a&S POLSKA
www.aspolska.pl

CZASOPISMO BRANŻY SECURITY
nr 1/2017
styczeń/luty
15 zł (w tym 8% VAT)

Transport a rynek SECURITY

TEMAT NUMERU
Planowane są duże inwestycje w poprawę bezpieczeństwa w sektorze transportu i logistyki.
str. 58

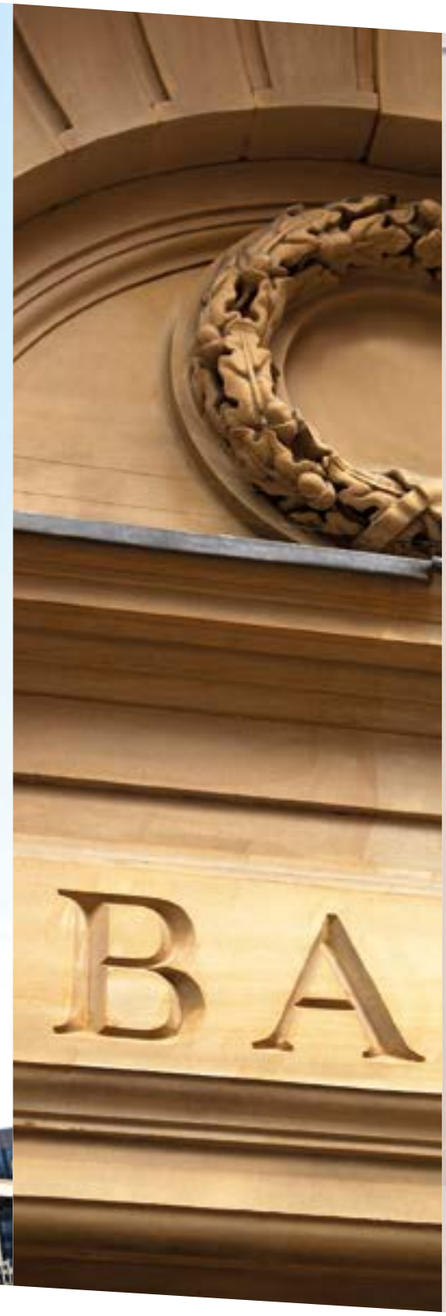
TOP 50 SECURITY 2016 NA ŚWIECIE

ISSN 2451-5175

INNOWACJE
Czy branża security jest innowacyjna?
Ostatnie analizy akcentują proinnowacyjny charakter norm i procesów normalizacji.
str. 52

OCHRONA PPOŻ.
Scenariusze pożarowe
Tworząc je, należy przeanalizować funkcje, sposób działania i skutki uboczne zadziałania urządzeń ppoż.
str. 94

NOWY DZIAŁ
Bezpieczeństwo biznesu
Istotne informacje dla osób odpowiedzialnych za bezpieczeństwo zarówno w małych firmach, jak i wielkich korporacjach.
str. 97



NR 1 NA ŚWIECIE

Hikvision Poland
The Park Warsaw, Budynek 1
Ul. Krakowiaków 50
02-255 Warszawa
T +48 22 460 01 50
F +48 22 464 32 11
info.pl@hikvision.com

www.hikvision.com

www.aspolska.pl

Drodzy Czytelnicy

Oddajemy w Państwa ręce nowe czasopismo „a&s Polska". Tworzy je zespół redakcyjny znanego dwumiesięcznika „Systemy Alarmowe", kontynuując tradycję najstarszego w Polsce tytułu branży security. Skład kolegium redakcyjnego i współpracujący autorzy gwarantują, że zachowamy wysoki poziom merytoryczny i opiniotwórczy charakter publikowanych treści.

W dziale **Rynek security** przybliżamy najważniejsze dla branży tematy oraz opinie ekspertów, z którymi współpracujemy od lat. Opisujemy nowości rynkowe, dobre praktyki i ciekawe realizacje, trendy i najnowsze rozwiązania oraz wydarzenia branżowe w Polsce i zagranicą.

By sprostać nowym oczekiwaniom rynku, prasa branżowa potrzebuje nowego impulsu. Przedstawiając ofertę security, będziemy odpowiadać na potrzeby różnych sektorów rynku. Pracujący w nich specjaliści odpowiedzialni za bezpieczeństwo to nowa grupa Czytelników, do której także adresujemy nasze czasopismo. Z myślą o nich tematem tego wydania jest **Bezpieczeństwo w transporcie i logistyce.** Omawiamy tę kwestię na wielu płaszczyznach, począwszy od przedstawienia metod zabezpieczeń i oferty branży security dla tego specyficznego sektora, skończywszy na komentarzach i opiniach profesjonalistów.

Ponadto – jako część „a&s International", największej na świecie grupy wydawniczej w branży – będziemy prezentować globalne spojrzenie na rynek, publikować rankingi oraz badania i analizy opracowane przez najlepszych specjalistów i renomowane instytuty badawcze.

W pierwszym numerze „a&s Polska" przedstawiamy **ranking TOP 50** – listę największych firm security na świecie wraz z obszernym omówieniem ich strategii, źródeł sukcesów i scenariuszy na przyszłość.

W „a&s Polska" ciekawe treści znajdą także specjaliści ds. **bezpieczeństwa biznesu**. Ten dział powstaje przy współpracy merytorycznej z firmą doradczą SASMA Europe. Autorzy, doświadczeni w swoich branżach, podejmują tematy istotne dla zarządzających szeroko pojętym bezpieczeństwem zarówno w małych firmach, jak i wielkich korporacjach.

„a&s Polska" to nie tylko czasopismo, to **Branżowa platforma wiedzy 360°**, zapewniająca najświeższe i najważniejsze informacje o bezpieczeństwie – portal internetowy **aspolska.pl**, newslettery, profile w mediach społecznościowych, wywiady wideo z interesującymi osobami z branży.

Miło nam również poinformować o zainicjowaniu cyklu **śniadań z ekspertami,** podczas których specjaliści w luźnej, nieformalnej atmosferze podzielą się swoimi doświadczeniami. Pierwsze tego typu spotkanie będzie dotyczyło bezpieczeństwa transportu i logistyki *(więcej na s. 91)*.

Ważnym wydarzeniem będzie **Warsaw Security Summit** – pierwsza w Polsce międzynarodowa konferencja branży security, którą zorganizujemy w czerwcu. Stanie się ona okazją do poznania globalnych trendów na rynku, wysłuchania prelekcji światowych ekspertów oraz wzięcia udziału w dyskusji na najważniejsze tematy naszej branży *(więcej na s. 119)*. O szczegółach będziemy informowali w kolejnych wydaniach „a&s Polska" oraz na bieżąco na portalu aspolska.pl.

Życzymy, aby ten rok był dla Państwa pomyślny, a nasz nowy tytuł stał się bogatym źródłem informacji branżowej, pomocnej w podejmowaniu ważnych zawodowych i biznesowych decyzji.

Marta Dynakowska
redaktor naczelna

Mariusz Kucharski
dyrektor zarządzający

www.aspolska.pl

a&s POLSKA

Wydawca
a&s Polska Sp. z o.o.

Adres wydawcy i redakcji
a&s Polska
Rondo1 (10. piętro)
Rondo ONZ 1, 00-124 Warszawa
tel. +48 22 418 71 59
e-mail: info@aspolska.pl
www.aspolska.pl

Dyrektor zarządzający
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Dział reportażu
Andrzej Popielski

Dział marketingu i reklamy
Iwona Krawiec

Kolegium redakcyjne
Norbert Bartkowiak
Edmund Basałyga
Sebastian Błażkiewicz
Janusz Bohdanowicz
Jan T. Grusznic
Roman Maksymowicz
Dariusz Mostowski
Przemysław Pierzchała
Janusz Sawicki
Stefan Jerzy Siudalski
Jerzy Sobstel
Paweł Wittich
Waldemar Wnęk
Aleksander M. Woronow

Korekta
Jolanta Kucharska

Projekt graficzny
Sylwester Dmowski

Prenumerata
www.aspolska.pl/prenumerata

Redakcja zastrzega sobie prawo skracania i adiustacji zamówionych tekstów. Artykułów niezamówionych i niezatwierdzonych do druku nie zwracamy. Opinie autorów nie muszą być tożsame z poglądami redakcji. Za treść reklam redakcja nie odpowiada. Przedruki tekstów bez zgody redakcji są niedozwolone.

a&s Polska jest częścią międzynarodowej grupy wydawniczej a&s International.

TEMAT NUMERU

RAPORT STR. 58

Bezpieczeństwo transportu

WYWIAD STR. 86

Kamery w stołecznej komunikacji

CASE STUDY STR. 92

Dworzec Łódź Fabryczna pod lupą pożarników

Kamery Axis z przetwornikami obrazu i obiektywami Canon

Axis Communications
www.axis.com/pl

Sieciowa kamera AXIS Q1659 to pierwszy model łączący cenioną przez profesjonalistów optykę Canon ze sprawdzonymi rozwiązaniami i know-how Axisa. Kamera charakteryzuje się ultrawysoką jakością obrazu, niespotykaną w segmencie szerokokątnych stałopozycyjnych urządzeń dozorowych. Nowatorski przetwornik oraz obiektyw EF Canona gwarantują niezrównane odwzorowanie kolorów i szczegółów oraz doskonały kontrast w najbardziej wymagających warunkach oświetleniowych.
AXIS Q1659 ma rozdzielczość 20 Mpix przy 8 kl./s, zapewniając szczegółowy obraz otwartych przestrzeni oraz obiektów znajdujących się w dużej odległości. Kamera wykorzystuje technologię lustrzanki cyfrowej (DSLR) i w zależności od potrzeb może współpracować z 7 różnymi obiektywami EF/EF-S.
Jest kompatybilna z największą w branży bazą oprogramowania do zarządzania materiałem wideo dostępną w ramach Programu *Axis Application Development Partner* (ADP) oraz z *AXIS Camera Station*.
W kamerze zastosowano udoskonaloną wersję opracowanej przez Axis technologii Zipstream, redukującej szerokość pasma i ograniczającej wielkość zapisu wideo bez utraty szczegółów obrazu. Złącze SFP umożliwia łączność za pomocą światłowodu z innymi elementami systemu, znajdującymi się w dużej odległości.
Debiut rynkowy kamery AXIS Q1659 zaplanowano na I kwartał 2017 r. Będzie ona dostępna w kanałach dystrybucyjnych Axis.

Mini-PTZ z serii GENSTAR *Image is Everything*

CBC Poland
cbc@cbcpoland.pl www.cbcpoland.pl

GANZ IP ZN8-P5NTAF62L – 3 Mpix zewnętrzna kamera miniPTZ z 12-krotnym zoomem oferująca nie tylko doskonałe parametry, ale też ciekawy design i kompaktowe wymiary. Specjalnie zaprojektowana 3-komorowa obudowa IP66 mieści zamontowane oddzielnie moduł kamery i promiennik IR, by obniżyć temperaturę wewnątrz obudowy, co wpływa na żywotność. Kamera jest wyposażona w wysokoefektywne soczewkowe diody IR-LED z dynamiczną regulacją szerokości wiązki o zasięgu do 60 m. Temperatura pracy kamery wynosi od -40° do 60°C. MiniPTZ może być stosowana na lotniskach, stacjach metra, parkingach, w hotelach, bankach, obiektach użyteczności publicznej, centrach handlowych oraz aplikacjach monitoringu miejskiego – doskonale odczytuje tablice rejestracyjne (nawet przy prędkości 100 km/h).
Hasło *Image is Everything* idealnie oddaje ideę serii GenSTAR, do której należą MiniPTZ. Serię wyróżnia wiele unikalnych technologii wspierających jakość obrazu, tj. funkcje Smart IR, DEFOG (korekcja mgły), tryb korytarzowy, ROI (*Region of Interest*).
W skład serii wchodzą 2-, 4- oraz 6-Mpix kamery kompaktowe, kopułkowe, bullet oraz *fisheye* z obiektywami stało- i zmiennoogniskowymi oraz motozoom. Wybrane modele obsługują funkcje analityczne: antysabotaż, linia perymetryczna i strefa perymetryczna. Ofertę uzupełniają 4-, 8-, 16- i 32-kanałowe rejestratory sieciowe NVR umożliwiające nagrywanie i wyświetlanie na żywo strumieni do 8 Mpix (4K), współpracujące z GenSTAR na zasadzie *plug & play*.

Tester PFM905

Dahua Technology
www.dahuasecurity.com/pl

Nowoczesne systemy zabezpieczeń stawiają przed instalatorami coraz większe wymagania. Aby ich praca była prostsza i efektywniejsza, Dahua Technology – czołowy producent urządzeń do systemów zabezpieczeń – wprowadziła na rynek przenośny zintegrowany tester PFM905 do kamer z interfejsami HDCVI, AHD, HDTVI, CVBS.

Tester ma wbudowane złącze RS485, obsługuje protokoły Pelco-D/P i inne – sterowanie kamerami obrotowymi PTZ.
W zwartej, odpornej na uszkodzenia obudowie zamknięto 4-calowy, kolorowy wyświetlacz o rozdzielczości 800 x 480. Wbudowana pamięć 8 GB oraz gniazdo SD pozwalają na zapisywanie nagrań z testowanych kamer.

Tester został wyposażony w wyjście zasilające 12 V. Wbudowany wymienny akumulator zapewnia nieprzerwaną pracę testera przez 5 godz. Użytecznym dodatkiem jest wbudowana latarka LED.

Kamera IP GT-CI51C5-36Z z obiektywem motozoom

Delta-Opti
www.delta.poznan.pl
sklep.delta.poznan.pl

Nowa kamera IP marki GEMINI TECHNOLOGY została wyposażona w rewelacyjny przetwornik Sony IMX178 pozwalający uzyskać ostry i czytelny obraz w rozdzielczości do 5 Mpix. Obiektyw motozoom o regulowanej ogniskowej w zakresie od 3,6 do 10 mm dodatkowo udostępnia funkcję P-Iris. Połączenie tych dwóch elementów zapewnia płynny obraz w maks. rozdzielczości 2592 x 1944 pikseli, przy czym zastosowana kompresja H.265 znacząco zmniejsza niezbędną do przesłania obrazu przepustowość sieci. Kamera zawiera również regulowany oświetlacz IR o maks. zasięgu 50 m. Całość zamknięto w estetycznej obudowie, radzącej sobie w trudnych warunkach atmosferycznych, a możliwość zasilania urządzenia poprzez PoE zgodnie ze standardem 802.3af pozwala ograniczyć doprowadzone przewody do minimum.
Model GT-CI51C5-36Z, poza niebanalnymi elementami składowymi, został doskonale wyposażony w zakresie oprogramowania. Funkcja WDR znacząco poprawia jakość obrazu przy dużym kontraście, cyfrowa redukcja szumów 3D-DNR natomiast zapewnia wyraźne nagranie nawet przy słabym oświetleniu. Atutem są też funkcje inteligentnej analizy obrazu, np. wykrywanie pozostawionego lub brakującego obiektu, naruszenia obszaru bądź linii czy śledzenie obiektu. Całości dopełnia możliwość łatwego i intuicyjnego sterowania kamerą z poziomu przeglądarki internetowej lub aplikacji mobilnych.

Minisystem pozycjonujący PTZ DS-2DY3320IW-DE4

Hikvision
www.hikvision.com

Oferta kamer firmy Hikvision – największego na świecie, według rankingu „a&s" Top 50, producenta branży security – została rozszerzona o minisystem pozycjonujący PTZ **DS-2DY3320IW-DE4** (3,0 Mpix). Kamera została wyposażona w przetwornik obrazu 1/2.8" Progressive scan CMOS.

W nowym modelu kamery zastosowano funkcję WDR (120 dB), oświetlacz IR o zasięgu do 100 m, a także zaawansowane funkcje łącznie z analizą obrazu.

Cechą, która wyróżnia ten model od innych kamer PTZ, jest większy zakres wychylenia pionowego *(Tilt),* wynoszący od -40° do 30°. Z kolei wartość wychylenia poziomego *(Pan)* osiąga 360°. To m.in. sprawia, że tę kamerę można polecić jako idealny sprzęt do systemów monitoringu imprez masowych, np. obserwowania trybun na stadionach.
Ponadto regulowany obiektyw z 20x zoomem optycznym zapewnia uzyskanie większej liczby szczegółów w przypadku monitorowania obszarów rozległych.

W kamerze **DS-2DY3320IW-DE4** zastosowano gniazdo na kartę pamięci 128 GB. Model jest zgodny ze specyfikacją ONVIF.

Ochrona perymetryczna Xtralis

Linc Polska
www.linc.pl

Xtralis specjalizuje się w systemach zabezpieczeń do ochrony perymetrycznej. Szybka detekcja i automatyczna identyfikacja zagrożenia, połączone z natychmiastowym powiadamianiem centrum monitoringu, to główne cele stawiane przez producenta.
Portfolio firmy obejmuje m.in. wielokanałowe systemy wideo do rejestracji, strumieniowania i powiadamiania wraz z zaawansowaną analityką (HeiTel i ADPRO), a także ADPRO PRO-E – wielokrotnie nagradzane czujki PIR dalekiego zasięgu do niezawodnej ochrony perymetrycznej. Dzięki połączeniu zdalnej platformy wideo z analityką i oprogramowaniem EMS Xtralis oferuje łatwy do zainstalowania, skuteczny system ochrony, gwarantujący wczesne ostrzeganie o zagrożeniu i niezawodność działania.
Linie HeiTel (CamDisc) i ADPRO (iFT i FastTrace™) mogą być wyposażone w inteligentną analitykę, np. IntrusionTrace™, LoiterTrace™, SmokeTrace™.
Nowa generacja czujek ADPRO PRO-E zapewnia wyjątkową skuteczność. Długi zakres detekcji (do 220 m), ochrona strefy podejścia 360PROtect i bezprzewodowa transmisja danych – cechy te czynią je innowacyjnymi i bezkonkurencyjnymi na rynku zabezpieczeń. Czujki są dostępne w różnych konfiguracjach dostosowanych do indywidualnych potrzeb i możliwości finansowych klienta. System oparty na platformie wideo oraz zewnętrznych czujek PIR APRO marki Xtralis stanowi profesjonalną i solidną podstawę każdego systemu ochrony.

Dźwiękowy System Ostrzegawczy APS-APROSYS

Schrack Seconet Polska
www.schrack-seconet.pl

Schrack Seconet Polska rozszerzył swoją ofertę handlową o kolejną grupę produktów – DSO. Mając na względzie obszar działania partnerów i wychodząc naprzeciw ich oczekiwaniom, firma udostępnia inwestorom kompleksowe rozwiązanie z zakresu SSP i DSO, przy jednoczesnym zachowaniu najwyższej jakości produktów.
Oferowany system DSO jest produkowany przez szwajcarską firmę G+M Elektronik AG, która podobnie jak Schrack Seconet należy do grupy SECURITAS AG. System posiada certyfikat CPR zgodności z PN-EN 54-16 oraz świadectwo dopuszczenia CNBOP-PIB.
APS-APROSYS ma budowę modułową i może pracować jako skupiony lub rozproszony. Dzięki modułowej budowie oraz innowacyjnemu układowi pomiaru linii głośnikowych z selektorami stref istnieje możliwość obsługi wielu linii głośnikowych przez jeden wzmacniacz mocy. Maksymalna moc głośników podłączonych do linii głośnikowej wynosi 500 W.
Uzupełnieniem oferty są certyfikowane głośniki pożarowe niemieckiej firmy IC Audio GmbH w następujących odmianach: sufitowe, naścienne, tubowe, projektory dźwięku i kolumny głośnikowe.
Wszystkich zainteresowanych systemem APS-APROSYS prosimy o kontakt z firmą Schrack Seconet. W drugim kwartale br. zostanie uruchomiony cykl szkoleń projektowych z zakresu DSO, o których firma będzie informowała na swojej stronie www.

Laserowy wykrywacz materiałów wybuchowych i narkotyków G-Scan Pro LDS 4500-G

Sklep detektywistyczny Spy Shop
www.spyshop.pl kontakt@spyshop.pl

G-Scan Pro to najnowocześniejszy, ręczny, przenośny detektor laserowy firmy Laser Detect Systems specjalizującej się w rozwiązaniach przeznaczonych do walki z przemytem, handlem narkotykami i atakami terrorystycznymi. Wykorzystuje spektroskopię Ramana do wykrywania materiałów wybuchowych (także wytworzonych w warunkach domowych), narkotyków i nielegalnych substancji w cieczach, ciałach stałych i proszkach. Analiza trwa tylko 3 s dzięki bogatej bibliotece materiałów niebezpiecznych, którą można rozbudowywać i aktualizować.
G-Scan Pro wyróżnia się minimalnym poziomem błędów i fałszywych alarmów (< 1%) oraz długością fali lasera: 532 nm.
Analizy porównawcze firmy LDS dowiodły, że w przeciwieństwie do laserów o długości fali 785 nm i 1064 nm (najczęściej spotykanych w tego typu urządzeniach) wykrywacz z laserem 532 nm najlepiej sprawdza się w wykrywaniu i identyfikacji próbek niefluorescencyjnych, substancji ukrytych w plastikowych i szklanych butelkach czy pojemnikach (np. transparentnych, półprzezroczystych i oranżowych), w organicznych rozpuszczalnikach i roztworach wodnych.
Wykrywacz cechuje się dwukrotną redukcją kosztów użytkowania, od 5 do 16 razy szybszą analizą substancji, 8-godzinną (maks.) pracą na wbudowanym akumulatorze.
G-Scan Pro LDS 4500-G jest dostępny w sklepie detektywistycznym Spy Shop. Istnieje możliwość umówienia się na testy sprzętu.

