmware à distance

Liaison externe

Périphériques / enregistrement de services

We listened to you

Attention, les voisins regardent (peut-être)

Éviter les effractions numériques

Les hackers et les cybercriminels sont de plus en plus audacieux et ingénieux, et même capter des flux vidéos ne les effraie plus. En quoi est-ce pour eux un « marché » lucratif et que faire pour vous protéger ?

On dirait le scénario d'un mauvais film de science-fiction, mais c'est pourtant la triste réalité : des hackers qui parviennent à se procurer les images de caméras de sécurité et peuvent, bien assis devant leur écran, observer tranquillement tout ce qu'elles captent. Sans oublier que ces caméras sont susceptibles d'offrir un point d'entrée à partir duquel les cybercriminels pourront plonger au cœur des réseaux informatiques des entreprises et organisations. Fin 2016, le célèbre service secret britannique, le MI6, n'a pas mâché ses mots en qualifiant ce problème de « menace pour la sécurité nationale » après que l'on ait appris qu'un des plus grands fournisseurs de matériel de vidéosurveillance au Royaume Uni est un Chinois lié aux plus hauts cercles du gouvernement. Les caméras sont installées notamment dans les aéroports, les bâtiments publics et le métro londonien.

Chez les particuliers aussi, on a relevé de nombreux cas où détourner la caméra de surveillance pour observer la chambre du bébé – ou celle des parents – avait été un véritable jeu d'enfant. Souvent, il ne s'agit pas que d'observer : les caméras peuvent aussi être commandées à distance... ou éteintes. Le site russe Insecam.org rassemble des centaines de ces flux vidéo provenant de caméras non sécurisées, offerts aux yeux du monde entier. On peut y voir des gens innocents poursuivant leurs activités dans des maisons, des magasins et des restaurants sans se douter le moins du monde qu'Internet tout entier pourrait les épier.

Coercition et chantage

Il est incontestable que les flux vidéos des caméras de sécurité constituent un objectif

très alléchant pour les cybercriminels. Les images permettent non seulement de surveiller les victimes, d'étudier leurs habitudes et leurs schémas de vie, mais on peut aussi les utiliser à des fins de coercition et de chantage, éteindre les caméras par pure malveillance, espionner des sites de production... Dès lors, les scénarios lucratifs ne manquent pas.

Se protéger : points d'attention et conseils

Pour vous prémunir correctement contre de telles pratiques, il est important de donner à vos caméras IP l'importance qu'elles méritent dans la politique de sécurité IT que votre entreprise a (espérons-le) mise en place. Tout comme pour les autres éléments, clients et serveurs, les caméras font partie du réseau de l'entreprise et c'est à ce titre qu'elles doivent être protégées. La plupart des effractions numériques ne peuvent avoir lieu que suite à une défaillance humaine, une négligence, une mauvaise configuration ou un contenu inadéquat. La protection commence donc avec le choix d'un fabricant fiable, d'un installateur compétent, et les connaissances des travailleurs qui vont utiliser le matériel.

Par exemple, il est très important que le déploiement et l'installation soient sécurisés. Si certains services ne sont pas utilisés, comme par exemple la fonctionnalité ftp (file transfer protocol), il sera de loin préférable de les désactiver. Ils permettent en effet à un hacker potentiel d'injecter, assez facilement, un code

et des scripts malveillants dans un réseau pour en prendre le contrôle. Il convient aussi de tenir compte d'éléments non techniques. Par exemple, en installant la caméra, il est non seulement important que le bon angle de vue apparaisse à l'écran, mais aussi que la caméra soit fixée suffisamment haut pour qu'on ne puisse pas l'endommager.

Il est également indispensable que tout l'appareillage du réseau, y compris les caméras, les serveurs, les imprimantes et les postes de travail soient équipés du dernier firmware en date. Très souvent, celui-ci intègre en effet des solutions remédiant aux failles de sécurité découvertes récemment. C'est d'ailleurs la raison pour laquelle un plan et un cycle d'entretien sont si importants : ils constituent, pour une entreprise, la seule manière de savoir quels appareils n'ont pas encore été mis à jour.