TOP 50 SECURITY 2016

Jill Lai a&s International

Liderzy rynku security

PIERWSZA „DZIESIĄTKA” NA ŚWIECIE

(na podstawie przychodów ze sprzedaży produktów w 2015 r.)

1	HIKVISION DIGITAL TECHNOLOGY
2	HONEYWELL SECURITY & FIRE
3	BOSCH SECURITY SYSTEMS
4	DAHUA TECHNOLOGY
5	SAFRAN IDENTITY & SECURITY
6	ASSA ABLOY
7	TYCO SECURITY PRODUCTS
8	AXIS COMMUNICATIONS
9	FLIR SYSTEMS
10	AIPHONE

Źródło: Ranking TOP 50, *a&s International*

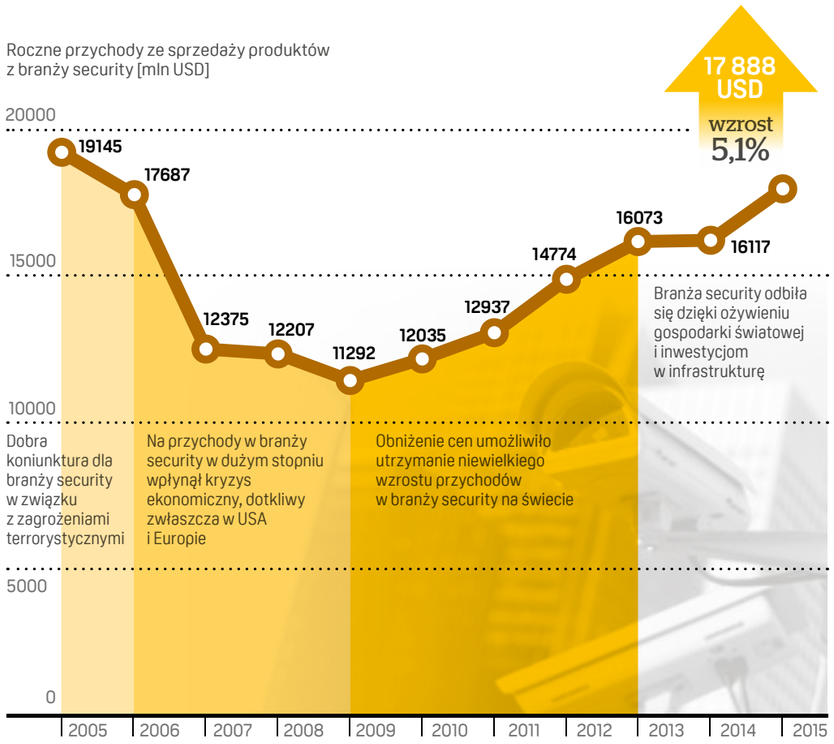
Miesięcznik *a&s International* co roku publikuje ranking TOP 50 branży security. Po raz pierwszy również Czytelnicy w Polsce mają okazję poznać listę pięćdziesięciu największych firm o ugruntowanej globalnej pozycji w branży.
Ranking powstał na podstawie przychodów spółek ze sprzedaży produktów zabezpieczeń technicznych w 2015 r.

Pierwszych dziesięć firm z listy TOP 50 uzyskało imponujące wyniki. Niektóre z nich w 2015 r. zanotowały rekordowe wskaźniki wzrostu, inne – zwłaszcza te mające siedziby w Azji (z wyłączeniem Chin) – musiały uporać się z pewnymi trudnościami.

W najnowszym rankingu pojawiło się pięć nowych firm. Oferują one niszowe technologie lub są markami z mocną pozycją na rynku.
Raport na temat 50 największych firm branży security został podzielony na trzy części: analiza rynku za lata 2015 i 2016, raport firmy badawczej Memoori na temat rynku zabezpieczeń technicznych w 2016 r. oraz lista rankingowa a&s TOP 50 security na świecie. Oto najważniejsze informacje na temat branży zabezpieczeń technicznych w 2015 i 2016 r.

A&S TOP 50 SECURITY W LATACH 2005–2015

Roczne przychody ze sprzedaży firm ujętych w rankingu



Wykres przedstawiający roczne przychody firm ujętych w rankingu a&s TOP 50 w latach 2005–2015 pokazuje wpływ kondycji gospodarki światowej oraz zagrożeń terrorystycznych na branżę security w ciągu ostatnich 11 lat. Postępująca konkurencja cenowa jest testem dla wszystkich firm z branży pod kątem umiejętności dostosowania się do nowych warunków na rynku.

W ostatnich dwóch latach większość producentów z branży security na świecie stanęła przed nowymi wyzwaniami. Głównym problemem nie były jednak zmiany globalnego zapotrzebowania na produkty security ani słabszy rozwój gospodarczy niektórych państw. We wszystkich regionach na całym świecie producenci musieli zmierzyć się z tym samym problemem – coraz silniejszą konkurencją cenową. Rywalizacja w tym obszarze z roku na rok jest coraz większa.

Znaczne obniżanie średnich cen urządzeń, obserwowane szczególnie w przypadku kamer IP, przekłada się bezpośrednio na wyraźne zmniejszenie zysków ich wytwórców.

Analitycy z branży security potwierdzają, że w 2015 r. wzrost obrotów na światowym rynku sprzętu dozoru wizyjnego uległ znacznemu spowolnieniu. Zgodnie z raportem brytyjskiego ośrodka badawczego Memoori rynek produktów zabezpieczeń technicznych w 2015 r. zwiększył się o 4,5%. Oznacza to duży spadek tempa wzrostu w porównaniu do 8,2% rocznego wzrostu, który odnotowano w ciągu ostatnich pięciu lat. Inna firma badawcza – IHS – przedstawiła jeszcze gorsze statystyki. Analityk IHS wyliczył, że w 2015 r. światowy rynek profesjonalnego sprzętu dozoru wizyjnego wzrósł zaledwie o 1,9%, biorąc pod uwagę przychody. Jest to uderzająca różnica w porównaniu do 14,2% w 2014 r. i 6,8% w 2013 r. W rankingu „a&s" TOP 50 przygotowanym w 2016 r. średni wskaźnik wzrostu największych pięćdziesięciu firm branży security był wyższy niż rok wcześniej i wynosił 5,1%, przy czym firma, która zajęła 50. pozycję, uzyskała przychody na poziomie zaledwie 4,9 mln USD. Rok wcześniej spółka na tym samym miejscu w rankingu odnotowała przychody w wysokości 19,4 mln USD. Spadkowi uległy więc podstawowe wskaźniki dotyczące rocznych przychodów ze sprzedaży produktów dla firm z branży security na świecie.

Jon Cropley, główny analityk ds. rynku telewizji dozorowej w firmie IHS, w ten sposób zdiagnozował problem: *w ostatnich latach ceny sprzętu szybko spadały. Przykładem jest m.in. średnia cena sieciowej kamery dozorowej, która w 2010 r. wynosiła ok. 500 USD, w 2015 r. natomiast nie przekraczała 130 USD. Sprzedawcy chińscy często oferowali produkty w niższych cenach niż ich konkurenci zachodni, w związku z czym zdobyli większy udział w rynku.*

Pierwsza dziesiątka odzwierciedla sytuację na świecie

Dziesięć największych firm – pierwszych na liście – uzyskało przychód wynoszący ok. 14 mld USD, co stanowi 80% przychodów wszystkich 50 firm uwzględnionych w rankingu. Takie wyniki są dowodem na ich dominację w branży i wyjątkowo wysoki udział w rynku globalnym. Co istotne, dziesięć największych firm radziło sobie dobrze pod względem zarówno wzrostu przychodów, jak i poziomu zysku. Ci dostawcy rozwiązań z zakresu zabezpieczeń technicznych umocnili swoją pozycję w ciągu ostatnich pięciu lat.

Firma badawcza IHS zauważyła również, że na rynku telewizji dozorowej w 2015 r. piętnastu największych dostawców wygenerowało 55% przychodów całego rynku dozoru wizyjnego.

Dynamiczny wzrost na rynku kontroli dostępu

Podobne wzrosty, jak dwie chińskie firmy z branży „telewizyjnej" z pierwszej dziesiątki rankingu, odnotowały także dwie firmy reprezentujące rynek kontroli dostępu. Rekordowy wynik odnotowały ASSA ABLOY i Safran Identity & Security. Ich dynamiczny rozwój obrazuje ożywienie na rynku kontroli dostępu, tłumaczone migracją użytkowników końcowych od mechanicznych do elektronicznych urządzeń i systemów kontroli dostępu oraz wprowadzeniem do oferty wielu innowacji technologicznych w dziedzinie kontroli dostępu i identyfikacji.

Podobne dane prezentują badania IHS. W 2015 r. światowy rynek kontroli dostępu odnotował dynamiczny wzrost (o 6,6%). Oczekuje się też, że wskaźnik wzrostu za rok 2016 zwiększy się jeszcze bardziej i osiągnie 7,2%.

Oznacza to, że rynek kontroli dostępu notuje teraz lepsze wyniki niż rynek telewizji dozorowej.

– *To doskonały czas dla podmiotów działających w branży security. Po dwudziestu latach ewolucji – od prostych plakietek z identyfikatorami po inteligentne karty, oparte na standardach systemy kontroli dostępu i rozwiązania mobilne – branża wkracza w nowy rozdział swojej historii: erę tożsamości połączonych w sieci.*

Dziesięć największych firm uzyskało przychód wynoszący ok. 14 mld USD, co stanowi 80% przychodów wszystkich 50 firm uwzględnionych w rankingu. Takie wyniki są dowodem na ich dominację w branży i wyjątkowo wysoki udział w rynku globalnym.

Będą one stosowane w różnych urządzeniach przez stale zwiększającą się liczbę kompatybilnych ze sobą aplikacji– podkreślił Stefan Widing, prezes i dyrektor generalny HID Global.
W sprawozdaniu ASSA ABLOY obejmującym oddział EMEA (Europa, Bliski Wschód i Afryka) zauważono także, że „w 2016 r. zapotrzebowanie na rozwiązania elektromechaniczne znacznie wzrosło. Skupienie się na innowacjach i nowych produktach wzmocniło obecność firmy na rynkach wschodzących, a nieustannie wdrażane środki poprawy efektywności przekładały się na dobry wskaźnik rentowności sprzedaży oddziału EMEA". Nowa w rankingu francuska firma Safran Identity & Security również rozwijała się dynamicznie, odnotowując wzrost obrotów o 23,7%. W sprawozdaniu Safran wskazuje, że największe przychody uzyskała w Stanach Zjednoczonych, gdzie dostarcza 85% wszystkich dokumentów praw jazdy i jest głównym dostawcą technologii biometrycznych na potrzeby FBI. Do rozwoju firmy w latach 2015–2016 w dużym stopniu przyczyniły się także inne projekty realizowane w USA, m.in. dotyczące dowodów osobistych, elektronicznych dowodów osobistych i paszportów oraz kontroli granicznej. Obecnie firma prowadzi negocjacje z funduszem Advent International, licząc na pomoc w osiąganiu dalszego rozwoju.

Według Baudouina Genouville'a, dyrektora ds. globalnych partnerstw w firmie Suprema, w branży kontroli dostępu jest widoczna tendencja do integracji wielu technologii, mającej rozwiązać więcej niż jeden problem użytkownika. Klienci firmy Suprema zostali podzieleni na trzy grupy. Ci, którzy kupują wyłącznie systemy kontroli dostępu, stanowią 25%. Kolejne 25% to osoby zainteresowane jedynie systemami do rejestracji czasu pracy. Pozostali (50%) szukają zintegrowanych rozwiązań z zakresu kontroli dostępu i rejestracji czasu pracy.
– *Oznacza to, że chcą oni nie tylko otwierać drzwi za pomocą naszych produktów, ale też używać tych rozwiązań do zarządzania czasem pracy i łączyć je z oprogramowaniem do zarządzania zasobami ludzkimi. Chcą, aby dział HR mógł zaoszczędzić czas i uniknąć błędów, które mogą się pojawić przy realizacji tych czynności na papierze lub w plikach Excel* – powiedział Baudouin Genouville. – *Połowa naszych klientów jest zainteresowana systemem zintegrowanym, dlatego interesuje się także technologiami biometrycznymi. Nie chodzi tylko o bezpieczeństwo, ale także o zarządzanie zasobami ludzkimi. Dotyczy to naszych klientów na całym świecie, w tym duże sieci restauracji szybkiej obsługi, takie jak Burger King czy sieci supermarketów jak Carrefour.*

Więcej dostawców kompleksowych rozwiązań dozoru wizyjnego

Na rynku telewizji dozorowej – zgodnie z przewidywaniami większości specjalistów branżowych i prognozami zawartymi w ostatnim raporcie IHS – największą firmą w branży security na świecie pod względem przychodów w 2015 r. został Hikvision Digital Technology. Po latach inwestowania w poprawę jakości produktów i wsparcia technicznego firma stała się dostawcą kompleksowych rozwiązań z zakresu dozoru wizyjnego, a jej produkty zostały dostosowane do wszystkich rodzajów rynków i branż. Firma uruchomiła swoje oddziały i przedstawicielstwa w wielu krajach na każdym kontynencie, a pięć ostatnich lat było okresem jej najszybszego rozwoju. Hikvision wraz ze swoim największym konkurentem – firmą Dahua Technology, która uplasowała się tuż za podium (4. miejsce w rankingu) – oraz innymi producentami chińskimi mieli największy wpływ na zmiany na globalnym rynku, zaostrzając konkurencję cenową. Te zmiany są też widoczne w wynikach sprzedaży.
W przeciwieństwie do pozostałych ośmiu firm z pierwszej dziesiątki Hikvision i Dahua notują największe wzrosty obrotów.
Na drugie miejsce w rankingu przesunęła się firma Honeywell, która wykazuje przychody ze sprzedaży produktów w dwóch działach: bezpieczeństwo pożarowe i zabezpieczenia techniczne. Firma Bosch Security Systems plasuje się na trzeciej pozycji – tę samą zajmowała w poprzedniej edycji rankingu. Wdrożyła liczne innowacje technologiczne, m.in. zapewniające uzyskanie dobrego obrazu w warunkach słabego oświetlenia, odświeżone oprogramowanie do zarządzania systemem telewizji dozorowej i kontroli dostępu oraz systemy automatyki budynkowej. Dzięki temu w 2015 r. osiągnęła rekordowy 10-procentowy wzrost. Pod koniec 2016 r. Bosch poinformował, że w roku 2017 połączy siły z Sony, aby podjąć współpracę m.in. w zakresie rozwiązań innowacyjnych oraz IoT.
Rekordowy wzrost zanotowała też firma Axis Communications pomimo trudności, jakie napotyka na części rynków rozwijających się, takich jak Chiny i Rosja oraz niektóre kraje europejskie. Zamierza teraz rozszerzać swoje portfolio o produkty wykraczające poza branżę telewizji dozorowej, by oferować klientom systemy zintegrowane.
Kolejny dostawca kompleksowych rozwiązań, Tyco Security Systems, utrzymuje stabilną pozycję. W roku 2015 firma osiągnęła nieznaczny, dwuprocentowy wzrost, podczas gdy rok wcześniej wyniósł on aż 16,9%. Mimo to Tyco Security Systems nadal zajmuje siódme miejsce w rankingu.

Dostawcy rozwiązań z zakresu dozoru wizyjnego, którzy znaleźli się w pierwszej dziesiątce rankingu, utrzymali roczny wzrost przychodów. Prawdopodobnie najważniejszym czynnikiem ich sukcesu jest wysoki poziom zagrożeń terrorystycznych na świecie, co wpływa na decyzje zakupowe klientów. Jednocześnie szybko reagowali na zmiany na rynku, rozwijali nowe zastosowania i wykraczali poza tradycyjne obszary swojej działalności dzięki fuzjom, przejęciom lub nawiązywaniu strategicznych partnerstw.

Automatyka budynkowa i inteligenty dom

Gdy coraz więcej firm zaczyna opracowywać kompleksowe rozwiązania, oznacza to, że najważniejsze technologie i główne kanały sprzedaży osiągnęły już wysoki poziom dojrzałości. To jednocześnie sygnał, że branża będzie nadal podlegać konsolidacji. Jak więc potoczą się losy 50 największych firm security? Dużo uwagi przyciągnęły niedawne przejęcia i wydzielenia spółek związane z automatyką budynkową i tzw. inteligentnym budynkiem.

Wydzielona została spółka Honeywell Security & Fire, która obecnie funkcjonuje w ramach oddziału zajmującego się produktami związanymi z automatyką.
– *Honeywell już teraz wytwarza wiele produktów i systemów przydatnych w zarządzaniu budynkiem począwszy od systemów security i ppoż., skończywszy na instalacjach grzewczych, wentylacyjnych i klimatyzacyjnych oraz systemach zarządzania budynkiem. W związku z tym mamy możliwość oferowania systemów zintegrowanych, które perfekcyjnie współpracują i są niezawodne* – podkreślił James Somerville Smith, North European Channel Marketing Leader w Honeywell Security & Fire.
Climatec, podmiot zależny firmy Bosch z siedzibą w Stanach Zjednoczonych, poinformował z kolei o przejęciu Skyline Automation, która specjalizuje się w automatyce budynkowej i inte-

RANKING TOP 50 SECURITY

Ranking obejmuje 50 największych producentów notowanych na giełdzie, biorąc pod uwagę wyłącznie przychody ze sprzedaży produktów, zysk brutto i marżę podane w ich sprawozdaniach finansowych za rok podatkowy 2015.

W rankingu ujęto zarówno firmy zajmujące się wyłącznie produkcją urządzeń, jak i dostawców kompleksowych rozwiązań. Analizując listę, warto poznać źródła sukcesów omawianych firm i przemyśleć wnioski, nie skupiając się na ich miejscach w rankingu.

Uwaga: redakcja „a&s International" nie ponosi żadnej odpowiedzialności za informacje finansowe przekazane przez poszczególne firmy. Aby umożliwić porównanie wyników, waluty inne niż dolar amerykański przeliczono po średnim kursie wymiany walut z dnia 11 lipca 2016 r. podawanym przez XE.com. Prezentowany ranking jest zestawieniem obiektywnym, opracowanym na podstawie informacji na temat wyników sprzedaży udostępnionych przez uczestników rankingu.

Hikvision i jego największy konkurent, Dahua Technology, oraz inni producenci chińscy mieli ogromny wpływ na zmiany na globalnym rynku, zaostrzając konkurencję cenową.

gracji systemów. Oferuje przy tym usługi instalacyjne i integracyjne różnych systemów działających w budynkach.
– *Dzięki przejęciu Skyline poszerzamy naszą działalność oraz wzmacniamy obecność na rynku amerykańskim, który charakteryzuje się stabilnym wzrostem* – ocenił Stefan Hartung, członek zarządu w Robert Bosch, odpowiedzialny za dział Energy and Building Technology.
Automatyka budynkowa i inteligentny dom będą zapewne pierwszymi odbiorcami korzystającymi z rozwiązań IoT, których centrum mogą stanowić systemy zabezpieczeń. Firma Bosch stale prowadzi w tym zakresie prace R&D, które zaowocują także rozwojem dla działu security. Bosch powołał już spółkę zależną Robert Bosch Smart Home, mającą na celu prowadzenie działalności związanej z inteligentnymi budynkami.

Pomimo mody na rozwiązania IoT zagrożenia cyberbezpieczeństwa spędzają sen z powiek, zwłaszcza że praca w sieci dotyczy coraz większej liczby urządzeń.

Możliwości rozwoju w obszarze inteligentnych budynków szuka także Fermax, znana na świecie firma zajmująca się systemami domofonowymi. – *Oprócz naszych dobrze znanych systemów domofonowych oferujemy także rozwiązania kompleksowe z zakresu kontroli dostępu, automatyki domowej oraz dozoru wizyjnego, które wykorzystują najnowsze technologie ułatwiające instalację* – powiedział Jeremy Palacio, dyrektor zarządzający Fermax Electronica.
Wzmocnienie pozycji poprzez możliwość oferowania kompleksowych rozwiązań mają także na celu duże przejęcia na rynku: Tyco Security Products przez Johnson Controls oraz Point Grey Research, producenta systemów wizyjnych na potrzeby automatyki przemysłowej, przez FLIR Systems. Z kolei MOBOTIX został kupiony przez firmę Konica Minolta, działającą głównie w obszarze urządzeń drukujących dla inteligentnych biur.
Fuzje i przejęcia oraz partnerstwa strategiczne wydają się teraz najszybszym sposobem dla dużych światowych firm do poszerzania działalności i pozyskiwania nowych klientów.

Obawy o cyberbezpieczeństwo: czy Chińczycy utrzymają wpływy?

Internet rzeczy (IoT) i big data to dwa główne trendy, które sprawią, że firmy będą musiały skupić się na konkretnych segmentach rynków i dostosowanych do nich specyficznych zastosowaniach bądź przeprowadzić głębokie zmiany swoich technologii i usług. Pomimo mody na rozwiązania IoT zagrożenia cyberbezpieczeństwa spędzają sen z powiek, zwłaszcza że praca w sieci dotyczy coraz większej liczby urządzeń. Kwestie cyberbezpieczeństwa mają również kluczowe znaczenie dla systemów zabezpieczeń technicznych.
Do historii przejdzie 21 października 2016 r. W tym dniu serwisy internetowe i kilka większych witryn na Wschodnim Wybrzeżu Stanów Zjednoczonych padły ofiarą cyberataku. Branża zabezpieczeń technicznych uświadomiła sobie wtedy kilka ważnych rzeczy. Krebs on Security, popularny blog na temat bezpieczeństwa cybernetycznego i badań nad bezpieczeństwem, poinformował, że „według specjalistów z zajmującej się bezpieczeństwem firmy Flashpoint atak został przypuszczony przynajmniej w pewnej części za pomocą botnetu Mirai" (botnet – grupa komputerów zainfekowanych złośliwym oprogramowaniem, pozostającym w ukryciu przed użytkownikiem i pozwalającym na zdalną kontrolę nad wszystkimi komputerami w ramach botnetu).
Allison Nixon, dyrektor ds. badań w firmie Flashpoint, poinformowała, że botnet wykorzystany do przeprowadzenia tego ataku został zbudowany ze zhakowanych urządzeń IoT, a zwłaszcza zainfekowanych rejestratorów DVR i kamer IP wyprodukowanych przez chińską firmę XiongMai Technologies. Co ważne, XiongMai jest producentem podzespołów, które inni dostawcy montują we własnych produktach. Te podzespoły do rejestratorów DVR i kamer IP są stosowane przez wiele dużych firm chińskich, które są producentami OEM lub dystrybuują urządzenia w ramach własnych kanałów sprzedaży.
Za „nieszczelności" są obwiniane nie tylko produkty firmy XiongMai, ale także większości producentów z Państwa Środka. Wprawdzie nie wszystkie produkty chińskie mają problemy z cyberbezpieczeństwem, ale klienci i użytkownicy powinni wziąć to pod uwagę przy nawiązywaniu współpracy z partnerami z różnych części świata.
Czy obawy związane z cyberbezpieczeństwem lub innymi aspektami politycznymi będą stanowić przeszkodę w rozwoju firm chińskich? Czy problemy z tym związane przyciągną klientów z powrotem do innych producentów azjatyckich (tajwańskich i koreańskich) lub zachodnich? W najbliższym czasie okaże się, jak specjaliści z branży security ocenią partnerów chińskich i jak chińskie firmy zareagują na obawy klientów. Jedno jest pewne: duże przedsiębiorstwa z branży zabezpieczeń już zaczęły traktować cyberbezpieczeństwo jako najwyższy priorytet w projektowaniu urządzeń i systemów zabezpieczeń. W branży security panuje powszechna zgoda co do tego, że w erze IoT w żadnym wypadku nie można zbagatelizować zagrożenia cybernetycznego. Można się więc spodziewać, że w najbliższej przyszłości nastąpią kolejne przejęcia firm – tym razem zajmujących się bezpieczeństwem cybernetycznym.

Polski rynek security

Jak na tle globalnego rynku wyglądają polskie firmy branży zabezpieczeń technicznych? Żaden spośród nielicznych polskich producentów nie trafił na listę największych na świecie. Wśród pierwszej „pięćdziesiątki" aż 24 firmy mają siedziby w Azji, europejskich producentów reprezentuje zaledwie 14 firm.
Badanie światowego rynku security „a&s International" przeprowadza już 13 lat. Podobne badania prowadzone są także na rynkach lokalnych. W tym roku po raz pierwszy poddamy analizie także polski rynek zabezpieczeń technicznych. Sprawdzimy, które firmy w Polsce osiągają największe obroty, którzy producenci odnoszą sukcesy, a którym nie wiedzie się najlepiej. Przebadamy, czy – tak jak na rynku globalnym – największą sprzedażą mogą się pochwalić producenci z Dalekiego Wschodu, czy może nieliczne polskie firmy nadal cieszą się u nas dużą popularnością.

Badanie *a&s TOP 20 polskiego rynku security* będzie listą rankingową firm o najwyższych przychodach w naszym kraju. Wraz z rankingiem opublikujemy jego obszerną analizę i podsumowanie, które opracują dla nas specjaliści ds. badania rynku. Ogłoszenie wyników badań zaplanowaliśmy na czerwiec tego roku.

WARUNKI UDZIAŁU W RANKINGU TOP 50

- W rankingu mogą uczestniczyć dostawcy urządzeń i systemów z branży security, w tym produktów telewizji dozorowej, kontroli dostępu, sygnalizacji włamania i napadu oraz produktów z więcej niż jednego z tych segmentów.
- Producenci urządzeń wytwarzający pod własną marką lub na zlecenie innych firm.
- Tylko firmy notowane na giełdzie.
(Uwaga: co roku miesięcznik *a&s International* uwzględnia również niewielką liczbę międzynarodowych firm nienotowanych na giełdzie, które udostępniają swoje poświadczone sprawozdania roczne. Ich udział w rankingu jest dokładnie analizowany pod kątem rozpoznawalności marki oraz udziału firmy w rynku międzynarodowym).
- Udział mogą wziąć firmy, które dostarczą sprawozdania finansowe za pełny rok 2014, pełny rok 2015 oraz za pierwszą połowę 2016 r. Sprawozdania muszą być sprawdzone lub zatwierdzone przez biegłego rewidenta.

W rankingu nie są uwzględniani: dystrybutorzy, integratorzy systemów, resellerzy, dealerzy, instalatorzy, agencje ochrony osób i mienia, firmy z branży bezpieczeństwa informacji i ochrony przeciwpożarowej oraz przychody powiązane z działalnością w tych obszarach.

TOP 50 SECURITY 2016

światowi liderzy SECURITY

Ranking 2016	Ranking 2015	NAZWA FIRMY	SIEDZIBA	GŁÓWNY OBSZAR DZIAŁANIA	PRZYCHODY W 2015 (MLN USD)	PRZYCHODY W 2014 (MLN USD)	WZROST PRZYCHODÓW (2014-2015)	WZROST ZYSKU (2014-2015)	MARŻA W 2015	ZYSK NETTO 2015 (MLN USD)	ZYSK NETTO 2014 (MLN USD)
1	2	**HIKVISION DIGITAL TECHNOLOGY**	Chiny	telewizja dozorowa	3522,5	2453,8	43,6%	29,7%	28,6%	878,7	699,2
2	1	**HONEYWELL SECURITY & FIRE**	USA	różne	2900,0	2800,0	3,6%				
3	3	**BOSCH SECURITY SYSTEMS**	Niemcy	różne	1538,5	1387,2	10,9%				
4	5	**DAHUA TECHNOLOGY**	Chiny	telewizja dozorowa	1505,5	1095,3	37,5%	26,0%	15,7%	206,3	170,9
5	4	**SAFRAN IDENTITY & SECURITY**	Francja	kontrola dostępu	1354,7	1094,8	23,7%				
6	6	**ASSA ABLOY** (Global Technologies)	Szwecja	kontrola dostępu	1061,2	840,5	26,3%				
7	7	**TYCO SECURITY PRODUCTS** (część Johnson Controls)	USA	różne	775,0	760,0	2,0%				
8	10	**AXIS COMMUNICATIONS**	Szwecja	telewizja dozorowa	773,7	635,5	21,7%	19,5%	50,8%	76,0	62,9
9	8	**FLIR SYSTEMS** (Surveillance & Security)	USA	telewizja dozorowa	729,6	699,1	4,4%				
10	12	**AIPHONE**	Japonia	systemy domofonowe	423,9	412,7	2,7%				
11	11	**ALLEGION** (Electronic Products & Access Control)	USA	kontrola dostępu	413,6	423,7	-2,4%				
12	14	**AVIGILON**	Kanada	telewizja dozorowa	281,4	206,8	36,1%	37,9%	57,4%		
13	17	**INFINOVA**	USA	telewizja dozorowa	270,8	146,3	85,1%	83,5%	3,8%	10,3	5,0
14	18	**OPTEX** (Security Sensors)	Japonia	sygn. włamania i napadu	141,1	129,3	9,2%				
15	16	**NEDAP**	Holandia	kontrola dostępu	138,2	139,0	-0,6%			4,2	16,2
16	13	**TKH GROUP** (Vision & Security Systems)	Holandia	telewizja dozorowa	135,3	84,7	59,8%				
17	22	**IDIS**	Korea Płd.	telewizja dozorowa	127,8	102,4	24,8%	17,1%	33,7%		
18	21	**TAMRON** (optyka Commercial/Industrial)	Japonia	telewizja dozorowa	127,1	125,7	1,1%				
19	20	**VIVOTEK**	Tajwan	telewizja dozorowa	120,4	104,8	14,9%	12,5%	37,2%	14,7	11,4
20	19	**VERINT SYSTEMS** (Video Intelligence)	USA	telewizja dozorowa	118,9	110,4	7,8%				

Ranking 2016	Ranking 2015	NAZWA FIRMY	SIEDZIBA	GŁÓWNY OBSZAR DZIAŁANIA	PRZYCHODY W 2015 (MLN USD)	PRZYCHODY W 2014 (MLN USD)	WZROST PRZYCHODÓW (2014-2015)	WZROST ZYSKU (2014-2015)	MARŻA W 2015	ZYSK NETTO 2015 (MLN USD)	ZYSK NETTO 2014 (MLN USD)
21	23	**COMMAX**	Korea Płd.	różne	99,6	95,6	4,2%	7,7%	22,3%		
22	24	**KOCOM**	Korea Płd.	różne	96,6	90,3	7,0%	14,7%	28,1%		
23	29	**MILESTONE SYSTEMS**	Dania	telewizja dozorowa	89,4	68,0	31,4%				
24	27	**NAPCO SECURITY SYSTEMS**	USA	różne	77,8	74,4	4,5%	9,8%		4,8	3,5
25	25	**MOBOTIX**	Niemcy	telewizja dozorowa	72,6	71,1	2,1%			3,7	1,0
26	26	**DYNACOLOR**	Tajwan	telewizja dozorowa	70,3	81,4	-13,6%	-15,8%	39,3%	1,5	15,9
27	28	**GEOVISION**	Tajwan	telewizja dozorowa	65,7	69,0	-4,8%	-11,9%	49,1%	10,9	15,2
28	38	**HDPRO**	Korea Płd.	telewizja dozorowa	64,0	57,6	11,2%	4,0%	12,8%		
29	**NOWA**	**IDENTIV**	USA	kontrola dostępu	60,8	81,2	-25,2%	-30,8%	38,1%		
30	30	**GEUTEBRUECK**	Niemcy	telewizja dozorowa	59,0	55,1	7,1%				
31	34	**SUPREMA**	Korea Płd.	kontrola dostępu	52,1	57,3	-9,2%	-12,2%	46,2%		
32	33	**AVTECH**	Tajwan	telewizja dozorowa	50,0	59,5	-16,0%	-38,5%	21,7%		
33	37	**DALI TECHNOLOGY**	Chiny	telewizja dozorowa	48,3	54,1	-10,8%	-38,1%	11,0%	4,8	7,6
34	32	**HITRON SYSTEMS**	Korea Płd.	telewizja dozorowa	47,5	63,0	-24,5%	-13,4%	6,1%		
35	35	**INDIGOVISION**	Wlk. Brytania	telewizja dozorowa	47,1	82,5	-42,9%	-49,3%	51,4%	-1,0	5,8
36	41	**FERMAX**	Hiszpania	systemy domofonowe	46,5	40,1	16,0%	12,8%	55,9%		
37	44	**VICON INDUSTRIES**	USA	telewizja dozorowa	44,9	34,9	28,7%	45,2%	39,3%		
38	46	**C-PRO ELECTRONICS**	Korea Płd.	telewizja dozorowa	36,0	33,5	7,4%	-3,0%	20,0%		
39	39	**EVERFOCUS ELECTRONICS**	Tajwan	telewizja dozorowa	35,9	50,8	-29,3%	-40,0%	24,7%	-5,5	-4,0
40	**NOWA**	**ACTI**	Tajwan	telewizja dozorowa	35,8	40,1	-10,6%	-16,4%	50,0%	0,4	0,4
41	**NOWA**	**COSTAR TECHNOLOGIES**	USA	telewizja dozorowa	33,7	36,1	-6,6%	-2,7%	39,2%	0,5	10,5
42	45	**INCON**	Korea Płd.	telewizja dozorowa	31,4	33,7	-6,6%	-12,6%	25,8%		
43	36	**ITX SECURITY**	Korea Płd.	telewizja dozorowa	30,9	58,8	-47,4%	-84,1%	5,6%	-13,0	-2,2
44	43	**MAGAL SECURITY SYSTEMS** (Perimeter Products)	Izrael	różne	30,8	37,6	-18,1%				
45	40	**SYNECTICS** (System Division)	Wlk. Brytania	telewizja dozorowa	25,2	24,6	2,5%	29,7%	4,1%		
46	48	**HI SHARP**	Tajwan	telewizja dozorowa	22,9	23,7	-3,5%	13,5%	20,5%	0,2	-0,5
47	49	**HUNT ELECTRONIC**	Tajwan	telewizja dozorowa	17,2	22,9	-24,8%	-30,5%	33,8%	1,0	2,7
48	**NOWA**	**DIGITAL BARRIERS** (Solutions Division)	Wlk. Brytania	telewizja dozorowa	16,3	9,2	77,0%	104,0%	49,8%	-9,7	-13,8
49	47	**EVERSPRING INDUSTRY**	Tajwan	różne	15,8	30,4	-48,0%	-63,2%	26,2%	5,3	-2,4
50	**NOWA**	**AXXONSOFT**	Rosja	telewizja dozorowa	4,9	5,9	-16,6%	-15,2%	72,7%	-0,2	0,1
				RAZEM	**17 888,2**	**15 294,1**	**5,1%**				

Spowolnienie wzrostu budzi obawy o kondycję rynku

Wartość globalnych obrotów na rynku zabezpieczeń technicznych zwiększyła się, ale **wiele czynników, m.in. umocnienie producentów chińskich, niekorzystnie wpłynęło na tempo wzrostu w segmencie telewizji dozorowej.**

Allan McHale
dyrektor,
Memoori Business Intelligence

Raport Memoori za rok 2016 pokazuje, że łączna wartość światowej produkcji urządzeń zabezpieczeń technicznych (w cenach producenta) wyniosła 28,4 mld dol., co oznacza 4,5-procentowy wzrost w porównaniu z 2015 r. W ciągu ostatnich pięciu lat średni roczny wzrost obrotów (CAGR) wyniósł 8,2%, ale zanotowano znaczny spadek jego dynamiki w ostatnich dwóch latach. Udział sprzedaży produktów dozoru wizyjnego w sprzedaży całej branży security wynosi 53% (blisko 15 mld dol.), kontroli dostępu – 24% (6,8 mld dol.), sygnalizacji włamania i napadu – 23% (6,6 mld dol.).

Segment kontroli dostępu utrzymał dotychczasową stopę wzrostu, wynoszącą ok. 10%. Producenci z roku na rok coraz bardziej angażowali się w rozwiązania IP i systemy bezprzewodowe oraz biometrię. Po raz drugi z rzędu segment ten wykazał najwyższą roczną stopę wzrostu w całej branży security.

Rynek systemów sygnalizacji włamania i napadu, „ojciec" zabezpieczeń technicznych, już dawno osiągnął dojrzałość. Mimo to także w tym segmencie są wprowadzane innowacje, a coraz częstsze wykorzystanie radarów i kamer termowizyjnych przyczyniło się do uzyskania 3,5-procentowego wzrostu w 2016 r.

W telewizji dozorowej tempo wzrostu zmniejszyło się do 4,2%. Jednocześnie wolumen sprzedaży rósł stabilnie, co oznacza, że znacznie spadły ceny jednostkowe produktów, głównie za sprawą polityki największych producentów chińskich, którzy rozpoczęli agresywną konkurencję cenową na rynkach zachodnich.

> Znacznie spadły ceny jednostkowe produktów telewizji dozorowej – głównie za sprawą polityki największych producentów chińskich, którzy rozpoczęli agresywną konkurencję cenową na rynkach zachodnich.

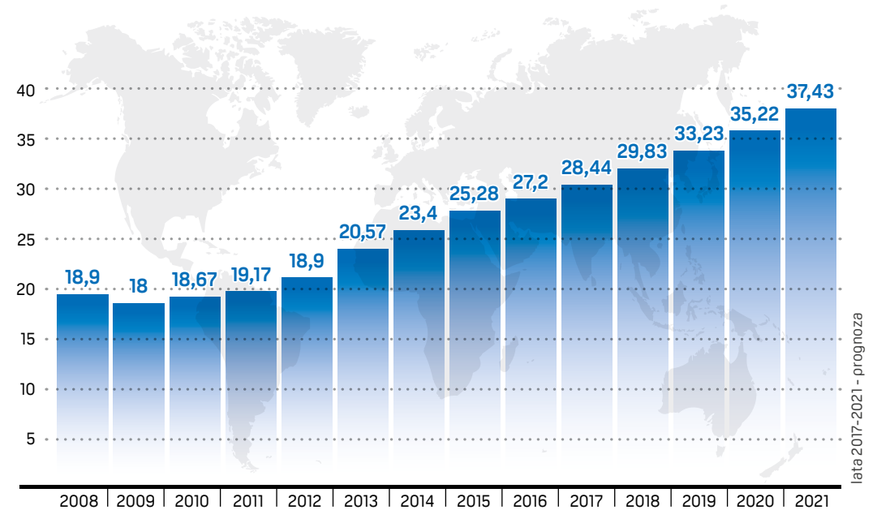
Rozwój regionalny

W roku 2016 największe zapotrzebowanie na zabezpieczenia techniczne odnotowano w Azji, głównie w Chinach. Nawet tam zanotowano jednak zmniejszenie zapotrzebowanie w porównaniu z rokiem 2015. Popyt w Ameryce Północnej można uznać za umiarkowany, najgorzej sytuacja przedstawiała się w Europie.
Prognoza Memoori na najbliższe pięć lat (2016–2021) zakłada powolną poprawę sytuacji gospodarczej na świecie oraz umiarkowany wzrost PKB w krajach rozwiniętych. W tym czasie prawdopodobnie nie uda się rozwiązać problemu terroryzmu, wzrosną zatem wydatki administracji rządowej przeznaczane na walkę z nim, co wpłynie korzystnie na kondycję rynku zabezpieczeń technicznych.
W sektorze komercyjnym zwiększy się zainteresowanie dalszym i głębszym integrowaniem ze sobą różnych systemów security, wspieranę przez technologię Internetu Rzeczy (Internet of Things, IoT). Kulminacja spodziewana jest w 2017 r., w kolejnych czterech latach popyt będzie rósł w stopniu umiarkowanym.
W pięcioleciu 2016–2021 średni roczny wzrost (CAGR) powinien wynieść średnio 5,7%. Nie jest to prognoza szczególnie optymistyczna, zważywszy że w burzliwym okresie od 2010 do końca 2015 r. udało się osiągnąć CAGR na poziomie 7,8%. Chociaż zwiększenie wolumenu sprzedaży znacznie przekroczy 10%, szansa na to, że wzrost przychodów ze sprzedaży osiągnie choćby połowę tej wartości, jest niewielka. Nadal będzie bowiem obserwowane obniżanie cen przez dużych producentów chińskich dążących do zwiększenia udziału w rynku i wielkości sprzedaży.
Rozwój rynku security jest stymulowany rozwojem technologii. Do tych, które mają dziś największą siłę oddziaływania, należą: VSaaS (*Video Surveillance as a Service* – dozór wizyjny jako usługa), ACaaS (*Access Control as a Service* – kontrola dostępu jako usługa), zarządzanie tożsamością (prawami dostępu do danych), biometria, analityka i platformy integrujące.

Chińscy producenci wymuszają zmiany

Obecnie głównym problemem wszystkich producentów zachodnich i pozostałych uczestników rynku telewizji dozorowej nie są jednak zawirowania spowodowane nowymi technologiami, lecz konieczność szybkiego wypracowania modelu biznesowego, umożliwiającego powstrzymanie napływającej fali produktów chińskich i konkurowanie z nimi.
Większość odnoszących sukcesy zachodnich producentów zabezpieczeń technicznych skoncentrowała swoją działalność na jednej dziedzinie, nieliczni zaś podjęli „specjalizację pionową", aby oferować rozwiązania kompleksowe. Nadal sprawdza się to w segmentach kontroli dostępu oraz sygnalizacji włamania i napadu.
W dziedzinie telewizji dozorowej natomiast zagrożenie ze strony dwóch znaczących producentów chińskich jest zbyt duże. Hikvision Digital Technology oraz Dahua Technology z powodzeniem zwiększają sprzedaż dzięki obniżaniu cen.
Korzystając ze specjalnych warunków na rodzimym rynku i pomocy finansowej ze strony rządu chińskiego, firmy te zdołały zrealizować swoje plany i z powodzeniem wkroczyły na rynki Ameryki Północnej i niektórych krajów Europy, w szybkim tempie zdobywając w nich udział. Obecnie lokują się odpowiednio na miejscach pierwszym i drugim wśród światowych producentów urządzeń dozoru wizyjnego i nie ma żadnych przesłanek, by wątpić, że strategia ta będzie kontynuowana.