Une fois la caméra déballée et pourvue du firmware le plus récent, n'oubliez pas



Il est conseillé d'identifier clairement des responsables et des « propriétaires » au niveau de vos collaborateurs. Dans de nombreuses organisations, la cybersécurité est mise en échec suite à une politique de droits d'accès peu cohérente.



de modifier immédiatement le mot de passe : les mots de passe standard de la plupart des fabricants sont très faciles à retrouver – parfois, une simple recherche sur Google suffit. Inutile de faciliter la tâche aux hackers potentiels. Dans le même ordre d'idées, évitez les mots de passe trop faciles à deviner. Votre date de naissance, le nom de votre chien, ou pire

encore, '123456' ou 'motdepasse'... sont donc radicalement exclus. Veillez aussi à changer régulièrement les mots de passe.

Bien entendu, la résistance du réseau est celle de son maillon le plus faible. Aussi, veillez à l'installation et au bon fonctionnement de pare-feu, et utilisez toujours des connexions sécurisées

(http digest authentication et HTTPS). Vous aurez ainsi la certitude que toutes les informations passant par le réseau sont verrouillées.

Enfin, il est également conseillé d'identifier clairement des responsables et des 'propriétaires' au niveau de vos collaborateurs. Dans de nombreuses organisations, la cybersécurité est mise en échec suite à

une politique de droits d'accès peu cohérente. Efforcez-vous toujours de respecter le principe des « comptes les moins privilégiés », ce qui signifie que les travailleurs n'ont accès qu'à l'infrastructure strictement nécessaire pour leur travail. En ce qui concerne spécifiquement l'utilisation de caméras IP, il est recommandé de ne laisser aucun appareil accéder directement aux caméras, sauf si c'est indispensable. Mieux vaut utiliser une station intermédiaire comme un système de gestion vidéo ou un proxy média.

Par Edwin Roobol, regional director Middle Europe chez Axis Communications

➤ www.axis.com

AXIS Companion



**Une solution
complète provenant
d'un seul fabricant,
parfait !**

**Cela signifie moins de
temps pour l'achat !**

Grâce à l'AXIS Companion Line, je peux répondre à la demande de mes clients en sécurité en leur offrant des produits haut de gamme.

**Êtes-vous intéressé à devenir
AXIS Companion Line Specialist ?
Rendez-vous sur notre site Internet
www.axiscompanion.com/apply
ou appelez-nous au
+31 10 750 46 00**



ATRIUM

plug et play
serveur web intégré
gestion facile

Atrium appartient à la dernière génération de systèmes de contrôle d'accès. Celui-ci offrent un avantage supplémentaire en termes de facilité en ajoutant une interface Web.

Ainsi, vous pouvez à partir de votre canapé ou de la plage gérer facilement votre système par votre tablette ou smartphone. Grâce à ses avantages d'intégration dans un système modulaire compact, Atrium offre une solution pour une porte ou plusieurs centaines de portes.

Contactez-nous pour une démo gratuite ou réservez votre formation gratuite au n° +32 (0)56 73 93 00.



Dans l'Onderzeebootloods de Rotterdam, étaient rassemblés un millier d'installateurs dans le domaine de la sécurité, parmi lesquels de nombreux visiteurs venus de Belgique.

SST2017 : Solutions de sécurité avancées dans l'Onderzeebootloods

La quatrième édition du Smart Security Technology (SST) s'est déroulé dans le RDM Onderzeebootloods, de l'ancienne zone portuaire de Rotterdam. Durant l'événement qui s'est déroulé dans cet endroit magnifique, SmartSD et ses fournisseurs ont exposé les techniques les plus récentes et les derniers développements en matière de sécurité électronique. Le spectacle d'ouverture présentait, outre une attention particulière pour la reconnaissance de visage, ou 'face matching', et la détection intrusion, un spectaculaire duel de caméras.