SPRZEDAŻ PRODUKTÓW SECURITY NA ŚWIECIE
2008–2021 (w mld USD)



Gdy w 2009 r. „*a&s International*" po raz pierwszy opublikował raport na temat rynku zabezpieczeń technicznych, żadna z tych dwóch firm, założonych dopiero w 2001 r., nie była uważana za poważnego konkurenta na międzynarodowym rynku branżowym. Spółka Hikvision zadebiutowała w indeksie MŚP chińskiej Giełdy Papierów Wartościowych w Shenzhen w maju 2010 r. Obecnie jej kapitalizacja rynkowa przekracza 20 mld dol., a firma zatrudnia ponad 18 tys. osób i ma przedstawicielstwa na całym świecie.
Czy w tej sytuacji zachodni producenci z zakresu telewizji dozorowej zareagują i przekształcą własne modele biznesowe, by sprostać tej konkurencji? Czy dotychczasowi liderzy, tacy jak Axis, Avigilon, Bosch, Panasonic czy Hanwha (poprzednio Samsung), ograniczą marże, by zwiększyć wolumen sprzedaży? Czy raczej postanowią jeszcze więcej inwestować w rozwój coraz bardziej innowacyjnych produktów, które zapewniają korzystniejszy wskaźnik TCO *(total cost of ownership* – całkowity koszt zakupu, instalacji, użytkowania i utrzymania produktu)?
Nie w każdym segmencie rynku decyduje jednak cena, a wskaźnik TCO nie zaspokaja wszystkich potrzeb nabywców. Większość wymienionych spółek zachodnich będzie miała trudności z przekroczeniem progu przychodów na poziomie 1 mld dol., chyba że zrównają swoje marże z marżami konkurentów chińskich albo dostarczą produkty o korzystniejszym TCO, chcąc uzyskać większy udział w rynku. Prawdopodobnie wybiorą tę drugą możliwość, łącząc ją z uzyskaniem efektu skali w wyniki fuzji i przejęć.

W poszukiwaniu zwycięskiej strategii

Należy oczekiwać, że w takich okolicznościach firmy zachodnie podejmą bardziej agresywne działania w zakresie przejęć innych producentów urządzeń dozoru wizyjnego. W ten sposób będą mogły zwiększyć sprzedaż i dołączyć do beneficjentów nieuniknionego utowarowienia (zwiększenia podaży kamer telewizji dozorowej obniżającego ich ceny). Na razie jednak zjawisko to nie osiągnęło takiej skali, by mogło wpłynąć na zachodzące na rynku zmiany.
Dalsza ucieczka w specjalizację nie stanowi właściwego rozwiązania i zapewne spowoduje, że firmy, które obrały tę drogę, staną się ostatecznie dostawcami rozwiązań security, a nie ich producentami. Niektóre jednak, licząc na przełom w technologii IoT, mogą uznać tę strategię za opłacalną, pozostawiając producentom walkę na ceny i marże.

Dane zaczerpnięto z raportu Memoori
„The Physical Security Business 2016 to 2021"

Największe wzrosty premią za kompleksowość oferty

15 NAJSZYBCIEJ ROSNĄCYCH FIRM WG RANKINGU TOP 50

miejsce	firma	przychody w 2015 r.	przychody w 2014 r.	wzrost przychodów (2014–2015)
1	**Infinova**	270,85	146,31	85,1%
2	**Digital Barriers** (dział Solutions)	16,28	9,20	77,0%
3	**TKH Group** (Vision & Security Systems)	135,35	84,71	59,8%
4	**Hikvision Digital Technology**	3522,52	2453,85	43,6%
5	**Dahua Technology**	1505,45	1095,26	37,5%
6	**Avigilon**	281,41	206,75	36,1%
7	**Milestone Systems**	89,35	67,98	31,4%
8	**Vicon Industries**	44,88	34,88	28,7%
9	**ASSA ABLOY** (Global Technologies)	1061,23	840,47	26,3%
10	**IDIS**	127,78	102,39	24,8%
11	**Safran Identity & Security**	1354,65	1094,77	23,7%
12	**Axis Communications**	773,73	635,54	21,7%
13	**Fermax**	46,48	40,09	16,0%
14	**VIVOTEK**	120,39	104,78	14,9%
15	**HDPRO**	64,05	57,59	11,2%

William Pao
a&s International

Analiza listy firm, które zanotowały największy wzrost przychodów ze sprzedaży w 2015 r. wyraźnie wskazuje, że nie występuje prosta korelacja pomiędzy wielkością przychodów spółki a tempem ich wzrostu.
Na szczycie tego zestawienia znalazła się Infinova, która w rankingu TOP 50 (wg wielkości przychodów) zajmuje dopiero 13. miejsce. Ten amerykański producent systemów telewizji dozorowej odnotował jednak rekordowy wzrost sprzedaży o 85,1%, głównie za sprawą poszerzenia oferty produktowej po przejęciu March Networks (w 2012 r.) i Swann (w 2014 r.). Francuski Safran Identity & Security, który na głównej liście zajmuje 5. miejsce, zanotował wzrost w ub.r. o 23,7%, lokując się w tym zestawieniu na 11. pozycji.
Mimo że na liście 15. najszybciej rozwijających się firm znalazło się wiele znanych marek, jedna z nich wybija się w sposób szczególny. To Digital Barriers, brytyjski dostawca rozwiązań bezprzewodowych, po raz pierwszy uwzględniony w rankingu TOP 50. Wprawdzie na głównej liście zajmuje 48. pozycję, to pod względem wzrostu sprzedaży uplasował się na 2. miejscu, m.in. dzięki bliskim relacjom z administracją rządową USA, która korzysta z rozwiązań tej firmy do ochrony granic, na potrzeby służb mundurowych czy w siłach zbrojnych.
Spójność między wielkością przychodu a jej wzrostem można zaobserwować w przypadku firmy ASSA ABLOY, która zajmuje 6. miejsce pod względem łącznej wartości sprzedaży oraz 9. miejsce pod względem stopy wzrostu, która w efekcie powszechnej migracji rozwiązań kontroli dostępu do IP wyniosła 26,3%. Dział security w TKH Group odnotował 59,8-procentowy wzrost, zajmując 3. pozycję, do czego po części przyczyniły się przejęcie przez tę spółkę firmy Commend Group oraz zwiększenie przychodów ze sprzedaży zagranicznej dzięki dużym projektom międzynarodowym.
Szóste miejsce pod względem wzrostu zajmuje kanadyjski Avigilon, którego sprzedaż urosła o 36,1% dzięki umocnieniu pozycji firmy w Ameryce Północnej i regionie EMEA (Europa, Bliski Wschód, Afryka) oraz rozpoczęciu sprzedaży na rynkach APAC (Azja i Pacyfik) i LATAM (Ameryka Łacińska).

Cechą wspólną większości firm znajdujących się na liście TOP 15 jest oferowanie rozwiązań kompleksowych w zakresie telewizji dozorowej. Taka opcja umożliwia proponowanie pełnego pakietu integratorom, którzy mogą poczynić oszczędności już na etapie zakupu, a dzięki prowadzeniu konserwacji i napraw przez wybraną przez nich, tę samą firmę uzyskują dalsze oszczędności w trakcie eksploatacji.
Infinova np. udostępnia zarówno kamery i rejestratory NVR, jak i oprogramowanie zarządzające całym systemem. Ofertę dopełnia światłowodami do transmisji obrazu, dźwięku i danych, umożliwiając przesyłanie 128 strumieni wizyjnych w pojedynczym włóknie.
Również koreańska firma IDIS – zajmująca 10. lokatę w rankingu pod względem tempa wzrostu – dąży do zajęcia pozycji dostawcy rozwiązań kompleksowych z półek średniej i wysokiej. Proponuje bogatą gamę kamer, rejestratorów NVR i akcesoriów sieciowych, uzupełniając je oprogramowaniem do ich obsługi.
Firma Avigilon, która dotychczas kierowała produkty do średniego i wysokiego segmentu rynku, oferuje obecnie rozwiązania także w segmencie najniższym, zapewniając przy tym rozwiązania kompleksowe. – *Od dawna słyniemy z produktów wyjątkowej jakości, skierowanych do klientów średniego i wysokiego segmentu rynku oraz zróżnicowanej grupy, począwszy od firm małych i średnich, skończywszy na wielkich korporacjach* – powiedział Darren Seed, wiceprezes Avigilon. – *W II kwartale 2016 r. obniżyliśmy ceny serii kamer i rejestratorów NVR H3, rozszerzając w ten sposób zakres odbiorców, do których kierujemy nasze produkty. To posunięcie zostało bardzo dobrze przyjęte. Niedawno wprowadziliśmy też nową serię kamer H4 SL przeznaczoną raczej dla klientów początkujących. Zapewniamy wiele zróżnicowanych rozwiązań, gdyż Avigilon jest tak naprawdę dostawcą rozwiązań, a nie produktów. Kamera sama w sobie jest jedynie produktem, a my oferujemy całe rozwiązanie.*
Milestone Systems – w odróżnieniu od większości spółek, które rozwój zawdzięczają kompleksowej ofercie – zdecydował się pozostać przy oprogramowaniu. W sprawozdaniu za rok 2015 firma szczyci się 32-procentowym wzrostem uzyskanym zarówno ze sprzedaży platformy otwartej, jak i dzięki prężnie działającej sieci partnerskiej.

Ze względu na zaciekłą konkurencję wiele spółek wykorzystuje możliwości spoza tradycyjnego obszaru zastosowań systemów security, aby podtrzymać wzrost obrotów. Przykładowo, tajwański Hi Sharp (który nie znalazł się wprawdzie na liście TOP 15) wkracza w nisze, takie jak systemy zabezpieczenia pojazdów, które umożliwiają prowadzenie pełnego dozoru nad flotą poprzez kamery pokładowe i rejestratory mobilne DVR. – *W przeszłości przychody z działalności w obszarze security dominowały nad sprzedażą zabezpieczeń pojazdów. Teraz proporcje się odwróciły* – ocenił Jerry Chiang, prezes Hi Sharp. – *Przed wejściem na rynek zabezpieczeń pojazdów trzeba wyrobić sobie renomę jako producent systemów zabezpieczeń technicznych. Dla innych producentów security z Tajwanu, którzy także mają doświadczenie w tym zakresie, Hi Sharp jest bezkonkurencyjny.*
Dwaj chińscy giganci na rynku telewizji dozorowej, Hikvision Digital Technology i Dahua Technology, zajmują podobne pozycje pod względem zarówno łącznych przychodów, jak i dynamiki ich wzrostu.
Hikvision – obecnie numer 1 na głównej liście TOP 50 – zajmuje 4. lokatę pod względem wzrostu. Z kolei Dahua plasuje się na 4. pozycji pod względem przychodów i na 5. miejscu, biorąc pod uwagę zwiększenie wartości sprzedaży.
Konkurencja na rynku zabezpieczeń technicznych jest dziś większa niż kiedykolwiek, co utrudnia firmom osiągnięcie trwałego wzrostu przychodów. Producenci mogą więc zdobywać przewagę konkurencyjną, oferując rozwiązania kompleksowe, odpowiadające potrzebom klientów. Dowodzi tego analiza działania najszybciej rozwijających się spółek ujętych w rankingu TOP 50.

Axis koncentruje się na rozwiązaniach zintegrowanych

Firma Axis rozszerza swoje portfolio o systemy kontroli dostępu oparte na rozwiązaniach sieciowych oraz urządzenia audio, w dalszym ciągu traktując telewizję dozorową jako działalność podstawową.

50 NAJWIĘKSZE WZROSTY 12 MIEJSCE

Axis Communications, pionier i lider w dziedzinie sieciowych systemów dozoru wizyjnego, ponownie zanotował dwucyfrowy wskaźnik wzrostu. Podstawową działalnością spółki nadal pozostaje telewizja dozorowa, lecz Axis rozszerza ofertę o kontrolę dostępu opartą na rozwiązaniach sieciowych, a także domofony oraz głośniki i megafony, udostępniając w ten sposób rozwiązania zintegrowane.

Zakładom produkcyjnym, w których wszystkie systemy zabezpieczeń działają w sieci, Axis oferuje np. kamery termowizyjne wykrywające podejrzaną aktywność osób na granicy chronionego obiektu.
W sytuacji detekcji system DSO emituje komunikat nakazujący intruzowi oddalenie się. Pracownicy firmy, dostawcy lub podwykonawcy mogą wtedy skontaktować się z operatorem znajdującym się wewnątrz obiektu za pośrednictwem interkomu IP, a pracownicy posiadający identyfikatory – przejść przez bramę, korzystając z systemu kontroli dostępu. – *Mamy więc detektor ochrony obwodowej z możliwością rozszerzenia o DSO oraz kontrolę dostępu zamiast tylko jednej kamery* – wyjaśnił Edwin Roobol, dyrektor regionu Europy Środkowej w Axis Communications.
– *Zauważyliśmy większe zainteresowanie zintegrowanymi rozwiązaniami security i w tym obszarze umacniamy swoją pozycję. W roku 2016 dokonaliśmy trzech przejęć: 2N, Citilog i Gnimatics, aby rozwinąć i poszerzyć naszą ofertę rozwiązań kompleksowych. Dało to impuls do rozpoczęcia nowych przedsięwzięć biznesowych i prac badawczo-rozwojowych, mających na celu opracowanie rozwiązań atrakcyjnych dla naszych odbiorców końcowych* – dodał Ray Mauritsson, prezes i dyrektor generalny Axis Communications.

Ray Mauritsson
prezes i dyrektor generalny Axis Communications

„Zauważyliśmy większy popyt na zintegrowane rozwiązania security – umacniamy swoją pozycję w tym obszarze”.

Po przejęciu dwa lata temu firmy Axis przez koncern Canon coraz głośniej o możliwościach synergii ich działania. – *Mocną stroną Canona jest optyka i posiadane patenty oraz wydajność i zdolności produkcyjne. Są to obszary, w których liczymy na współpracę i potencjalne korzyści* – powiedział Edwin Roobol.
Axis wprowadził już do sprzedaży kamerę łączącą jego technologię z optyką Canon. Jednocześnie przejął w całości marketing i sprzedaż wszystkich sieciowych urządzeń telewizji dozorowej Canona na rynkach EMEA i Ameryki Północnej. – *Jedną z korzyści jest to, że nie musimy już konkurować. Współpracujemy ze sobą, co jest moim zdaniem znacznie bardziej rozsądne* – podsumował Edwin Roobol.

50 NAJWIĘKSZE WZROSTY 5 MIEJSCE

Dahua uważa video+ za przyszłość telewizji dozorowej

Liquan Fu
prezes Dahua Technology

Segment dozoru wizyjnego wyszedł poza obszar tradycyjnych zabezpieczenia, a branża migruje w kierunku, który Dahua określa jako video+.

Dahua Technology znacznie awansowała w rankingu TOP 50. Spółka, której łączne przychody sięgają 1,5 mld dol., plasuje się obecnie na 4. miejscu pod względem sprzedaży oraz na 5. pozycji, jeśli chodzi o wzrost przychodów. Znaczną część przychodów firmy stanowią wpływy uzyskiwane za granicą.
– *Uważamy, że działania firmy w zakresie ekspansji zagranicznej pomogły nam w utrzymaniu szybkiego tempa wzrostu w ostatnich dwóch latach. Dahua posiada ponad 20 oddziałów poza granicami Chin. Rozwijaliśmy te lokalizacje, aby zapewnić lokalnym rynkom wyższą jakość obsługi oraz szybszą reakcję na ich potrzeby* – powiedział Liquan Fu, prezes Dahua Technology.
Segment telewizji dozorowej notuje dynamiczny rozwój, toteż Dahua co roku przeznacza ok. 10% przychodów ze sprzedaży na badania i rozwój nowych technologii. Firma dokonała znaczących postępów w zakresie algorytmów rozpoznawania twarzy dzięki zastosowaniu technologii sztucznej inteligencji. Pobiła przy tym rekord w rozpoznawaniu twarzy w bazie LFW[1], pokonując takie firmy, jak Google.
Według Dahua Technology segment dozoru wizyjnego wyszedł poza obszar tradycyjnych zabezpieczeń, a branża zmierza w kierunku, który spółka określa jako video+, czyli dozór wizyjny wspomagany przez big data i sztuczną inteligencję. Określenie video+ można także scharakteryzować jako połączenie dwóch funkcji: „dozoru wizyjnego o wielowymiarowym aspekcie” oraz „dozoru wizyjnego o wielowymiarowych zastosowaniach”.
Pierwsza uwzględnia informacje przestrzenne o obiekcie i otoczeniu oraz rozpoznawanie głosu i identyfikację na podstawie cech biometrycznych, druga ma na celu wspieranie pełnej gamy zastosowań biznesowych, takich jak inteligentne miasta, inteligentny transport, przemysłowy system wizyjny[2] oraz automatyczne systemy alarmowania i podejmowania decyzji.
Według Dahua obecna tendencja konsolidacji branży ulegnie niebawem spowolnieniu, pojawi się natomiast wielu nowych graczy. Według firmy rynek security poszerza się ze względu na wdrażanie nowych technologii, które umożliwią działanie video+.
To właśnie ma przyciągnąć na rynek zabezpieczeń technicznych nowych graczy pochodzących głównie z branży oprogramowania i posiadających doświadczenie w zakresie sztucznej inteligencji.

1) *Labeled Faces in the Wild (LFW)* – baza fotografii twarzy służąca do badań nad technologiami ich rozpoznawania.
2) Przemysłowy system wizyjny służy najczęściej do sprawdzania cech fizycznych obiektów takich jak wymiary, kształt, kolor, stan powierzchni (połysk, chropowatość, nadruk itp.). Dane pozyskane przy jego użyciu stanowią podstawę do podjęcia odpowiedniej decyzji, np. o kolejnym etapie procesu wytwórczego.

Sukces TKH ma źródło w ofercie dla specyficznych użytkowników

50 NAJWIĘKSZE WZROSTY 3 MIEJSCE

Grupa TKH prowadzi działalność w zakresie ochrony w trzech głównych obszarach: maszyn dla przemysłu oponiarskiego, kabli i rozwiązań dla budownictwa. Blisko 60-procentowy wzrost przychodów uplasował firmę na 3. miejscu pod względem dynamiki sprzedaży.
– *W obszarze tych trzech filarów jesteśmy drugą największą firmą i osiągnęliśmy największy wzrost* – powiedział Magnus Ekerot, dyrektor generalny Security Vision Group, wchodzącej w skład TKH.

Grupa TKH jest właścicielem 16 spółek. Dostarcza rozwiązania z dziedziny security przeznaczone dla odbiorców siedmiu głównych segmentów: parkingowego, morskiego, naftowo-gazowego, infrastruktury, ochrony zdrowia, monitoringu miejskiego oraz administracji rządowej.

Security Vision Group, dzięki wsparciu pozostałych podmiotów z grupy TKH, oferuje rozwiązania kompleksowe. Jedną z przykładowych realizacji przytaczanych przez Magnusa Ekerota jest Międzynarodowy Trybunał Sprawiedliwości w Hadze, gdzie spółka dostarczyła okablowanie, kamery telewizji dozorowej, system interkomowy oraz system sygnalizacji włamania i napadu.
– *Klient kupuje rozwiązanie kompleksowe od jednej spółki, a ona obsługuje go poprzez certyfikowanych instalatorów i partnerów przeszkolonych w montażu. Może również oferować mu akcesoria, przewody i oprzyrządowanie. Klient nie potrzebuje żadnych pośredników* – podkreślił Magnus Ekerot.
Według firmy kluczem do sukcesu jest jej zdolność do wspierania strategii bezpieczeństwa użytkownika końcowego poprzez oferowanie mu nie tylko specjalistycznych, ale także konwencjonalnych zabezpieczeń technicznych.
– *Daje to TKH wyjątkową pozycję. Przykładowo spółka z branży naftowej, w której aktywnie działamy, potrzebuje kamer do dozoru bram i ogrodzenia. Ale na jej terenie są również wykonywane określone procesy, które należy monitorować na wypadek wystąpienia pożaru, przecieków czy ognisk wysokiej temperatury. My oderujemy specjalistyczne rozwiązania, niezwykle inteligentne urządzenia, odpowiadające na potrzeby najbardziej wymagającego użytkownika* – podsumował Magnus Ekerot. ■

Hikvision stawia na ekspansję na rynki zagraniczne

Firma Hikvision rozpoczęła działalność wychodzącą poza tradycyjnie pojmowany segment telewizji dozorowej i wkraczając przy tym na obszary, w których niezbędne jest łączenie dozoru wizyjnego, sztucznej inteligencji i big data.

Keen Yao
wiceprezes
Hikvision Digital Technology

Firma zajęła 1. miejsce w rankingu TOP 50, przecinając wszelkie spekulacje dotyczące tego, czy chiński gigant w dziedzinie dozoru wizyjnego zdoła się wspiąć na szczyt. Spółka wyszła na prowadzenie, osiągając 3,5 mld dol. przychodu w 2015 r. Ten rekordowy poziom sprzedaży zapewnił 43,6-procentowy wzrost w porównaniu do roku 2014, stawiając Hikvision na 4. miejscu w kategorii dynamiki wzrostu sprzedaży. Dochody z zagranicy stanowią obecnie większą część łącznych przychodów spółki.

Keen Yao, wiceprezes International Business Center w Hikvision, podkreśla wzmożoną ekspansję na rynki zagraniczne. – *Posiadamy 28 oddziałów na całym świecie i zatrudniamy za granicą ponad 700 pracowników, gwarantując lokalne wsparcie klientów. To jeden z powodów, dla których w ostatnich latach możliwe było osiągnięcie tak szybkiego tempa wzrostu naszej działalności poza granicami kraju* – powiedział.

W branży, w której obserwuje się coraz większą rywalizację i bezpardonową wojnę cenową wypowiedzianą przez chińskie firmy, także Hikvision rozpoczął działalność poza tradycyjnie pojmowanym segmentem telewizji dozorowej, wchodząc w obszary, w których niezbędne jest łączenie dozoru wizyjnego, sztucznej inteligencji i big data. Przykładowo w zastosowaniach ITS (inteligentne systemy transportowe) rozwiązanie Hikvision umożliwia detekcję twarzy kierowcy i ustalenie, czy jest on właścicielem pojazdu. W zastosowaniach domowych z kolei technologia Hikvision jest w stanie nauczyć się, kto jest członkiem rodziny, a kto obcym.

Ponieważ przeprowadzanie niezwykle skomplikowanej analizy wymaga dużych mocy obliczeniowych, spółka niedawno zawarła porozumienie z firmą Modivius (start-up wspierany przez Google), której jednostka przetwarzania obrazu Myriad 2 zastosowana w urządzeniach Hikvision odpowiada za funkcje „głębokiego uczenia się". Produkty zaprezentowano w ub. roku na targach Security China w Pekinie.

Segment telewizji dozorowej nadal będzie podstawą działalności Hikvision, jednak spółka uważa big data za nieunikniony trend, dlatego kieruje swoją uwagę na rozwiązania i produkty w większym stopniu oparte na Internecie Rzeczy (IoT). Zgodnie z tą koncepcją Hikvision przejął w ub.r. firmę Pyronix, brytyjskiego dostawcę systemów sygnalizacji włamania i napadu. Planowana jest silniejsza integracja systemów dozoru wizyjnego z SSWiN, dzięki czemu jedno zdarzenie będzie aktywować kolejne w ramach szerokiego środowiska IoT.

Do innych zaawansowanych rozwiązań wdrożonych przez Hikvision, na razie głównie w Chinach, należy wykorzystanie dronów i robotów do prowadzenia dozoru w kluczowych obszarach niedostępnych dla ludzi.

„Posiadamy 28 oddziałów na całym świecie i zatrudniamy za granicą ponad 700 pracowników, gwarantując klientom lokalne wsparcie. To jeden z powodów, dla których w ostatnich latach było możliwe osiągnięcie tak szybkiego tempa wzrostu naszej działalności międzynarodowej".

IDIS przywiązuje szczególną wagę do bezpieczeństwa sieciowego

IDIS koncentruje się na rozwiązaniach kompleksowych, które zaspokoją różne potrzeby użytkowników przy niższym koszcie całkowitym.

James Min
dyrektor generalny ds. sprzedaży (region EMEA), IDIS

W roku 2015 spośród producentów koreańskich najwyższy, blisko 25-procentowy wzrost przychodów odnotowała firma IDIS. W rankingu TOP 50 spółka zajmuje 17. miejsce pod względem przychodów, 10. pozycję, zważywszy na ich dynamikę. Jak twierdzi James Min, dyrektor generalny ds. sprzedaży w regionie EMEA, znaczny wzrost nastąpił we wszystkich regionach, szczególnie w obu Amerykach oraz krajach Europy, Bliskiego Wschodu i Afryki.

Zdaniem Jamesa Mina największym problemem dla branży jest obecnie zalew tanich i niskiej jakości kamer IP, prowadzący do wojny cenowej, która skutkuje pogorszeniem jakości produktów i niezadowoleniem klientów. IDIS nie podąża tą ścieżką. Spółka skupiła się na rozwiązaniach kompleksowych, które zaspokajają różne potrzeby użytkowników przy niższym koszcie całkowitym. Przykładowo, dzięki oferowanym przez firmę szerokokątnym obiektywom 4K typu rybie oko użytkownik potrzebuje tylko jednej kamery zamiast kilku, aby objąć dozorem większy obszar. Standard kompresji H.265 oraz własny koder IDIS *Intelligent Codec* wymagają z kolei mniejszego zapotrzebowania na przepustowość pasma oraz przestrzeni dyskowej na przechowywanie nagrań wysokiej jakości, co przyczynia się do dalszych oszczędności.

– *Nasza strategia na rok 2016 zakłada, że staniemy się wiarygodnym dostawcą rozwiązań kompleksowych, skoncentrowanych na półki średnią i wysoką. Nie sprzedajemy urządzeń, lecz sprawdzone rozwiązania obejmujące szeroki asortyment kamer, rejestratorów NVR i akcesoriów sieciowych* – powiedział James Min. – *Oferowanie doskonałego rozwiązania nie polega na obniżaniu cen, lecz na dostarczaniu klientom produktów wysokiej jakości w rozsądnej cenie, przy jednoczesnym zapewnieniu niskich kosztów całkowitych podczas eksploatacji.*

W przyszłości spółka zamierza opracowywać więcej rozwiązań z wartością dodaną oraz skupić się na cyberbezpieczeństwie.

– *DirectIP np. funkcjonuje we własnej dedykowanej sieci, aby takich urządzeń jak kamery nie wykorzystano do włamania do sieci korporacyjnej. Korzystamy z własnej, opatentowanej struktury plików, co dodatkowo utrudnia włamanie, podczas gdy niektórzy inni producenci opierają się na systemie Windows lub ogólnodostępnym Linuksie* – wyjaśnił James Min. – *W naszych rejestratorach NVR zainstalowano zastrzeżoną, wbudowaną wersję Linuksa, która nie jest ogólnie dostępna, a w komunikacji w sieci opieramy się na branżowym standardzie SSL/TLS oraz – w zależności od zapotrzebowania – na szyfrowaniu danych logowania, filtrowaniu IP, IEEE 801.1x i TLS/SMTP.*

OPTEX widzi potrzebę integracji

OPTEX zapowiada rewolucję, która zbliży nas do technologii dualnej.

W ubiegłym roku OPTEX odnotował ponad 9-procentowy wzrost sprzedaży, zajmując 16. pozycję w rankingu TOP 50 pod względem wzrostu przychodów. Jest to więc najszybciej rosnąca spółka wśród wszystkich dostawców japońskich.
OPTEX został liderem w zakresie systemów sygnalizacji włamania i napadu przeznaczonych do różnorodnych zastosowań, w tym na rynki security i automatyki przemysłowej, w medycynie, ochronie środowiska i innych.
W zastosowaniach security czujki OPTEX są wykorzystywane w segmentach mieszkaniowym i komercyjnym oraz infrastrukturze krytycznej. Ten ostatni rynek należy do głównych źródeł przychodów firmy. Firma obserwuje zwiększone zainteresowanie czujkami ochrony zewnętrznej również na komercyjnym i mieszkaniowym rynku oświetleniowym.

– Biorąc pod uwagę rozwój wydarzeń w Europie, zwiększoną aktywność terrorystyczną i ogólnoświatowe zagrożenie zwiększeniem liczby włamań do domów, coraz powszechniejsza staje się świadomość potrzeby posiadania systemów alarmowych. Dostrzegamy m.in. wzrost zapotrzebowania na systemy ochrony perymetrycznej obiektów mieszkalnych wśród użytkowników końcowych – podkreślił Jacques Vaarre, zastępca dyrektora zarządzającego w firmie OPTEX Europe. Czujki OPTEX są popularne, niezawodne i cieszą się renomą na całym świecie.
– W otoczeniu zewnętrznym na pracę kamer oddziałuje światło, cienie, owady czy poruszająca się roślinność. Z tego powodu tradycyjne czujki ruchu czy detektory laserowe poinformują nas jedynie, że coś je uaktywniło, ale nie są w stanie zinterpretować, co konkretnie było przyczyną. Dzięki kamerze można to zobaczyć. Dlatego trend, a raczej nadchodząca rewolucja, którą dostrzega firma OPTEX, zbliża nas do technologii dualnej, czyli niezawodnego połączenia dwóch technologii detekcji, które mogą się wzajemnie wspierać – powiedział Jacques Vaarre.
Przykładem przytaczanym przez Vaarre'a jest wieża widokowa, u której podstawy zamontowano laserowe czujki OPTEX wykrywające wspinanie się. Są one zintegrowane z główną platformą VMS stosowaną już wcześniej. Podniosło to poziom niezawodności rozwiązania, a w efekcie także satysfakcję klienta.
W zakresie kontroli dostępu czujki OPTEX mogą być integrowane np. z drzwiami obrotowymi w obiektach infrastruktury krytycznej, zapobiegając podwójnym wejściom (tzw. metodą „na barana").
Oprócz rozwiązań do ochrony perymetrycznej i kontroli dostępu OPTEX obsługuje znaczną część azjatyckiego rynku analizy w segmencie sprzedaży detalicznej, dostarczając narzędzia do zliczania osób i zarządzania kolejkami dla małych sklepów, dużych sieci i wielkich przedsiębiorstw.
– Odbywa się to za pośrednictwem naszej spółki zależnej Giken Trastem, do której należy 60% japońskiego rynku analityki wizyjnej (VCA) dla handlu – zaznaczył Vaarre. *– Według firmy rynek analityki w handlu detalicznym w Europie i Ameryce Północnej będzie się rozwijał, co daje szansę na dodatkowe realizacje dla branży security.*

W zastosowaniach security czujki OPTEX są wykorzystywane w segmentach mieszkaniowym i komercyjnym oraz infrastrukturze krytycznej.

Jacques Vaarre
zastępca dyrektora zarządzającego, OPTEX Europe

50 NAJWIĘKSZE WZROSTY 17 MIEJSCE

Owen Chen
prezes VIVOTEK

50 NAJWIĘKSZE WZROSTY 14 MIEJSCE

VIVOTEK skupia się na współpracy z partnerami

Firmy z branży security przykładają większą wagę do rozwiązań specjalistycznych, opracowanych we współpracy z odpowiednimi partnerami.

Tajwański VIVOTEK ma za sobą udany rok 2015, w którym przychody sięgnęły 120,4 mln dol., co oznacza wzrost o 14,9% w stosunku do roku poprzedniego. Dobra passa trwała także w 2016 r. Co ważne, spółce udało się utrzymać wzrost we wszystkich kolejnych miesiącach.

Firma czerpie z know-how firm działających w tym samym ekosystemie, ale w innych obszarach i zastosowaniach.

Według Owena Chena, prezesa VIVOTEK, wskaźniki wzrostu są dowodem na skuteczność aktualnej strategii firmy, stanowiącej odpowiedź na masową sprzedaż i konkurencję cenową w branży security. Spółka dokonała przekształceń w swoim zespole B+R, aby podnieść jego skuteczność i produktywność. Wprowadzono m.in. technologię Smart Stream II uzupełniającą standard kompresji H.265, co pozwoliło obniżyć wymaganą przepustowość łącza i zapotrzebowanie na przestrzeń do przechowywania danych nawet o 80%.
Najistotniejsze jednak według Owena Chena jest to, że firmy z rynku zabezpieczeń obecnie przykładają większą wagę do oferowania rozwiązań, nie zaś do pojedynczych produktów.
– To dzięki technologii Internetu Rzeczy (IoT). Zapotrzebowanie na różne urządzenia mobilne, łączące się z siecią domy i samochody, a także drony i roboty wywierają również wpływ na rozwój tradycyjnych produktów i technologii z dziedziny zabezpieczeń. Dlatego nieszablonowe myślenie o rozwiązaniach do zastosowań spoza rynku security ma niebagatelne znaczenie – podkreślił Owen Chen.
W tym kontekście VIVOTEK rozpoczął poszukiwanie odpowiednich partnerów. Prezes firmy podkreśla, że czerpanie z know-how firm działających w tym samym ekosystemie, ale w innych obszarach i zastosowaniach umożliwiło szybkie opracowanie nowych rozwiązań.
Partnerami w ekosystemie firmy są głównie zewnętrzni producenci oprogramowania i sprzętu. Niedawno VIVOTEK poinformował o nawiązaniu współpracy technologicznej z austriackim NETAVIS Software, specjalizującym się w systemach telewizji dozorowej IP opartych na rozwiązaniach serwerowych oraz zintegrowanej analizie obrazu wideo. Pozwoli to na opracowanie produktu do dokładnego trójwymiarowego zliczania osób, połączonego z platformą NETAVIS w zakresie analityki biznesowej.
Wcześniej VIVOTEK podpisał strategiczne porozumienia z kilkoma spółkami.
Firma Genetec pomoże dostarczać nowe, oparte na chmurze rozwiązanie dozoru wizyjnego jako usługi (VSaaS) – Stratocast. Z kolei partnerstwo z Videonetics i Neural Labs przyczyni się do rozwoju produktów z zakresu identyfikacji numerów tablic rejestracyjnych.
– W sieciowym świecie przyszłości jedna firma nie będzie w stanie samodzielnie dostarczać wszystkich technologii i rozwiązań – zauważył Owen Chen.
– Dlatego powinniśmy współpracować w ramach swoistego ekosystemu, by zapewnić spółce stabilną pozycję.

Zmiana kursu receptą na przetrwanie

Na rynku zabezpieczeń technicznych zachodzi obecnie sporo zmian, które powodują, że wiele firm musiało zastanowić się nad swoją strategią działania i ponownie ją przeanalizować. **Niektórzy mają tę analizę za sobą i podjęli już decyzję o zmianach kursu.**

Branża zabezpieczeń technicznych znalazła się w trudnym okresie. Spowolnienie gospodarcze na świecie oraz wzrost znaczenia producentów chińskich wywołały zamieszanie na rynkach, skłaniając wiele firm do podjęcia zdecydowanych kroków zmierzających do zmian organizacyjnych.

Ze sprawozdania przygotowanego w 2016 r. przez brytyjską firmę badawczą IHS wynika, że całkowita wartość sprzedaży produktów dozoru wizyjnego zmniejszyła się nie ze względu na niższy wolumen sprzedaży, lecz z powodu spadku cen podyktowanego przede wszystkim poszerzeniem się konkurencji (głównie cenowej) ze strony producentów z Chin. Firmy z branży security rozważają różne warianty sprostania stojącym przed nimi wyzwaniom. Niektóre zdecydowały się na wzmocnienie poprzez fuzje i przejęcia, inne rozbudowały swoje portfolio o produkty wykraczające poza ich tradycyjne obszary działalności. Część natomiast nie udźwignęła ciężaru rywalizacji – zrezygnowała z konkurowania na rynku niskich kosztów produkcji i przekazała tę produkcję w outsourcing.

Dave Petratis
prezes, Allegion

RANKING TOP 50 SECURITY 11 MIEJSCE

Allegion chce zwiększyć udział w rynku

Mimo kilku istotnych przejęć przychody firmy pozostały jednak na niskim poziomie.

W 2016 r. amerykańska firma Allegion, dostawca rozwiązań z zakresu kontroli dostępu, przeprowadziła kilka ważnych przejęć. Pomogły one wzmocnić jej pozycję na rynku. Jednak mimo to przychody spółki ze sprzedaży urządzeń i systemów kontroli dostępu spadły o prawie 2,5% względem poprzedniego roku.

Pod względem obrotów Allegion to obecnie druga na świecie firma kontroli dostępu. Należą do niej marki: Schlage, LCN, Von Duprin, SimonsVoss i Interflex.

– *Ze względu na mechaniczną naturę urządzeń kontroli dostępu rynki tej branży mają charakter lokalny w przeciwieństwie do rynku dozoru wizyjnego, bardziej powszechnego i jednolitego* – powiedział Dave Petratis, prezes firmy Allegion.

– *W Europie dynamika rynku KD kształtuje się różnie w poszczególnych krajach, np. zamek stosowany w Portugalii jest inny niż ten, którego używa się w Niemczech. Rynek północnoamerykański wydaje się bardziej jednolity, ale z kolei tam wymagania zawarte w kodeksach dobrych praktyk i normach są różne dla firm z Nowego Jorku i Los Angeles. To jedne z czynników przyczyniających się do złożoności branży security. Z tego względu niewiele firm będzie w stanie poradzić sobie z komunikacją w ramach globalnych protokołów dostępu.*

W regionie Azji i Pacyfiku firma przejęła trzy spółki: Milre, będącą drugą co do wielkości firmą w branży zabezpieczeń elektronicznych w Korei Południowej, oraz australijskie FSH i Brio. Sam Allegion działa w branży kontroli dostępu już od kilkudziesięciu lat. Globalne marki należące do firmy obejmują teraz: Schlage, LCN, Von Duprin, SimonsVoss i Interflex. Pod względem obrotów to obecnie druga na świecie firma kontroli dostępu.

- *Mówiąc o technologii, myślimy o software i firmware, kwestiach miniaturyzacji, żywotności baterii i dostosowaniu rozwiązań do konkretnych zastosowań* – tłumaczy prezes firmy. – *Pracujemy w różnych regionach i na różnych rynkach. Dla Allegion ważne jest portfolio marek, ponieważ dzięki ich technologiom firma może oferować rozwiązania odbiorcom z różnych specyficznych segmentów rynku.*

Ponad rok temu firma kupiła SimonsVoss. Dzięki temu przejęciu Allegion oferuje teraz urządzenia kontroli dostępu, które są mniejsze, bardziej inteligentne i mogą odegrać stymulującą rolę w rozwoju technologii urządzeń działających w sieci, tzw. *connected world.*

– *Jednym z najważniejszych obszarów zainteresowania firmy Allegion jest konwergencja rozwiązań mechanicznych i elektronicznych* – podkreślił Dave Petratis. – *SimonsVoss to silna marka, która łączy nowoczesne technologie, dużą żywotność baterii oraz miniaturyzację produktów, czyli innowacje, które przynoszą ogromne korzyści klientom i są związane z tą konwergencją.*

Aby zrealizować wyraźnie sprecyzowane plany uzyskania większego udziału w rynku, firma planuje rozszerzenie działalności w Europie i na innych kontynentach. Jest przekonana, że rynek europejski będzie oferował coraz większe możliwości rozwoju w miarę integrowania elektroniki z systemami mechanicznymi. Kierownictwo firmy podkreśla, że Allegion wyróżnia się spośród konkurencji otwartymi protokołami i bogatym portfolio realizacji.

– *Stosujemy otwarte protokoły, by urządzenia mogły zapewniać wymianę informacji z systemami zarządzania budynkiem BMS oraz systemami kontroli dostępu. Chcemy oferować klientom system współpracujący z innymi działającymi już w obiektach* – wyjaśnił Dave Petratis.

– *Naszym ostatnim sukcesem jest współpraca z Apple. W salonach tej marki można kupić nasze zamki. Dzięki technologii IoT staliśmy się częścią platformy Apple HomeKit. Rozwój, rentowność i innowacyjność to główne czynniki wzrostu, do których dąży nasza firma i nasi pracownicy.*

Przejęcia wzmacniają pozycję FLIR jako dostawcy kompleksowych rozwiązań. Firma nadal będzie też oferować systemy o architekturze otwartej

FLIR, znany producent kamer termowizyjnych, poszerza ofertę o kamery pracujące w zakresie światła widzialnego.

Firmą, która w ostatnich latach dokonała poważnych zmian w portfolio produktów, jest bez wątpienia FLIR Systems, producent kamer termowizyjnych. Stało się to głównie za sprawą kilku przejęć przeprowadzonych w ostatnim czasie, np. w 2016 r. firma kupiła spółkę DVTEL.

W roku 2015 przychody FLIR ze sprzedaży produktów telewizji dozorowej spadły o 3,3%, głównie ze względu na zmniejszające się wciąż zapotrzebowanie ze strony klientów amerykańskich z sektora administracji rządowej oraz spadek przychodów ze sprzedaży linii produktowych, takich jak specjalistyczne kamery *airborne* (montowane w samolotach i śmigłowcach) oraz systemy zintegrowane. Pion urządzeń security nadrobił jednak z naddatkiem te straty dzięki 26,5-procentowemu wzrostowi przychodów.

– *Dzięki naszej nowej ofercie cenowej i portfolio produktów zwróciliśmy się ku segmentowi niższych cen i niższej specjalizacji* – powiedział David Montague, dyrektor ds. sprzedaży urządzeń security na region EMEA w firmie FLIR Systems.

– *Część segmentu sprzętu termowizyjnego przekształcamy na produkty z segmentu towarów powszechnego dostępu. Klienci kupują takie urządzenia od dystrybutora. Nie mówimy tu więc o realizacji specjalistycznych projektów, lecz o prostej sprzedaży towarów.*

Strategia biznesowa, polegająca na kupnie kilku spółek branży security, ma na celu zbliżenie firmy do dostawców rozwiązań kompleksowych. Chociaż ten plan jest wprowadzany w życie, John Distelzweig wskazał, że spółka nadal oferuje produkty w pełni kompatybilne z architekturą otwartą.

– *Nasze kamery są zgodne ze standardem ONVIF i mają certyfikaty zgodności z innymi systemami telewizji dozorowej. Nigdy z tego nie zrezygnujemy. W tej branży bardzo duże znaczenie ma to, by utrzymać otwartość architektury i wszechstronną kompatybilność* – dodał John Distelzweig. – *Dlatego do naszych systemów dozoru wizyjnego włączamy kamery różnych producentów, z kolei nasze kamery są kompatybilne z różnymi systemami VMS. Nie chcielibyśmy znaleźć się w kategorii mniej lub bardziej zamkniętych systemów. Nasza strategia jest inna. Wierzymy, że przyszłość branży i nasza siła leżą w możliwości współpracy z produktami różnych marek, dzięki czemu możemy oferować dodatkowe funkcje.*

Należy jednak podkreślić, że zdecydowanie trudniej zbudować system z elementów pochodzących od wielu producentów.

– *Nasze produkty obejmują przede wszystkim rozwiązania kompleksowe i przekrojowe, a nie rozwiązania dla konkretnych segmentów* – dodał David Montague. – *Mimo to, dzięki przejęciu firmy DVTEL, nasze systemy dozorowe mogą także zapewniać specyficzne potrzeby konkretnych odbiorców, np. w sektorze handlu użytkownicy mogą chcieć poznać liczbę osób wchodzących do sklepu. Oferujemy więc konkretne aplikacje, które mają zastosowanie w różnych segmentach rynku.* ■

John Distelzweig
wiceprezes i dyrektor zarządzający działu produktów security, FLIR Systems

Poprzez przejęcie kilku spółek branży security FLIR Systems ma się stać dostawcą rozwiązań kompleksowych.

Geutebrueck koncentruje się na wybranych grupach klientów

Skoncentrowanie się na wybranych grupach klientów i rozwiązywanie ich problemów pomogło firmie stawić czoła wyzwaniom na rynku.