Après la réussite de l'édition SST de l'an dernier dans le cadre de la Gentse Eskimofabriek, SmartSD avait tout fait, cette fois encore, pour une présentation spectaculaire. Dans l'ancien hangar de lancement de sous-marins, joliment rénové, de la zone portuaire de Rotterdam, un millier d'installateurs de matériel de sécurité s'étaient rassemblés, parmi lesquels, cette fois également, de nombreux visiteurs venus de Belgique. « SmartSD veut continuer à se développer, tant sur le marché belge qu'aux Pays-Bas. C'est pourquoi nous continuons à investir dans des compétences techniques et dans l'assistance à nos clients. Diverses raisons nous ont décidés à troquer prochainement notre implantation de Gilze, devenue trop exiguë, pour un immeuble plus spacieux et plus confortable, à nouveau à Breda. Nos clients belges seront toujours les bienvenus dans notre filiale de Wilrijk. La sécurité est un

secteur de haute technologie. L'innovation est bien entendu très importante, mais les relations avec nos clients et fournisseurs le sont tout autant ; c'est pourquoi nous organisons cet événement annuel, qui se déroule tour à tour en Belgique et aux Pays-Bas », déclare Rik van Aken (spécialiste marketing communications chez SmartSD). L'an prochain, cet éminent distributeur de solutions de vidéosurveillance, de contrôle d'accès et de détection intrusion et incendie, fêtera son 10^e anniversaire.

Face matching

Outre les 43 exposants et les nombreuses « kitchenettes » belges (bien achalandées),

il y avait également un vaste programme de séminaires. Et cerise sur le gâteau, le spectacle d'ouverture était présenté par les responsables produits de SmartSD. Avec pour thème « face matching » ou reconnaissance faciale, Bruno Taymans, business development manager CCTV & Integrated Systems, était chargé d'essayer



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



Étant donné l'importance croissante de la reconnaissance faciale, SmartSD s'est rapproché d'Herta, le fabricant espagnol spécialisé dans le développement de logiciels de reconnaissance faciale.



La technologie des caméras se développe sans cesse plus rapidement, et sur plusieurs plans : plus grande sensibilité des capteurs, plus grande résolution, obturation plus rapide...

les plâtres : « La technologie concernant la reconnaissance faciale a fait, ces dernières années, d'énormes progrès. Étant donné la récente vague d'attentats et la problématique croissante de la sécurité, l'intérêt pour la reconnaissance faciale ne cesse de croître. C'est pourquoi SmartSD s'est rapproché d'Herta, le fabricant espagnol spécialisé dans le développement de logiciels de reconnaissance faciale. Ils consistent à comparer des photos haute résolution, rassemblées dans une base de données, avec des flux vidéo en direct. Un logiciel spécial permet, à partir d'un seul angle de prise de vue de prendre différentes photos de référence biométriques, d'une ou plusieurs personnes, puis de les convertir en 3D. Il est ainsi possible de détecter une ou plusieurs personnes. Le logiciel permet d'analyser jusqu'à 115 vues par seconde, alors que, par exemple, 25 images seulement ont été enregistrées. La seule limite à ce type de reconnaissance faciale est que, pour chaque visage, il faut un minimum de 100 pixels. Pour chaque personne détectée, il est possible de voir avec quelle photo de référence il y a correspondance.

Ces photos sont stockées dans le système d'analyse vidéo. Le système Herta offre aussi la possibilité d'envoyer une alarme. »

Confiance dans le 'Cloud'

Son collègue Jeroen Vons expliquait les évolutions technologiques en matière de systèmes d'alarme intrusion. « Inim Electronics, Vanderbilt et RISCO Group ont en réserve de belles solutions 'cloud' qui facilitent la vie de l'installateur. Le temps des systèmes de détection avec un pavé numérique ordinaire, éventuellement équipé de leds d'état, et capables uniquement de mettre en marche et d'arrêter, est derrière nous. À présent, chacun est pendu à son smartphone, sur lequel il est possible de télécharger une appli de panneau d'alarme d'intrusion. Nous n'avons

pas à nous en faire ou avoir peur de la liaison 'cloud' par elle-même. Cette dernière est sûre, sans plus. Les choses comme les notifications push, peuvent en fin de compte être sous notre contrôle. »

Plus de solutions 'cloud'

Avec ses nouvelles caméras VuPoint, qui peuvent être couplées, via P2P, en plug & play au cloud, et à la nouvelle extension des solutions Smart Home, le Groupe RISCO continue à innover. Toutes les technologies peuvent être commandées via la même application RISCO. Inim Electronics présente Inim Cloud. Cette solution permet de commander les panneaux Smart Living, d'où que l'on soit. Au niveau de la détection incendie, Inim lance le système modulaire d'alarme incendie Praesidia. Vanderbilt se concentre sur le développement et la fourniture de produits et systèmes de contrôle d'accès et de détection intrusion tels que MAGIC, SPC, Seismisch... L'extension du cloud SPC Connect permet à l'installateur de disposer d'un outil particulier pour gérer facilement et entretenir les panneaux SPC. Le cloud SPC Connect permet entre autres,

via une intégration vidéo, une visualisation à l'aide de plans.

Duel de caméras

Ensuite, son collègue Bruno Taymans reprit à nouveau le flambeau pour un spectaculaire duel de caméras. « Avec la sensibilité du capteur, la résolution plus élevée, l'obturation plus rapide de la caméra, le zoom plus puissant ainsi que l'évolution du domaine de recherche, constituent les développements majeurs de la technologie des caméras. Cette fois, ce ne sont pas de nouveaux modèles de caméras de divers fournisseurs qui sont mis dans la balance. Il s'agit plutôt, pour chaque fournisseur, d'une comparaison des paramètres des modèles de caméras actuelles avec ceux d'il y a 2 ou 3 ans. » Ainsi, chez Mobotix, on a comparé l'ancien modèle M12-model (3 Mpx) au nouveau M16 (6 Mpx). Les deux ont été testés, tels que sortis de l'emballage, au même endroit et dans les mêmes conditions (jour/nuit). Pour la nouvelle solution l'une des nouveautés est un programme 'sécurité' qui permet d'optimiser la caméra pour... des applications de sécurité. Ceci donne une image utilisable. Grâce au capteur ultra sensible, la personne est reconnaissable à l'écran.

Solutions caméra sophistiquées

Hikvision lance ses nouveaux produits Turbo HD 4.0 qui utilisent la nouvelle technologie H.265+ de vidéo-compression. Les nouvelles caméras Easy IP3.0 sont équipées de cette technologie et obtiennent des performances de vidéo supérieures. Elles disposent d'une plage dynamique étendue True WDR 120 dB ainsi qu'entre autres d'une Hikvision EXIR 2.0 avec un éclairage Smart IR, ainsi que de la technologie Darkfighter pour éclairage ultra-réduit. Samsung Hanwha et Dahua proposent également de nouvelles solutions. Sony présente de nouvelles caméras très photosensibles, équipées de capteurs Exmor R TM CMOS. Les caméras G6-R, en full HD, offrent une technologie d'image avancée pour un éclairage minimal de 0,006 lux, répondant à la demande de caméras plus photosensibles dans le cadre de la vidéosurveillance.

Par 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



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

Un demi-siècle de prévention incendie

C'est après l'incendie qui a ravagé l'Innovation à Bruxelles le 22 mai 1967, coûtant la vie à 251 personnes, que l'asbl ANPI a vu le jour à l'initiative de la Fédération professionnelle des assurances (Assuralia). ANPI est l'acronyme d'« Association Nationale pour la Protection de l'Incendie et le Vol ». Un demi-siècle plus tard, ANPI est devenue la référence qui réunit tous les acteurs de la prévention incendie dans notre pays : Assuralia, mais aussi le SPF Intérieur, AFT Détection, Agoria et l'ORI. Le 22 mai 2017 a été une journée de commémoration et de perspectives d'avenir.

Après que l'historien Siegfried Evens ait évoqué l'incendie de l'Innovation, le directeur général d'ANPI, Alain Verhoyen, a parlé de l'attitude du Belge vis-à-vis des risques d'incendie. Il a présenté les résultats de la dernière étude portant sur deux ans et s'est rallié au message lancé récemment par Agoria en matière de protection incendie. Celui-ci met en avant le fait qu'une entreprise sur deux spécialisée en sécurité incendie estime que dans notre pays, les bâtiments sont loin d'être suffisamment protégés contre l'incendie. En règle générale, les bâtiments récents ne posent guère problème, mais ceux qui sont plus anciens ne sont pas suffisamment contrôlés. De nombreux gestionnaires d'immeubles pré-supposent – à tort – qu'il suffit d'installer des sprinklers et un système de détection de fumée pour garantir la sécurité incendie.