Niemiecka firma GEUTEBRUECK stwierdziła, że trudniej utrzymać konkurencyjność w branży security, skupiając się jedynie na produktach. W stawieniu czoła temu wyzwaniu pomaga strategia polegająca na koncentrowaniu się na wybranych segmentach klientów i dostarczaniu rozwiązań dostosowanych do ich potrzeb.

– *Skupiamy się na konkretnych grupach użytkowników i rozmawiamy z nimi bezpośrednio o ich problemach, a także o rozwiązaniach, które możemy im zaoferować* – powiedziała Katharina Geutebrück, dyrektor zarządzająca firmy. – *Gdy rozmawiamy o ich oczekiwaniach, o tym, jak je spełnić i jakie korzyści można przy tym osiągnąć, nie musimy ograniczać się tylko do oferowania produktów. Rozmawiamy o zwrocie z inwestycji uzyskiwanym dzięki stosowaniu danego rozwiązania.*

Katharina Geutebrück
dyrektor zarządzająca, GEUTEBRUECK

Oprócz systemów security GEUTEBRUECK oferuje rozwiązania i usługi doradcze w zakresie optymalizacji oraz zabezpieczania operacyjnych procesów biznesowych, głównie na potrzeby logistyki i produkcji.

Przykładem specyficznego rynku docelowego dla firmy jest logistyka. Nie jest to jednak segment zupełnie nowy dla GEUTEBRUECK, chociaż wcześniej był określany jako bezpieczeństwo łańcucha dostaw.

– *Patrzymy na cały łańcuch: od zamówienia po dostawę* – podkreśliła Katharina Geutebrück. – *Na każdy proces, w ramach którego towary są przenoszone z punktu A do punktu B.*

Oprócz systemów typowych dla branży security firma GEUTEBRUECK oferuje rozwiązania i usługi doradcze w zakresie optymalizacji i zabezpieczania operacyjnych procesów biznesowych, zwłaszcza na potrzeby logistyki i produkcji.

– *Oferujemy systemy dozoru wizyjnego zapewniające ochronę przed zagrożeniami z zewnątrz, a także pomagamy zoptymalizować procesy logistyczne i zwiększyć ich efektywność. Nazywamy to „obrazowaniem wartości”* – powiedziała dyrektor zarządzająca. – *Nie są to zastosowania związane bezpośrednio z bezpieczeństwem. Chodzi raczej o odkrywanie korzyści płynących z tych procesów, w tym przypadku ewentualnych kosztownych błędów pracowników lub uszkodzenia towarów przez osoby trzecie.*

Spółka stawia również na bezpośredni kontakt z odpowiedzialnymi za procesy produkcyjne i logistyczne decydentami we współpracujących z nią firmach i organizacjach. Rozwiązania dla nich obejmują jednak nie tylko dozór wizyjny.

– *Sam obraz z kamer nic nie znaczy* – podkreśliła Katharina Geutebrück. – *Konieczne są informacje dodatkowe, które powiedzą nam, co musimy zobaczyć, aby obraz był użyteczny. A użyteczny obraz wizyjny to taki, który dostarcza odpowiednich informacji dokładnie wtedy, kiedy tego potrzebujemy, i przyczynia się do usunięcia błędów, zanim przełożą się na zbędne koszty. Umożliwia też wykrycie sprawców ewentualnych szkód oraz pomaga zaoszczędzić czas i pieniądze. Informacje dodatkowe mogą pochodzić z analizowanego obrazu wizyjnego lub być uzyskiwanie dzięki współpracy systemu zarządzania telewizją dozorową z systemem innego dostawcy, np. zarządzającym magazynami.*

Wraz z postępem technicznym coraz większe znaczenie dla branży security mają także takie koncepcje, jak Internet Rzeczy (IoT). To coraz bardziej istotne w tworzeniu rozwiązań dostosowanych do wymagań niektórych segmentów. ■

Mobotix wykorzysta mocne strony nowego właściciela

Właścicielem firmy MOBOTIX od 2016 r. jest japońska Konica Minolta.

Wydarzeniem roku dla firmy MOBOTIX było jej przejęcie przez japońską grupę Konica Minolta, specjalizującą się w rozwiązaniach do drukowania i zarządzania biurem. MOBOTIX stara się to wykorzystać, aby wzmocnić swoją pozycję na rynku security. W rozmowie z „a&s International" Uwe Barthelmes, dyrektor ds. marketingu w MOBOTIX, powiedział, że ma ona interesujący plan wykorzystania technologii obu firm. Jako przykład podał oferowaną przez japońską firmę technologię LiDAR 3D, którą można połączyć z technologią wizyjną i termowizyjną firmy MOBOTIX w jeden system.

– Połączenie technologii LiDAR 3D, technologii wizyjnej i termowizyjnej oraz opartych na nich rozwiązań umożliwi powstanie nowej generacji produktów z zakresu ochrony obwodowej – powiedział Uwe Barthelmes. *– Oznacza to możliwość generowania informacji „trójwymiarowych", np. o odległości i rozmiarach obiektów. Dzięki temu możemy sobie wyobrazić bardziej niezawodne systemy alarmowe, które np. ograniczają liczbę fałszywych alarmów powodowanych przez małe zwierzęta czy inne nieistotne czynniki.*

Takie zastosowanie pozwoli wprowadzić nową generację czujek, łączącą technologię czujników optycznych i termicznych z technologią LiDAR 3D. Dzięki temu połączeniu firmy będą mogły wykorzystać synergię różnych technologii. To istotne także z biznesowego punktu widzenia: każda z firm ma własne portfolio klientów, więc w pewnym zakresie będą się nimi dzieliły.

– Konica Minolta ma bardzo mocną pozycję na rynku druku i zarządzania biurem. W wielu krajach prowadzi świetnie prosperujące oddziały. Obecnie pracujemy nad możliwością połączenia zasobów i wymiany doświadczeń, które mogą przynieść korzyści obu firmom – dodał dyrektor ds. marketingu w firmie MOBOTIX.

Baza klientów jest dość zróżnicowana. Są to przede wszystkim użytkownicy końcowi, tacy jak małe biura, prywatne gabinety lekarskie, biura księgowe czy gospodarstwa domowe.

Nowością w firmie są też rozwiązania plug & play, które może teraz oferować klientom do samodzielnego montażu. Jeden z nich – wideodomofon IP T25 – jest przeznaczony dla odbiorców sektora mieszkalnego. Inne tego rodzaju rozwiązanie, zaprojektowane wspólnie z Tandberg Data, obejmuje kamery MOBOTIX i serwer NAS.

– Wcześniej użytkownicy końcowi nie odważyliby się samodzielnie przeprowadzać instalacji urządzeń security – zaznaczył Uwe Barthelmes. – Być może zaangażowaliby instalatora, żeby zamontował kamery, którymi po uruchomieniu można już zarządzać we własnym zakresie. A może ten położyłby jedynie kable, ale nie znałby się na urządzeniach IP. Dzięki nowym rozwiązaniom plug & play użytkownik może przeprowadzić instalację samodzielnie, a jednocześnie bardzo łatwo. Wszystkie elementy, w tym kamery czy serwer NAS, są już wstępnie skonfigurowane. Ryzyko niepowodzenia takiej instalacji jest dla klienta niewielkie. ■

Magal chce zdobyć nowe segmenty rynku

Firma, która ma silne kompetencje w dziedzinie projektów, poświęci teraz więcej uwagi produktom.

Izraelska firma ochrony obwodowej, dzięki przejęciu spółki Aimetis, poszerza swoją ofertę o systemy VMS.

Firma Magal Security Systems jest jednym z największych na świecie producentów rozwiązań do ochrony perymetrycznej (obwodowej). Ma dwa działy biznesowe: jeden zajmuje się projektami, drugi oferuje produkty. W roku 2016 sprzedaż pionu projektów spadła w stosunku do roku poprzedniego, podczas gdy przychody ze sprzedaży produktów wzrosły.

Hagai Katz, wiceprezes ds. marketingu i rozwoju biznesu, stwierdził, że rynek pionu projektów nie gwarantuje już stabilnego rozwoju. Niepewna sytuacja wynika z tego, że w jednym roku można zrealizować ciekawy i intratny projekt, dzięki któremu cały rok będzie należał do udanych, a w kolejnym nie przeprowadzić już żadnej realizacji. W związku z tym firma zamierza wzmocnić swój pion produktowy. Realizacją tej strategii jest ubiegłoroczne przejęcie spółki Aimetis. Kupując tego kanadyjskiego dostawcę systemów VMS, Magal Security Systems mógł włączyć do swojego portfolio nowy rodzaj produktów. Dzięki temu firma specjalizująca się dotychczas w rozwiązaniach z zakresu ochrony obwodowej zdobyła nowe kompetencje, które pozwolą jej wzmocnić swoją obecność na rynku i wejść w nowe segmenty. To przejęcie pomoże poszerzyć ofertę i rozpocząć działalność na innych niż do tej pory obszarach rynku.

– W ubiegłym roku poinformowaliśmy o przejęciu spółki Aimetis, które pozwoliło nam wprowadzić do oferty nowe rozwiązania z zakresu telewizji dozorowej – powiedział Hagai Katz. *– Wcześniej byliśmy aktywni głównie na rynku rozwiązań ochrony zewnętrznej, w takich obszarach jak granice, porty morskie, lotniska czy więzienia. Takie projekty stanowiły aż 90% naszych realizacji. Rozwiązania ochrony wewnętrznej czasem wchodziły w zakres tych projektów, ale nie był to nasz podstawowy produkt. Po włączeniu do portfolio systemów VMS proporcje się zmieniły. Większość zabezpieczeń jest jednak instalowana wewnątrz budynków, a jedynie część na zewnątrz.*

Dzięki tak poszerzonej ofercie rozpoczęliśmy działalność w segmentach rynkowych, w których dotychczas nie byliśmy obecni, takich jak edukacja czy hotelarstwo. Z kolei znane nam projekty „safe city" dotyczą głównie przestrzeni zewnętrznych, ale są zdominowane przez kamery dozorowe i systemy VMS. Nie jest to więc dla nas rynek nowy, lecz teraz znacznie większy. ■

IndigoVision rezygnuje z produkcji sprzętu na rzecz oprogramowania

Przychody firmy w 2015 r. spadły o 23% w porównaniu do poprzednich 12 miesięcy.

IndigoVision należy do firm, które w 2015 r. odnotowały drastyczny spadek przychodów. W tym właśnie okresie sprzedaż spadła o 23% w stosunku do poprzednich 12 miesięcy. Firma tłumaczy ten fakt agresywną konkurencją ze strony producentów chińskich i zaznacza, że rok 2016 był dla niej zdecydowanie lepszy. W pierwszej połowie 2016 r. odnotowała znaczną poprawę, a straty zostały odrobione.

Obecnie IndigoVision stawia na współpracę z producentami chińskimi, traktując to posunięcie jako część własnej ścieżki do osiągnięcia sukcesu. W rozmowie z „a&s International" Marcus Kneen, prezes IndigoVision, wyjaśnił założenia nowej strategii:

– Ostatnie trzy lata były okresem diametralnych zmian na rynku security. Chiny wysunęły się na czoło producentów sprzętu dzięki strategii nastawionej na oferowanie niskich cen. Po zdobyciu pozycji lidera skupiły się na rozwijaniu kompetencji technicznych. Spodziewamy się, że także w zakresie technologii niedługo uzyskają czołową pozycję.

Taka sytuacja jest obserwowana na ich rynkach krajowych na Dalekim Wschodzie, gdzie mają uprzywilejowaną pozycję, a także na bardziej konkurencyjnych rynkach zachodnich.

– Zmiany w branży stwarzają zagrożenia, ale i nowe możliwości rozwoju – podkreślił Marcus Kneen.

IndigoVision podjął decyzję o zakończeniu prac nad tworzeniem nowych urządzeń. Specjalistyczną wiedzę na temat kamer telewizji dozorowej wykorzysta teraz, doradzając producentom OEM, by ci zapewnili produktom najwyższą jakość, z jakiej słyną urządzenia IndigoVision. Firma przeanalizowała swoją dotychczasową ofertę i zdecydowała się przesunąć siły techniczne na tworzenie oprogramowania. Ma to być rozwiązanie kompleksowe, w którym użytkownicy będą mogli swobodnie dobrać kamery, zdecydować o sposobie przechowywania materiałów wizyjnych, rodzaju zarządzania całym systemem dozoru wizyjnego i jego integracji.

Prezes zdradził, że w 2016 r. firma sprzedała 20–30% więcej sprzętu i oprogramowania pod względem wolumenu sprzedaży niż w poprzednim roku. Przewiduje, że ten trend utrzyma się także w 2017 r., a przychody dzięki zmianie strategii firmy będą bezpieczne.

– W IV kwartale 2015 r. firma wprowadziła na rynek system VMS w różnych wersjach dostosowanych do różnych odbiorców końcowych – podkreślił Marcus Kneen. *– Myślę, że dostosowanie oprogramowania do specyficznych grup odbiorców pozwoli nam zdobyć większą część rynku. Nasze produkty obejmują teraz więcej poziomów cenowych: od rozwiązań na jedną do ośmiu kamer, po wdrożenia nawet na 40 tysięcy kamer. Dysponujemy więc ofertą dostosowaną do wymagań wszystkich segmentów klientów.* ■

Sieger Volkers
dyrektor zarządzający, Nedap

50 RANKING TOP 50 SECURITY 15 MIEJSCE

Nedap skupia się na cyberbezpieczeństwie

Większość firm oferuje rozwiązania end-to-end, Nedap jest wyjątkiem.

Główny rynek firmy Nedap, rynek klientów korporacyjnych, pozostaje stabilny pomimo spowolnienia gospodarki europejskiej. Sytuacja gospodarcza ma obecnie ograniczony wpływ na zachowania zakupowe klientów korporacyjnych w zakresie inwestycji w zabezpieczenia, ponieważ do inwestowania w te rozwiązania zmusza ich coraz większe ryzyko zamachów terrorystycznych i ataków cybernetycznych. Wzrost sprzedaży na tym rynku nie jest duży, ale firma nie odnotowała spadku.

– *To stabilny wzrost i stabilny rynek* – stwierdził Sieger Volkers, dyrektor zarządzający działu Security Management w firmie Nedap.

Coraz częściej odnotowuje się ataki hakerskie na duże firmy i instytucje. Nedap dostrzega to zjawisko i kładzie duży nacisk na kwestie związane z cyberbezpieczeństwem. Może tu wykorzystać własne doświadczenie z zakresu IT, bo w tej branży firma rozpoczynała działalność.

– *Nasze działania polegają na zapewnieniu bezpiecznej kontroli dostępu gwarantowanej przez stosowane przez nas technologie* – podkreślił Sieger Volkers. – *Obserwujemy znaczące zmiany na rynku i uważam, że jesteśmy jedyną firmą, która potrafi zapewnić bezpieczeństwo od krytycznych elementów systemu, przez oprogramowanie, bazy danych, środowisko serwerowe, aż po karty i czytniki kart. Ma temu służyć połączenie sił firm Nedap i AET Europe, mające na celu zapewnienie najwyższych poziomów bezpiecznego szyfrowania i uwierzytelniania. Dzięki temu dane przechowywane we wszystkich elementach systemu kontroli dostępu, a także łączność między nimi pozostaną bezpieczne.*

Cechą wyróżniającą Nedap spośród innych firm na rynku jest koncentracja na oprogramowaniu mimo silnej tendencji do oferowania rozwiązań typu end-to-end.

– *Wielu użytkowników końcowych korzysta z produktów kupionych wiele lat temu. Często mają problemy z modernizacją czy zmianą systemu kontroli dostępu na nowy. Ten system jest bowiem powiązany z wewnętrznymi bazami danych czy kamerami telewizji dozorowej. Decyzje o wyborze konkretnego systemu zostały podjęte lata temu, a firmy nadal są związane tymi wyborami. Nie mogą tego zmienić ze względów finansowych, nie zawsze mają na to fundusze. To główne wyzwanie, z którym mamy do czynienia codziennie* – powiedział Sieger Volkers, przywołując punkt widzenia klientów.

> Sytuacja gospodarcza ma obecnie ograniczony wpływ na zachowania zakupowe klientów w zakresie inwestycji w zabezpieczenia. Do inwestowania w te rozwiązania zmusza ich coraz większe ryzyko zamachów terrorystycznych i ataków cybernetycznych.

– *W przypadku starszych systemów, gdy firmy chcą przeprowadzić migrację, mogą jej dokonać w kilku etapach. Teraz nie muszą przenosić wszystkiego od razu* – podkreślił Sieger Volkers. – *Mogą to zrobić krok po kroku. W takiej sytuacji nie potrzebujemy przeprowadzać całej inwestycji w danym roku, a firma może rozłożyć te środki na kilka lat, stworzyć plan jej stopniowej realizacji i z czasem w pełni przejść na nowe systemy kontroli dostępu.*

W tym kontekście dobrym rozwiązaniem jest korzystanie z platform otwartych, które pozwalają na późniejsze dodanie dowolnego elementu. Nie zmuszają przy tym do zakupu całej linii produktowej.

Na rynku przeprowadzono wiele fuzji i przejęć. Kiedy firma oferuje kilka rozwiązań, konieczność posiadania systemów otwartych staje się jednym z priorytetów. Sieger Volkers podkreślił jednak, że ostatecznie klient i tak będzie wolał pracować z jednym systemem. ■

NOWI GRACZE W RANKINGU

INTERESUJĄCE INNOWACYJNE SPÓŁKI ZYSKUJĄ PRZEWAGĘ

Większość uczestników tegorocznego rankingu TOP 50 to znane marki, **pojawiło się też kilka nowych firm, m.in. ACTi, Digital Barriers, AxxonSoft, Costar Technologies i Identiv.**

William Pao,
Prasanth Aby Thomas
a&s International

Firma ACTi rozpoczęła działalność jako tradycyjny producent urządzeń dozoru wizyjnego, ale z czasem na poważnie zajęła się analityką, chcąc poszerzyć ofertę dla klientów, przede wszystkim z segmentu handlu detalicznego.

Z kolei AxxonSoft to firma tworząca oprogramowanie umożliwiające pełną integrację z innymi systemami, takimi jak kontrola dostępu czy sygnalizacja pożarowa, oferująca klientom pełne bezpłatne wsparcie techniczne.

Firma Digital Barriers, która uplasowała się na drugiej pozycji pod względem najszybszego wzrostu, zawdzięcza sukces zaawansowanej technologii bezprzewodowego strumieniowego przesyłu obrazu wizyjnego, przeznaczonej do specjalnych wdrożeń w takich obszarach, jak kontrola granic.

Firma Costar natomiast jest znana z odpornych na wstrząsy urządzeń dozoru wizyjnego o wzmocnionej konstrukcji, często stosowanych w projektach administracji rządowej i wojskowych.

Identiv z kolei oferuje specjalistyczne rozwiązania z zakresu kontroli dostępu dla instytucji administracji rządowej, wykorzystując doświadczenie przejętej firmy Hirsch.

W miarę wzrostu konkurencji w branży security wchodzenie w segmenty niszowe i oferowanie rozwiązań poszukiwanych przez takich użytkowników jest jednym ze sposobów do utrzymania rentowności oraz zapewnienia zrównoważonego rozwoju firmy w trudnej sytuacji rynkowej. Nowi uczestnicy rankingu właśnie takim podejściem zapewnili sobie przewagę konkurencyjną.

ACTI STAWIA NA ANALIZĘ DANYCH

Z firmy skoncentrowanej na tradycyjnych rozwiązaniach z zakresu zabezpieczeń ACTi – w warunkach silnej konkurencji na rynku – zmieniła strategię na rzecz dostarczania użytkownikom usług z zakresu analityki biznesowej.

Juber Chu
prezes, ACTi

Tajwańska firma ACTi, po raz pierwszy notowana w rankingu TOP 50, jest pionierem w dziedzinie sieciowych systemów dozoru wizyjnego. Założona w 2003 r. oferowała początkowo tradycyjne rozwiązania z zakresu zabezpieczeń. Konkurencja na rynku wymusiła jednak zmianę jej strategii. Obecnie firma świadczy usługi z zakresu analityki biznesowej.

– *Kiedy tworzyliśmy firmę, przyjęliśmy nazwę ACTi, od: Applied Content Technology Innovation, która odzwierciedla naszą pierwotną wizję zakładającą dostarczanie informacji, zapewniających klientom wymierne korzyści* – powiedział Juber Chu, prezes ACTi. – *Nasz główny cel obejmujący świadczenie usług i dostarczanie rozwiązań w teorii był dobry, ale technologie, głównie w zakresie chmury obliczeniowej i analizy danych, w tamtym momencie były niedostępne. Zaczęliśmy więc od branży security.*

Obecnie nowe technologie, takie jak IoT i chmury obliczeniowe, zaczynają przybierać bardziej dojrzały kształt.

Z tego względu w 2010 r. firma zmieniła kierunek swojej działalności i skupiła się na świadczeniu usług, wykorzystując posiadaną wiedzę w zakresie big data.

W centrum wielu rozwiązań ACTi znajdują się dane dostarczane przez kamery i inne urządzenia. Mogą być one przetwarzane i analizowane przez specjalne algorytmy, które Juber Chu nazywa „robotami".

W ub. r. firma nawiązała partnerstwo strategiczne ze spółką Microsoft Azure Taiwan, której technologie chmurowe zostaną wykorzystane do dostarczenia usług analitycznych, a klienci będą z nich mogli korzystać na zasadzie abonamentu miesięcznego.

Dane z każdego urządzenia są przesyłane do chmury, dlatego dzięki swoim „robotom" ACTi może dostarczać specjalne usługi dostosowane do potrzeb konkretnych użytkowników, zastosowań i celów. Oprócz kwestii bezpieczeństwa firma może pomóc użytkownikom z różnych segmentów w kolejnych dwóch obszarach: zarządzaniu operacyjnym i analityce biznesowej. Przykładowo, aby umożliwić użytkownikom końcowym z branży handlu detalicznego pozyskiwanie informacji o klientach, rozwiązania ACTi obejmują systemy wizyjne zliczające i analizujące ruch w sklepie. Systemy przekazują te dane do chmury obliczeniowej, a dane statystyczne udostępniają uprawnionym użytkownikom na ich komputery i urządzenia mobilne. Na tej podstawie użytkownik może odpowiednio np. ulokować towar na półkach lub dostosować liczbę pracowników.

ACTi oferuje również rozwiązanie, które zapewnia automatyczną obsługę i wsparcie sprzedaży bez angażowania pracowników. Użytkownik może zeskanować wizytówkę klienta, a jej obraz zostanie przekształcony na tekst i dane, które następnie będą analizowane w chmurze obliczeniowej. Zostaną więc pozyskane informacje, czy jest to klient nowy, czy powracający, czym zajmuje się jego firma, a nawet jakich narzędzi może potrzebować w zakresie prowadzonej przez siebie działalności.

Ponadto ACTi nawiązała współpracę z Ricoh, japońskim dostawcą rozwiązań biurowych. co pozwoli jej wykorzystać doświadczenie w dziedzinie analityki biznesowej opartej na chmurze obliczeniowej i zapewnić swoim klientom kompleksowe usługi.

Zamiast oferować jedynie urządzenia dozoru wizyjnego, które w warunkach silnej konkurencji na rynku stały się towarem masowym, firma korzysta z nowych technologii, takich jak IoT i analiza danych, aby zapewnić użytkownikom dodatkowe korzyści. To recepta ACTi na sukces. Firma osiągnęła swój cel w tym zakresie i może służyć za przykład innym podmiotom z branży.

AXXONSOFT ŁĄCZY ANALITYKĘ BIZNESOWĄ Z OPROGRAMOWANIEM, ABY ZWIĘKSZYĆ BEZPIECZEŃSTWO I WYDAJNOŚĆ OPERACYJNĄ

Oprogramowanie AxxonSoft wyróżnia się możliwością pełnej integracji z innymi systemami: dozoru wizyjnego, kontroli dostępu, po sygnalizację pożarową. Zapewnia jednocześnie elastyczność i obniżenie kosztów, które mają kluczowe znaczenie dla integratorów systemów.

Firma AxxonSoft, rosyjski dostawca rozwiązań PSIM i VMS, po raz pierwszy występuje w rankingu TOP 50 branży security. W ciągu kilku lat przekształciła się z przedsiębiorstwa obsługującego rynek Europy Wschodniej w międzynarodową spółkę prowadzącą działalność na całym świecie. Jej sukces ma źródło w doświadczeniu firmy w tworzeniu oprogramowania.

– *Wszystkie osoby, które ze mną pracują, to inżynierowie oprogramowania. Również ja, chociaż od dawna pracuję jako menedżer, jestem z wykształcenia inżynierem oprogramowania* – podkreślił Yury Akhmetov, Business Development Director w AxxonSoft.

Cechą odróżniającą oprogramowanie tej firmy od konkurencji – jak podkreślają przedstawiciele AxxonSoft – jest pełna integracja z innymi systemami: dozoru wizyjnego, kontroli dostępu czy sygnalizacji pożarowej. Zapewnia przy tym elastyczność oraz obniżenie kosztów, które mają kluczowe znaczenie dla integratorów systemów.

– *Nasi konkurenci przekonują: „nasze rozwiązanie możecie integrować z czymkolwiek chcecie". Ale tak naprawdę integratorzy mogą potrzebować integracji jedynie niewielkiej części systemu do konkretnego projektu, zamiast wydawać pieniądze na integrację całych systemów* – powiedział Yury Akhmetov. – *Od początku nasza strategia była oparta na tym, że sami przeprowadzaliśmy integrację. Łączyliśmy przykładowe urządzenia i sami budowaliśmy interfejs, żeby upewnić się, że działa bez zarzutu.*

Firma nie pobiera opłat za wsparcie techniczne ani aktualizacje. Klient tylko raz płaci za produkt. W tej kwocie zawiera się kompleksowa i kompetentna pomoc techniczna.

AxxonSoft wyróżnia się również tym, że w swoje systemy VMS wbudowuje zaawansowane funkcje z zakresu analityki i wyszukiwania. Narzędzie MomentQuest szybko przechodzi do poszukiwanej sceny w zarejestrowanym materiale wizyjnym po określeniu pożądanych kryteriów, z kolei TimeCompressor pozwala na „inteligentne" przeglądanie wszystkich poruszających się obiektów jednocześnie, a interaktywna mapa 3D wizualizuje lokalizację kamer i zdarzeń w obiekcie.

Wprawdzie klienci zazwyczaj kojarzą AxxonSoft z firmą oferującą systemy dozoru wizyjnego, w rzeczywistości na początku funkcjonowała jako dostawca rozwiązań PSIM, a dopiero potem poszerzyła działalność o VMS. Dzisiaj odnosi sukces w obu tych obszarach dzięki produktom AxxonIntellect (PSIM) i AxxonNext (VMS) pomagającym osiągnąć efekt, który Yury Akhmetov określa: „od prostych projektów do rozbudowanych zastosowań profesjonalnych", co wynika głównie ze skalowalnej natury oprogramowania.

– *Nasze produkty wspierają nieograniczoną liczbę lokalizacji i serwerów* – podkreślił Yury Akhmetov, dodając, że najnowsza wersja oprogramowania umożliwia również optymalizację sprzętu komputerowego, pozwalającego użytkownikom końcowym rozpoznawać obiekty na obrazie wizyjnym w czasie rzeczywistym. Inwestor może więc zaoszczędzić na doborze odpowiedniego sprzętu spełniającego jego oczekiwania.

– *Na serwerze i7 CPU przy 8 GB RAM, jaki mamy w zwykłym laptopie, system VMS może obsługiwać sto kamer HD i wyświetlać obraz ze wszystkich jednocześnie. Nie wymaga to zakupu dodatkowych kosztownych urządzeń. Rozwiązanie działa na zwykłej karcie graficznej. To duże osiągnięcie. Integratorzy systemów zaznaczają, że aby utrzymać pracę stu kamer na takim poziomie, dotychczas potrzebowali czterech takich komputerów* – ocenił Yury Akhmetov.

Rozwiązanie PSIM AxxonIntellect oferuje natomiast uniwersalny interfejs, który umożliwia zarządzanie wszystkimi podłączonymi do niego podsystemami.

– *Gdy zatrudniamy nowego operatora, musimy zainwestować w jego szkolenie. Może się zdarzyć tak, że będziemy musieli nauczyć go obsługi trzech różnych interfejsów, a to bywa kosztowne. Staramy się to usprawnić: oferujemy więc jeden interfejs do wszystkiego. Szkolenie z obsługi tradycyjnego systemu PSIM może trwać nawet trzy dni, z obsługi naszego systemu tylko trzy godziny. To rozwiązanie tańsze i dlatego bardziej atrakcyjne dla klienta* – podsumował Yury Akhmetov.

Yury Akhmetov
Business Development Director, AxxonSoft

COSTAR TECHNOLOGIES: RAZEM RAŹNIEJ

Mimo połączenia firmy CohuHD i Costar Video obsługują różne segmenty rynku, uzupełniając się pod kątem oferty produktów i bazy klientów.

Mike Rose
wiceprezes ds. sprzedaży, Costar Technologies

Amerykański Costar Technologies to do niedawna dwa oddzielnie działające przedsiębiorstwa: Costar Video i CohuHD, z których druga firma w 2014 r. wchłonęła pierwszą. Costar Technologies pojawiła się w rankingu TOP 50 po raz pierwszy dzięki dynamicznemu rozwojowi osiągniętemu wspólnie z CohuHD w ubiegłym roku.

– *CohuHD odnotowuje duży wzrost przede wszystkim dzięki większym środkom przeznaczanym na projekty infrastrukturalne w Stanach Zjednoczonych. Wiele z nich wymaga zastosowania technologii, które oferuje CohuHD* – powiedział Mike Rose, wiceprezes ds. sprzedaży w Costar Technologies. – *Pion Costar Video również bardzo dobrze sobie radził w tym roku. Atrakcyjnym rynkiem jest dla nas nadal handel detaliczny, a drugi interesujący nas segment, czyli sektor finansowy, także jest stabilny.*

Pomimo połączenia firmy CohuHD i Costar Video obsługują inne segmenty rynku, uzupełniając się pod kątem oferty produktów i bazy klientów. CohuHD jest znana ze specjalistycznego sprzętu dozoru wizyjnego o wzmocnionej konstrukcji, sprawdzającego się w bardzo trudnych warunkach. Jest on stosowany głównie przez instytucje administracji rządowej i wojsko.

– *Przykładowo w segmencie dozoru ruchu drogowego, w którym kamery umieszcza się na słupach na bardzo ruchliwych skrzyżowaniach lub przy autostradach, konieczna jest niezawodna kamera wymagająca minimalnej obsługi i konserwacji. Obudowy naszych kamer są wypełniane azotem chroniącym je przed dostępem wilgoci. Kamery mają czujniki, które informują użytkowników o ewentualnych awariach* – wyjaśnił Mike Rose.

Costar Video koncentruje się na rynku amerykańskim. Zamierza kierować swoją ofertę dla handlu detalicznego i bankowości również do innych odbiorców. Firma oferuje pełen asortyment kamer, w tym kamery analogowe i sieciowe kamery HD, które są dostosowane do potrzeb tych rynków. Według Mike'a Rose'a jedną z cech wyróżniających segment docelowy Costar Video jest rosnąca liczba kamer analogowych HD, które zapewniają doskonałą jakość obrazu, korzystając z istniejącego okablowania koncentrycznego.

– *Rok lub dwa lata temu myśleliśmy, że to przejściowa moda, że potrwa chwilę, a potem klienci przejdą bezpośrednio na sprzęt sieciowy. Okazało się jednak, że jakość obrazu, wydajność i cena spowodowały, iż technologia ta przetrwała kolejnych pięć lat, a oferowane przez nas produkty HDCVI nadal są dla rynku atrakcyjne* – stwierdził Mike Rose.

Głównym wyzwaniem, z jakim mierzy się Costar Video w swoim segmencie docelowym, jest konkurencja marek azjatyckich, które zdominowały kanały dystrybucji.

– *Producenci azjatyccy wprost zaleali rynek sprzętem o skrajnie niskich cenach. Prowadzą działalność w zasadzie we wszystkich regionach świata i niekiedy konkurują z własnymi klientami poprzez sprzedaż bezpośrednią. Firma Costar takich metod nie stosuje* – zapewnił Mike Rose. – *Naszą receptą na walkę z tak prowadzoną konkurencją jest zejście im z drogi i pozwolenie na masową sprzedaż tanich produktów. My natomiast wykorzystujemy powstałą lukę, wprowadzając niezawodne produkty o znacznie niższym poziomie cenowym niż oferowane przez większych producentów systemów VMS. Nasza oferta jest skierowana na rynek ze średniej półki* – podsumował Mike Rose.

Zak Doffman
prezes,
Digital Barriers

**Brytyjska firma Digital Barriers, która w ostatnich latach dokonała kilku przejęć, odnotowała obecnie ponad 50-procentowy wzrost sprzedaży.
Oferuje m.in. unikatowy produkt pozwalający wykrywać broń palną schowaną pod ubraniem.**

IMPONUJĄCY WZROST DIGITAL BARRIERS

Digital Barriers oferuje inteligentne rozwiązania dozoru wizyjnego. Specjalizuje się w szybkiej transmisji strumieni wizyjnych bez opóźnień, transmisji obrazów w sieciach bezprzewodowych, w tym sieciach telefonii komórkowej, satelitarnych, sieciach typu mesh oraz w chmurze. Spółka zapewnia, że jest w stanie bezprzewodowo przesyłać materiał wizyjny wydajniej niż przy użyciu jakiejkolwiek innej technologii dostępnej na rynku. Oznacza to, że nawet w przypadku gdy dostępna lub opłacalna jest jedynie bardzo mała szerokość pasma, Digital Barriers zapewnia przesyłanie obrazu w czasie rzeczywistym.
– Osiągnęliśmy sukces zarówno dzięki oferowaniu transmisji obrazu wizyjnego z pojazdów, jak i udostępnieniu dozoru wizyjnego dużych obszarów, takich jak granice czy obiekty wojskowe. Te zastosowania stanowią główne obszary rozwoju Digital Barriers
– podkreślił Zak Doffman, prezes firmy.

– Kolejnym obszarem, w którym obserwujemy wzrost, jest analiza treści materiału wizyjnego. Duża liczba zainstalowanych kamer wymaga automatyzacji analizy materiału wizyjnego umożliwiającej wykrywanie zagrożeń. Co istotne, dzięki nowoczesnym funkcjom kamer, które stają się coraz bardziej „inteligentne", nie musimy przesyłać wszystkich informacji do centrum.

Przychody firmy w 2016 r. były o ponad 50% większe niż w roku 2015. Firma przypisuje ten wzrost zmianie strategii biznesowej, przenoszącej nacisk z produktów na rozwiązania, tj. oferowaniu w pełni zintegrowanych rozwiązań zamiast urządzeń i oprogramowania. Pomogło to podtrzymać dotychczasowe lub nawiązać nowe długoterminowe relacje z klientami i partnerami. To z kolei doprowadziło do znacznego, ponad 50-procentowego wzrostu w zakresie rozwiązań zintegrowanych.
– Rok 2016 był dla nas bardzo dobry. Zwiększyliśmy ponad dwukrotnie przychody osiągane za granicą, a łączne przychody firmy o ponad 50%. To bez wątpienia bardzo dużo
– powiedział Doffman.
– W ostatnich pięciu latach zajmowaliśmy się łączeniem różnych technologii, by uzyskać rozwiązania kompleksowe, które teraz są dostępne w naszej ofercie. Mamy kluczowych klientów z niemal 40 krajów. Decydują się na zakup naszych rozwiązań, ponieważ mogą z nich natychmiast korzystać.

Ta brytyjska firma została założona w 2008 r. przez byłych pracowników spółki Detica zajmującej się analizą danych, następnie jako Digital Barriers przejęła kilka innych firm. Obecnie oferuje unikatowy produkt pozwalający wykrywać broń palną schowaną pod ubraniem. Współpracę w tym zakresie nawiązała z G4S, jedną z największych na świecie agencji ochrony osób i mienia.

– Gdy zakładaliśmy firmę, dozór wizyjny stawał się obszarem w coraz większym stopniu wykorzystującym zaawansowane technologie– wspomina Zak Doffman. *– Wtedy rynek był jeszcze zdominowany przez technologie o standardowej rozdzielczości, ale wykorzystanie kamer sieciowych, kamer HD i analizy obrazu wciąż rosło. Uznaliśmy, że przy tak rozdrobnionej branży są technologie, do których wielu klientów na świecie nie ma dostępu. Dlatego dokonaliśmy przejęcia aż 15 spółek. Kupiliśmy potrzebne technologie i stworzyliśmy światowej klasy rozwiązania, które zapewniają nam znaczną przewagę na rynku. Wdrażamy platformę sprzedaży, aby dotrzeć do klientów na całym świecie. W ciągu ostatnich pięciu lat kupiliśmy nowe technologie, zaktualizowaliśmy je, zainwestowaliśmy i opracowaliśmy rozwiązania, które oferujemy klientom na całym świecie.*

Firma jest obecna na większości rynków na świecie, a gros przychodów osiąga w USA (5-krotny wzrost w pierwszej połowie br. finansowego) oraz w Azji.

IDENTIV SKUPIA SIĘ NA SPECJALISTYCZNYCH ROZWIĄZANIACH DLA ADMINISTRACJI RZĄDOWEJ

Połączenie wykorzystania big data, IoT i rozwiązań mobilnych w kontroli dostępu sprawi, że zarządzanie tożsamością będzie ważniejsze niż dotychczas.

John Piccininni
wiceprezes ds. marketingu i rozwoju, Identiv

Identiv, debiutant w tegorocznym rankingu TOP 50, to amerykański producent urządzeń i oprogramowania z zakresu kontroli dostępu oraz zarządzania tożsamością. Niektóre jego produkty są sprzedawane pod marką Hirsch, którą Identiv kupił w 2009 r.
W 2015 r. firma wprowadziła produkty i usługi, obejmujące kompleksowe rozwiązania z zakresu kontroli dostępu na bazie platformy Hirsch Velocity (przeznaczone dla administracji amerykańskiej do zarządzania tożsamością, danymi uwierzytelniającymi i dostępem), platformę kontroli dostępu IC-PAM (sprzedawana na całym świecie przez Cisco i resellerów) oraz czytniki uTrust, które można stosować w niemal każdym systemie (obsługują wiele technologii uwierzytelniania, w tym Wiegand i RS-485 OSDP). Identiv koncentruje się na rynkach, na których dostęp do zasobów fizycznych i logicznych jest ściśle kontrolowany i monitorowany. Najważniejszym klientem firmy jest administracja rządowa USA, wymagająca rozwiązań zgodnych ze standardem FICAM, który określa sposób walidacji cyfrowych certyfikatów przechowywanych na kartach dostępowych do drzwi i sieci.
– Identiv spełnia wszystkie amerykańskie standardy dotyczące kontroli dostępu i monitorowania, w tym wymogi FICAM z zakresu kart inteligentnych. Wysoki poziom szyfrowania na drodze przesyłu danych oparty na standardach ISO zapewnia bezpieczną komunikację od karty do czytnika, od czytnika do kontrolera i od kontrolera do serwera – mówi John Piccininni, wiceprezes ds. marketingu i rozwoju w Identiv. Ponadto firma wykonuje projekty w obiektach infrastruktury krytycznej i edukacyjnych. Oba te segmenty potrzebują rozwiązań, które są bezpieczne, niezawodne i umożliwiają sprawną integrację.
– Placówki edukacyjne potrzebują systemów zabezpieczeń, które ograniczają dostęp do pewnych obszarów, zapewniają otwarty dostęp do innych, zabezpieczają obszary mieszkalne, są zintegrowane z dozorem wizyjnym oraz komunikacją i zarządzaniem działaniami w sytuacjach nagłych, masowymi powiadomieniami i innymi systemami – wyjaśnił Piccininni. *– Zazwyczaj system kontroli dostępu do budynku lub kampusu obejmuje zarządzanie bazą danych studentów danej placówki, pozwala na uwzględnienie informacji na temat studentów i harmonogramów zajęć, przypisuje odpowiednie przywileje dostępu i umożliwia drukowanie identyfikatorów.*
Aby zapewnić tego rodzaju integrację, John Piccininni wskazuje na rolę standaryzacji.
– W tym przypadku należy przestrzegać standardów. Programy, które pozwalają nam komunikować się z innymi systemami, są napisane w standardowych językach programowania. Dzięki tym narzędziom można łatwo zapewnić integrację z zewnętrznymi bazami danych użytkowników. Można również z wyprzedzeniem przesyłać informacje i powiadomienia z naszego systemu do innych, takich jak systemy telewizji dozorowej czy platformy zarządzające – podkreślił.
Zapytany o przyszłość rynku John Piccininni stwierdził, że łączne wykorzystanie big data, IoT i rozwiązań mobilnych w kontroli dostępu będzie trendem, który sprawi, że zarządzanie tożsamością nabierze większego znaczenia.
– Kiedy wszystko się ze sobą łączy, zarówno ludzie, jak i urządzenia muszą posiadać tożsamość, którą będą się posługiwać, aby inni mogli im zaufać. Chodzi o potrzebę zapewnienia zaufania między ludźmi, urządzeniami i procesami
– stwierdził John Piccininni. To jedno z najważniejszych wyzwań w automatyzacji procesów, przy jednoczesnym zapewnieniu wysokiego poziomu bezpieczeństwa.

Schrack Seconet Polska
ul. Domaniewska 44a
02-672 Warszawa
http://schrack-seconet.pl

Będzie dobrze... albo źle

Co czeka branżę bezpieczeństwa pożarowego w 2017 r.?

Początek roku to zwykle czas podsumowań, rachunków sumienia i planów na przyszłość. Świat jest podzielony na ekspertów wróżących wszystkim lub wybranym świetlaną przyszłość oraz takich, którzy wieszczą kłopoty i każą się mieć niektórym lub wszystkim na baczności.

Grzegorz Ćwiek
prezes Schrack Seconet Polska

Można zauważyć, że dla wszystkich interesariuszy rynku bezpieczeństwa, a szczególnie bezpieczeństwa pożarowego, głosy te i prognozy są tyleż ważne, co zupełnie nieistotne. A jednak wszyscy, którzy interesują się poważnie losem tej branży, na przełomie grudnia i stycznia spędzają sporo czasu albo poszukując informacji na ten temat, albo dyskutując. W związku z tym można zadać sobie pytanie: czy warto.
Tak jak nieco przewrotny jest tytuł tego artykułu i jego początek, tak dalej można byłoby brnąć, twierdząc, że albo tak, albo nie. I tu znowu znaleźlibyśmy sporą grupę popierających każde z tych stanowisk. Ale co dalej? Skoro i jedni, i drudzy mają rację, to gdyby nie zastanawiać się nad tym, co dalej lub co by było, nie popełniłoby się błędu. Jednocześnie analizując skrupulatnie dostępne dane, także nie zrobilibyśmy sobie krzywdy, a wręcz przeciwnie. **I tutaj dochodzimy do jednej z ważniejszych i trudniejszych kwestii związanych z rynkiem bezpieczeństwa pożarowego w Polsce. Nie mamy sensownych danych do analizy!**

Rynek bezpieczeństwa pożarowego – czy to przyjrzymy się rynkowi systemów lub urządzeń elektronicznych (produktów aktywnych), czy zabezpieczeniom pasywnym, czy inwestycjom, projektom, instalacjom, fuzjom i przejęciom, czy nawet statystyce pożarowej – wszędzie cisza lub informacje niepełne, zdawkowe... To jeden z największych problemów naszej branży w kraju i bariera dla przedsiębiorców chcących rzetelnie ocenić sytuację na rynku oraz określić swoje szanse na sukces w roku następnym.