De 53 à 80.000 mots

Jan De Saedeleer, du SPF Intérieur, a passé en revue le cadre législatif actuel en matière de prévention des incendies après avoir retracé son évolution. Lorsque la catastrophe bruxelloise est survenue, la législation en la matière consistait en... un seul et unique article de 53 mots. Après l'incendie, cet article a été réécrit, d'un point de vue ciblé mais surtout plus restrictif. L'AR du 7 juillet 1994 et ses annexes définissent principalement les prescriptions en matière d'incendie pour, notamment, les bâtiments industriels et les immeubles de bureau. Pour autant, on constate que c'est souvent dans les maisons et immeubles d'appartements que les incendies font le plus de victimes. En

2017, cet AR (qui a déjà été modifié à... 9 reprises) compte plus de 80.000 mots. Bernard Desmet (Assuralia) a parlé de l'organisation de l'assurance incendie dans notre pays, et de ce qu'elle couvre au juste. Benoit Stockbroeckx d'ANPI a ensuite pris la parole pour expliquer les divers niveaux de normalisation.

« Aujourd'hui, la détection incendie ne se limite pas à la technologie; c'est aussi une question d'analyse du risque et de procédures opérationnelles. »
Marnix Steenbeke, président d'Agoria Fire Technologies (AFT) Détection

Détection incendie

La première norme en matière de détection incendie, NBN S21-100, qui a été

publiée en 1986, se limitait principalement aux détecteurs de température, de fumée et de flamme. Dans la pratique, ils étaient principalement destinés aux environnements de bureau. « La détection incendie précise a apporté un plus. Mais l'inconvénient de ces systèmes, c'est qu'ils lançaient souvent de fausses alertes dans d'autres environnements suite à la présence d'humidité, de vent, de poussière etc. » précise Marnix Steenbeke, président d'Agoria Fire Technologies (AFT) Détection. « En 2017, les détecteurs ont énormément évolué sur le plan technologique. » Ils sont adressables, et munis d'une compensation de dérive pour garder une sensibilité constante. La présence d'isolateurs de courts-circuits permettent de réduire l'impact des coupures de câble et des courts-circuits sur l'ensemble de l'installation. On peut également vérifier leur encrassement à



Lors de la catastrophe de l'Innovation à Bruxelles, la législation en la matière consistait en... un seul et unique article de 53 mots. Après l'incendie, cet article a été réécrit, d'un point de vue ciblé mais surtout plus restrictif. Photo : cérémonie de commémoration



François Asselman du Belgian Fire Sprinkler Network a notamment évoqué l'affinage des composants et systèmes dans les dispositifs d'extinction automatiques.



Jan De Saedeleer, du SPF Intérieur : « Le contrôle de la détection incendie dans les maisons et les immeubles d'appartements doit encore s'améliorer. »



« Aujourd'hui, la détection incendie est une affaire d'analyse de risque, de solutions technologiques et de procédures opérationnelles », explique Marnix Steenbeke d'AFT Détection.



Alain Verhoyen (directeur général ANPI) a présenté les résultats de la dernière étude d'une durée de deux ans.

distance. Aujourd'hui, on trouve aussi sur le marché des détecteurs multicritères qui peuvent mesurer fumée, température, CO etc. Ils peuvent être raccordés à l'aide de réseaux peer-to-peer redondants, ce qui permet d'équiper et de gérer un nombre important de détecteurs. »

Les systèmes d'échantillonnage d'air sont apparus dans le commerce au moment où les systèmes d'extinction au gaz ont été interdits. « Ils offrent l'avantage de permettre la détection très rapide d'un incendie, et de retarder ainsi la nécessité d'une intervention manuelle. Ces systèmes sont disponibles en classe A, B et C, dans toutes les tailles, tous les poids et toutes les dimensions. Autre solution contemporaine : les détecteurs de température linéaires, du modèle de base à la fibre optique, qui sont surtout utilisés dans les environnements sensibles à la corrosion, ou ceux pour lesquels un détecteur ponctuel conventionnel ne convient pas », poursuit Steenbeke.

Détection sans fil et détection par caméra

Un groupe de travail planche actuellement sur une autre piste : celle de la détection sans fil. « Cette formule ne constitue pas une solution miracle. Travailler sans fil implique notamment une fréquence radio, des longueurs d'onde et des bandes passantes; or, il n'est pas possible de transmettre des signaux à une distance illimitée à travers des murs et autres obstacles. La détection sans fil n'est donc efficace que dans les environnements excluant les câblages classiques, par exemple les bâtiments présentant une valeur historique. Enfin, la détection par caméra constitue peut-être l'avenir de la détection incendie. Elle permet d'obtenir une image parfaite des particules de fumée présentes dans un grand local », poursuit Steenbeke. La conclusion du président d'AFT Détection est triple. « Un bon installateur de systèmes d'alarme est certifié, possède les connaissances requises, et sait résoudre les problèmes en utilisant le bon produit au bon endroit. Aujourd'hui, la détection incendie ne se limite pas à la technologie; c'est aussi une question d'analyse du risque et de procédures opérationnelles. » Il

a également lancé un appel au monde des assurances pour qu'il offre, d'une manière ou d'une autre, un soutien financier aux entreprises qui installent des systèmes de détection incendie dans leurs locaux.

Perfectionner les composants et les systèmes

François Asselman du Belgian Fire Sprinkler Network et administrateur d'ANPI a parlé de nouveaux développements spécifiques en matière d'installations d'extinction automatiques. « Il y a tout d'abord le perfectionnement des composants et des systèmes. Pensons par exemple à la différenciation en fonction des risques et des charges calorifiques à protéger, du temps de réaction pour un sprinkler (68°) qui se chiffre à présent à 7 secondes (32 auparavant), et aux sprinklers de nouvelle génération qui sont notamment dotés de systèmes intelligents, et combinent principes de détection et déclenchement intelligent. Ces nouveaux développements touchent aussi la conception et la réalisation, la préfabrication des canalisations en usine et l'utilisation des fixations au montage. »

« Un système d'évacuation des fumées et de la chaleur peut contribuer à améliorer et à garantir le niveau de sécurité incendie global, en mettant l'accent sur une évacuation et un soutien sûrs durant l'intervention des pompiers », ajoute Robby De Roeck (Fire Safety Engineer chez Brakel Aero sa et administrateur de l'asbl FiroProNet).

Par Philip Declercq

www.anpi.be

DAITEM SYSTÈMES D'ALARME SANS FIL

100 % SANS FIL

INCERT

CENTRALE PARLANTE

5 ANS D'AUTONOMIE (BATTERIES)

COMMUNICATION SÉCURISÉE

PILOTABLE VIA L'APP e-DAITEM

5 ANS DE GARANTIE



Dahua Technology introduit une caméra thermique pour le marché commercial

Jusqu'à présent, la plupart des caméras thermiques sur le marché industriel sont assez volumineuses et trop coûteuses pour la plupart des projets commerciaux. Dahua lance aujourd'hui la caméra bullet mini-hybride thermique intuitive DH-TPC-BF2120. Cette caméra de petite taille, avec un spectre dual-channel et des fonctions intelligentes, est proposée à un prix abordable.

<http://www.dahuasecurity.com>



Panasonic présente son nouveau système d'interphones vidéo sur IP

Panasonic a lancé un nouveau système d'interphones vidéo Full IP qui répond à la demande croissante d'intégration de différents systèmes dans les bâtiments. Ce nouveau modèle IP (VL-VN1900) fonctionne avec une vaste gamme d'appareils, notamment des caméras CCTV réseau, des téléphones SIP et des enregistreurs vidéo réseau. Grâce à son alimentation PoE (Power over Ethernet), le système peut être connecté à l'aide d'un seul câble, ce qui facilite l'installation tout en réduisant les coûts. De plus, couplé à un boîtier de contrôle, il peut supporter jusqu'à 2000 appareils SIP alimentés en PoE.

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



Axis améliore sa technologie Zipstream

Axis annonce des améliorations à sa technologie de compression Zipstream pour accompagner la hausse des besoins en diffusion et stockage des données produites par les caméras panoramiques à 360° et les modèles de résolution 4K. Préservant les détails importants des séquences vidéo à des fins d'analyse, Zipstream réduit les besoins en bande passante et en stockage d'au moins 50 % en moyenne. Axis annonce également la commercialisation de deux nouveaux dômes intégrant cette technologie Zipstream améliorée, pour une surveillance vidéo économique à haute résolution sur 360°.

www.axis.com

ARAS Security étend son assortiment CamTech avec VMS

ARAS introduit le système CamTech VMS qui, du fait de son concept modulaire, répond idéalement à la philosophie 'toujours une solution sur mesure'. Du contrôle PTZ au fisheye-dewarping et de la reconnaissance faciale aux signes distinctifs, le système de gestion de vidéo CamTech VMS est évolutif, fiable, puissant et flexible. L'application de Video Analytics permet d'économiser des coûts de gestion. Outre les images vidéo, il est possible d'effectuer des recherches sur base de métadonnées : retrouver les bonnes images plus rapidement rend donc le suivi plus efficace et plus utile. De plus, grâce au caractère ouvert du système, il est possible de raccorder 4.000 caméras IP de plus de 130 marques.

www.aras.nl



Solution de surveillance Full HD via le câble coaxial

La demande de solutions d'observation par caméra analogique est toujours bien là. IDIS propose DirectCX™, une solution analogique avancée FULL HD fondée sur la technologie HD-TVI. Les avantages de DirectCX™ : solution idéale pour le marché de remplacement avec la préservation du câble coaxial existant, il suffit d'échanger les caméras et l'enregistreur à disque dur ; qualité d'image Full HD en temps réel (30ips@1080p) sans perte de qualité ni ralentissement ; réglages du menu de la caméra OSD via le câble coaxial ; distances de câble jusqu'à 500 mtr.

www.idisglobal.com

2ème génération de lecteurs Paxton intégrant la Genuine HID Technology

En 2017, Paxton a intégré la Genuine HID Technology™ dans la plupart des lecteurs Proximity. Désormais, vous pouvez activer la fonctionnalité HID grâce à l'utilisation de la carte licence HID Proximity. Via cette carte licence HID disponible séparément, il est possible d'activer HID™ sur les lecteurs Paxton Proximity. Les cartes de licence sont disponibles avec 1, 5 ou 10 licences. Lorsque la carte de licence est proposée sur les lecteurs compatibles, la fonctionnalité HID™ Prox® 125 kHz est activée. Outre cette fonctionnalité, le lecteur conserve la possibilité de lire les cartes et tags Paxton et EM.

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



LES NOUVEAUX ENREGISTREURS SILENCIEUX DE SEFICA

Compatibilité Onvif et reconnaissance de plaques



Sefica poursuit le développement de son offre de NVR avec l'introduction de la gamme ImageBox.

Ces enregistreurs sans ventilateur (Passive Cooling Technology) et compatibles Onvif sont disponibles en 2 versions:

IBX-09: un NVR 9 canaux IP compatible Windows/MAC. La détection de mouvement et le Smart Motion Search intégrés sont configurables par caméra, quel qu'en soit le type.

IBX-02-ANPR: un NVR pour 2 caméras avec reconnaissance intégrée des plaques d'immatriculation (ANPR). Avec la synchronisation automatique des logiciels ANPR et ImageBox, vous trouvez rapidement la plaque d'immatriculation désirée.

Sefica.
secure. protect. prevent.

Sefica est une marque de qualité exclusive de



RAS sprl
Brugsesteenweg 257, 8500 Kortrijk
T +32(0)56 36 37 42
contact@sefica.be
www.sefica.be



OKTOPUS VEILLE SUR VOTRE SÉCURITÉ

PERSONNES • BIENS IMMOBILIERS • PROCESSUS INDUSTRIELS • LOCALISATION DE VEHICULES ET AUTRES OBJETS MOBILES



LA TÉLÉSURVEILLANCE : VOTRE GARANTIE SÉCURITÉ

- Collaborateurs triés sur le volet
- Infrastructure technique de pointe
- Procédures conçues sur mesure
- Souplesse des services administratifs et opérationnels
- Garanties morales, techniques et fonctionnelles
- Services opérationnels 24h/24



Agréé par le Service Public Fédéral Intérieur
et les compagnies d'assurances (ASSURALIA).
Certifié: ISO 9001-2000

Avenue Louise 331
1050 Bruxelles
Tél.: 32-2-542 05 42
Fax: 32-2-542 05 43
contact@oktopus.com

www.oktopus.com