Najczęściej czytamy o trendach za granicą, o fuzjach i przejęciach na rynku światowym, nowych i przełomowych technologiach „z Zachodu", ale **o naszym, rodzimym rynku tak naprawdę nie wiemy zbyt wiele. Nie mamy wiedzy lub nawet wiarygodnych szacunków, jaka jest wielkość rynku, np. systemów wykrywania pożaru, ilu jest w Polsce aktywnych projektantów, instalatorów, integratorów. Nie mamy wiedzy, ile firm w branży w danym roku upadło, jaka jest szansa na powodzenie w działalności tutaj, a jakie są bariery i zagrożenia dla start-upów.**
Żadna instytucja publiczna, izba czy agencja badawcza nie prowadzi wiarygodnych (a nawet jakichkolwiek!) statystyk pozwalających na sensowną ocenę i analizę stanu obecnego, więc trudno uzasadniać spekulacje dotyczące przyszłości.
W przypadku firm o ugruntowanej pozycji lub należących do większych grup kapitałowych czy koncernów międzynarodowych taki stan rzeczy może nie stanowić dużej przeszkody w planowaniu przyszłości, bo korzystają z danych dostępnych za granicą lub informacji gromadzonych w ciągu roku przez szerokie grono pracowników lub kooperantów. Ważną kwestią jest znalezienie pewnych analogii, różnic i podobieństw w celu jak najlepszego wykorzystania takich danych w działalności operacyjnej w Polsce lub planowaniu strategicznym, ale tutaj z pomocą przychodzi doświadczenie.
Inaczej przyszłość postrzegają różne grupy interesariuszy naszego rynku: dla producentów wyznaczają ją nowe produkty wprowadzane do obrotu, zmiany w modelu działalności (np. dystrybucyjnej) albo zmiany w strukturze łańcucha wartości.
Zupełnie inaczej nowe wyzwania będą postrzegać duże zespoły projektowe, a jeszcze inaczej mniejsze, freelancerzy. Całkiem odmiennie integratorzy lub drobni instalatorzy.

Brak rzetelnych badań rynkowych, wiarygodnych danych statystycznych i analiz jakościowych to kłopot w prowadzeniu biznesu i planowaniu zrównoważonego wzrostu i rozwoju. Wraz z dojrzewaniem rynku (a od początku jego rozwoju minęło „dopiero" nieco ponad 25 lat) wszyscy liczymy na to, że stanie się on bardziej przewidywalny i przyjazny także dzięki pojawieniu się na nim firm, agencji lub wydawnictw opiniotwórczych, które dostarczą niezbędnych informacji lub przynajmniej uporządkują te, które są dostępne w wielu przypadkowych miejscach.
Żeby do tego doszło, musi zostać spełniony następny warunek, chociaż w Polsce będzie to dość trudne: uczestnicy naszego rynku muszą „chcieć" podzielić się z innymi wiedzą lub przynajmniej niektórymi danymi statystycznymi z własnego podwórka. Wszyscy musimy mieć świadomość, że jeżeli już ktoś zechce przeprowadzić badania w tym zakresie, MY powinniśmy nieobojętnie, a wręcz z zainteresowaniem pomóc w ich przygotowaniu.
Dzięki temu stworzymy również w naszym kraju bardziej przyjazną i przewidywalną przestrzeń do pracy i rozwoju, co z pewnością przełoży się na lepsze wykorzystanie środków finansowych w zakresie inwestycji w nowe produkty, usługi czy rozwój zespołów osobowych. Takiej zmiany życzylibyśmy sobie zapewne wszyscy, wróżąc przyszłość na początku roku.
A jaki ten rok będzie naprawdę, zobaczymy. Dla Schrack Seconet ubiegły był kolejnym rekordowym rokiem w działalności zarówno w Polsce, jak i na świecie. Wraz z nowymi produktami wprowadzanymi do sprzedaży (np. DSO) i coraz większym udziałem w rynku krajowym i globalnym przewidujemy mnóstwo pracy, jeszcze większe zaangażowanie w poważne i ciekawe projekty oraz jeszcze więcej dobrej zabawy podczas organizowanych przez nas imprez własnych (jak Ogólnopolskie Dni Zintegrowanych Systemów Bezpieczeństwa Schrack Seconet i Partnerzy) i ogólnobranżowych (jak Międzynarodowy Zlot Motocyklowy Branży Systemów Bezpieczeństwa czy Branżowe Spotkanie Kobiet).
Przede wszystkim jednak chciałbym podziękować za współpracę w roku ubiegłym wszystkim naszym Klientom, Partnerom, Współpracownikom i całemu Zespołowi Schrack Seconet w Polsce! Nasz ogromny sukces w roku 2016 jest Waszą zasługą. Jestem przekonany, że będziemy wspólnie budowali kolejne sukcesy w roku 2017!

Liczymy na to, że „a&s Polska" także przyczyni się do rozwoju rynku zabezpieczeń w Polsce. Życzymy powodzenia na nowej drodze i kto wie – może to właśnie WY znajdziecie lekarstwo na potrzeby informacyjne naszej branży? – *Grzegorz Ćwiek, prezes Schrack Seconet Polska*

Czy normalizacja sprzyja innowacyjności?

W ostatnich wydaniach „Systemów Alarmowych” zostało opublikowanych kilka artykułów na temat innowacyjności. Był to początek cyklu artykułów prezentujących różne aspekty innowacyjności oraz innowacyjne osiągnięcia firm polskich działających w obszarze zabezpieczeń technicznych. **Redakcja „a&s Polska” zadecydowała o kontynuacji tego cyklu i zaprasza do nadsyłania propozycji interesujących publikacji. Szczególnie mile będą widziane artykuły prezentujące organizację prac rozwojowych i innowacyjnych w firmach polskich oraz ich innowacyjne osiągnięcia.**

Jerzy W. Sobstel
Stowarzyszenie Ekspertów Normalizacji, Walidacji i Certyfikacji NOWACERT

Innowacyjność jest zjawiskiem złożonym, opisywanym z różnych punktów widzenia. Poświęcono jej wiele publikacji, książek i konferencji. Poszukiwaniem odpowiedzi na pytanie postawione w tytule tego artykułu zaczęto się poważnie zajmować stosunkowo niedawno. Systematyczne badania naukowe na ten temat są inspirowane i finansowane przez agendy rządowe w takich krajach jak USA, Niemcy i Wielka Brytania [1], [2], a więc tam, gdzie politykę innowacyjną państwa traktuje się poważnie, nie tylko fasadowoi buduje dla niej solidne podstawy naukowe. „Podręcznik Oslo” [3], który określa podstawy statystycznej oceny innowacyjności, klasyfikuje normy jako wiedzę skodyfikowaną, czyli z natury sztywną i niesprzyjającą nowym pomysłom. Proces opracowywania nowej normy jest natomiast potocznie postrzegany jako długotrwały, złożony i kosztowny, co może opóźniać wdrożenie innowacji, nie przynosząc jej twórcy żadnych korzyści. Te zakorzenione poglądy są obecnie poddawane zasadniczej rewizji.

Pierwsza wersja „Podręcznika Oslo” powstała ćwierć wieku temu i wtedy taka klasyfikacja była w pełni uzasadniona. Ówczesne normy wyrobów, a także dyrektywy europejskie starego podejścia określały konkretne „przepisy” na wykonanie produktów.

Obecnie normy są specyfikacjami wymagań funkcjonalnych stawianych urządzeniom i systemom, określają kryteria dotyczące bezpieczeństwa ich użytkowania, ochrony środowiska itd. Nie ograniczają inwencji projektantów, stwarzając raczej bezpieczne ramy ich działalności twórczej. W przypadku norm zharmonizowanych, np. z rozporządzeniem CPR, są one wręcz katalogiem cech użytkowych, które mogą być poddawane weryfikacji, jeżeli producent sobie tego zażyczy. Różnorodność norm jest także znacznie większa niż było to jeszcze ćwierć wieku temu.

Stosujemy normy zaliczane do kilku grup [4]:

- normy podstawowe – określają terminologię, zasady, znaki i symbole,
- normy badań – definiują warunki i metody przeprowadzania badań oraz interpretacji ich wyników,
- specyfikacje techniczne – definiują charakterystyki produktów (wyrobów i usług) oraz ich wartości progowe, interfejsy i warunki współdziałania, wymagania środowiskowe, wymagania dotyczące zdrowia i bezpieczeństwa,
- normy dotyczące organizacji – opisują funkcje oraz relacje wewnętrzne i zewnętrzne przedsiębiorstw, zarządzanie różnymi aspektami jakości, bezpieczeństwa, zarządzanie projektami i procesami.

Poszczególne rodzaje norm powinny się pojawiać i być stosowane na różnych etapach powstawania nowego produktu: od badań naukowych, poprzez wdrażanie do produkcji i stosowania, aż po moralną „śmierć” i wycofanie z rynku. Sprzyja temu różnorodność dokumentów normalizacyjnych.

Poza pełnymi normami opracowywanymi w Europie przez CEN, CENELEC i ETSI oraz na płaszczyźnie międzynarodowej przez ISO, IEC i ITU są wydawane dokumenty niższej rangi: specyfikacje techniczne, rekomendacje techniczne i porozumienia warsztatowe. Te ostatnie mogą być wstępem do opracowania pełnych norm, ale mogą być opracowane i opublikowane w czasie zaledwie kilku tygodni.

Publikowane w ostatnim czasie analizy oraz materiały konferencyjne akcentują proinnowacyjny charakter norm i procesów normalizacji. Przykładowo w opracowaniu *The Impact of Standardization and Standards on Innovation* [2] przedstawiono analizę wpływu normalizacji na poszczególne fazy wdrażania innowacji.

Po pierwsze na badania, jako stronę podażową innowacyjności, wskazując na normy jako drogę transferu rezultatów badań.

Po drugie na interakcje pomiędzy normami a ochroną własności intelektualnej, identyfikując zarówno efekt wzmacniający, jak i możliwe zagrożenia.

Po trzecie na stronę popytową, gdzie normy umożliwiają marketing nowych wynalazków oraz innowacyjnych technologii i pozyskiwanie zaufania, a także wparcia ze strony wszystkich interesariuszy, czego rezultatem, w szczególności, jest uwzględnianie innowacyjnych wyrobów w zamówieniach publicznych.

Podsumowując wyniki tej analizy, wskazano że:

a) normalizacja wspomaga koncentrację, zachowanie spójności oraz masę krytyczną dla nowych, wyłaniających się technologii i rynków. Pozwala to lepiej wykorzystać posiadane zasoby zarówno ludzkie, jak i finansowe. Jest to szczególnie ważne dla małych i średnich przedsiębiorstw, których nie stać na forsowanie swoich rozwiązań;

b) normy dotyczące metod pomiarowych i testowania pomagają firmom innowacyjnym wykazywać swoim klientom, że ich innowacyjne produkty posiadają deklarowane cechy użytkowe, a także nie stwarzają zagrożenia dla zdrowia, bezpieczeństwa i środowiska. Te cechy użytkowe muszą być zdefiniowane w sposób jednolity (normy terminologiczne), a ich wartości graniczne określone w dokumencie odniesienia (normy produktu);

c) normy kodyfikują i upowszechniają aktualny stan (state of the art) w danej dziedzinie wiedzy, technologii i najlepszych praktyk;

d) otwartość procesu normalizacji oraz dostępność norm umożliwiają konkurencję pomiędzy technologiami i w ramach poszczególnych technologii, przyczyniając się do rozwoju opartego na innowacyjności.

Uważa się obecnie [1], [2], [4], że badania naukowe, normalizacja oraz innowacyjność tworzą (powinny tworzyć) triadę powiązanych i wzajemnie zależnych procesów, które czasami występują naprzemiennie, wzajemnie się stymulując i wzmacniając.

W wielu specyfikacjach konkursów ogłaszanych w ramach programu HORYZONT 2020 pojawia się wymóg powiązania prac badawczych i rozwojowych z istniejącymi normami lub opracowania projektu nowej normy bezpośrednio w ramach projektu. Przykładem takiego konkursu w obszarze bezpieczeństwa jest SEC-19-BES-2016 dotyczący działania innowacyjnego, którego trwałym efektem musi być projekt normy, nad którą prace będą kontynuowane w jednej z europejskich organizacji normalizacyjnych.

Największe europejskie organizacje normalizacyjne (niestety bez udziału PKN) pracowały w projekcie BRIDGIT – *Bridging the Gap between Research and Standardization* [8] finansowanym przez Komisję Europejską oraz EFTA.

Proinnowacyjny charakter normalizacji jest także demonstrowany na licznych konferencjach, takich jak *International Conference on Standardization and Innovation* [5] zorganizowana w CERN w Genewie, *European Conference: Standards-Your Innovation Bridge* [6] czy też *9th International Conference on Standardization and Innovation in Information Technology* [7].

Na zakończenie, mam nadzieję niezbyt reprezentatywny, przykład z rodzimego podwórka. Uczestniczyłem niedawno w jednej z licznych, międzynarodowych konferencji poświęconych innowacyjności. W towarzyszącej konferencji wystawie prezentowały się głównie polskie start-upy. Zapytałem ponad trzydziestu wystawców-innowatorów, czy znają normy dotyczące ich produktów i czy wiedzą, skąd się takie normy biorą. O normach niektórzy z nich coś słyszeli, natomiast nikt z grona młodych inżynierów nie wiedział ani jak, ani gdzie te istotne dla nich normy powstają. Nie wiedzieli też kto te normy opracowuje, a tym bardziej czy i jak w takich pracach mogliby uczestniczyć.

Mówi się, że twórczy geniusz bywa skutkiem niewiedzy o tym, że czegoś nie wolno lub nie da się zrobić. Najwspanialsze jednak pomysły, żeby mogły przekształcić się w innowacje, muszą przejść twardą lekcję zetknięcia z rynkiem, jego regulacjami, normalizacją i certyfikacją, a także z popytem i zamówieniami publicznymi.

Literatura

[1] Eoin O´Sullivan Laure Brevignon-Dodin: *Role of Standardisation in support of Emerging Technologies*. A Study for the Department of Business, Innovation & Skills (BIS) and the Brutish Standards Institution (BSI) University of Cambridge. June 2012
[2] Knut Blind: *The Impact of Standardization and Standards on Innovation*. TU Berlin, Rotterdam School of Management and Fraunhofer FOKUS. Nesta Working Paper 13/15 November 2013
[3] *„Podręcznik Oslo”* Zasady gromadzenia i interpretacji danych dotyczących innowacji. Wydanie trzecie. Wspólne wydawnictwo OECD i Eurostatu. Wydanie polskie 2008.
[4] http://www.cencenelec.eu/research
[5] http://www.iso.org/sites/standardsinnovationconference
[6] http://wsstp.eu/events/european-conference-standards-your-innovation-bridge/
[7] http://sites.ieee.org/siit2015
[8] http://www.cencenelec.eu/research/BRIDGIT/Pages/default.aspx

Ela-compil
ul. Słoneczna 15a, 60-286 Poznań
office@ela.pl
www.ela.pl

Drony

Wykorzystanie bezzałogowych statków powietrznych w systemach bezpieczeństwa

Od kilku lat rynek dronów rozwija się intensywnie zarówno w Polsce, jak i na świecie. **Do niedawna technologia bezzałogowych statków powietrznych była zastrzeżona wyłącznie dla wojska, dziś ma do niej dostęp niemal każdy.** Dostępność jest naturalnie zależna od stopnia skomplikowania, wyposażenia i zasięgu urządzenia.

Norbert Bartkowiak
ela-compil

Drony (bezzałogowe statki powietrzne) mają wiele możliwych zastosowań. Mogą być wykorzystywane nie tylko w ochronie obiektów, ale także w logistyce czy kontroli inwestycji. Są narzędziem, które zarówno poszerza zakres oferowanych usług, jak i znacząco obniża koszty działalności.

Potencjał zastosowania statków powietrznych zwiększają stale ulepszane konstrukcje dronów oraz ich odporność na zjawiska atmosferyczne, coraz większy zasięg, a także bardziej precyzyjne sterowanie.

Na poszerzenie zakresu zastosowań urządzeń ma również wpływ dynamicznie rozwijający się rynek telewizji dozorowej i systemów telemetrycznych, w które drony mogą być wyposażone.

Potencjał zastosowania dronów w systemach bezpieczeństwa

Technologia bezzałogowych statków lotniczych ma ogromny potencjał w przypadku systemów bezpieczeństwa. Do patrolowania terenu, którego ochroną dotychczas zajmowało się nawet kilkaset osób, obecnie można użyć tylko jednego drona.

Obszarami zastosowań nowych technologii są również zintegrowane systemy bezpieczeństwa. W roku 2016 na targach SECURITY w Essen firma ela-soft GmbH zademonstrowała integrację „bezzałogowców" z systemem bezpieczeństwa GEMOS.

Wartością dodaną każdej integracji jest efekt synergii w postaci funkcjonalności, jakiej nie posiada żaden z podsystemów. Tak jest również w przypadku, gdy drony zostają „usieciowione" w ramach jednego systemu. Staje się możliwe nawiązywanie interakcji pomiędzy poszczególnymi podsystemami. Integracja systemu GEMOS z bezzałogowymi statkami lotniczymi wydaje się naturalna, biorąc pod uwagę fakt, że w systemie GEMOS od dawna jest wykorzystywana grafika oparta na współrzędnych pozwalających na określenie położenia danego elementu na mapie.

Możliwe jest zatem zdefiniowanie automatycznej trasy przelotu wykonywanego przez dron bez udziału operatora. Interesującym przykładem jest wykorzystanie dronów wyposażonych w kamery do wsparcia ochrony obwodowej. Może to być np. funkcja patrolowa, zgodnie z którą dron wykonuje zaprogramowany przelot na granicy strzeżonej strefy i przekazuje obraz do stanowiska ochrony obiektu. Dron dokonuje przelotu wg zadanej trasy od punktu A do punktu B, okrążając każdy punkt i przekazując obraz na żywo. Taka misja może zawierać dowolną liczbę punktów trasy i ścieżki. Obserwatora może wspierać moduł analizy obrazu, który prezentuje ewentualne anomalie w czasie rzeczywistym.

Kiedy zostaje osiągnięty końcowy punkt trasy, dron wraca do stacji ładującej. W module kalendarza można również zaplanować misje cykliczne wg założonego wcześniej planu.

Dron może być też poderwany do lotu do konkretnego punktu wskazanego przez system GEMOS. Można wykorzystać zamontowaną na dronie kamerę do weryfikacji alarmu wywołanego w którymś z podsystemów, np. ochrony obwodowej czy sygnalizacji pożarowej.

W przypadku faktycznego wtargnięcia do chronionej strefy operator może przejąć kontrolę nad dronem, aby śledzić ewentualną drogę ucieczki intruza.

Drony mogą być również źródłem sygnału alarmowego, np. gdy podczas zadanego lotu patrolowego pokładowy miernik gazu, temperatury lub kamera termowizyjna wykryją przekroczenie zadanego progu mierzonej wielkości.

Prawny aspekt wykorzystania dronów

W ubiegłym roku (7 września) weszło w życie nowe rozporządzenie Ministra Infrastruktury i Budownictwa zmieniające rozporządzenie w sprawie wyłączenia zastosowania niektórych przepisów ustawy *Prawo lotnicze* do niektórych rodzajów statków powietrznych oraz określenia warunków i wymagań dotyczących używania tych statków. Reguluje ono przepisy dotyczące latania bezzałogowymi statkami powietrznymi.

W rozporządzeniu doprecyzowano istniejące przepisy, wyodrębniając statki powietrzne używane rekreacyjnie lub sportowo od bezzałogowych statków powietrznych (dronów), które są przeznaczone do innych celów, m.in. związanych z prowadzeniem działalności gospodarczej i zarobkowej.

Różne zastosowania urządzeń wymusiły konieczność doprecyzowania przepisów odrębnie dla każdej grupy.

Nowe przepisy dotyczące wykorzystania dronów w działalności gospodarczej nakładają na użytkownika obowiązek posiadania świadectwa kwalifikacji bezzałogowego statku powietrznego. Urządzenia te muszą być też wyposażone w tabliczkę znamionową z nazwą podmiotu będącego właścicielem, światła ostrzegawcze (w nocy), kamizelkę ostrzegawczą, system FailSafe oraz instrukcję operacyjną podmiotu.

Więcej informacji na temat szczegółowych przepisów dotyczących zasad wykorzystania dronów znajduje się na stronie Ministerstwa Infrastruktury i Budownictwa.

Wykorzystanie dronów w praktyce jest zatem ograniczone przepisami prawnymi. Zgodnie z nimi odpowiedzialność za wykonywany lot bezzałogowego statku powietrznego ponosi operator. W przypadku sterowania dronem w sposób automatyczny, wg zaprogramowanych sekwencji, występuje kwestia przypisania odpowiedzialności za taki lot.

Integracja dronów w ramach zintegrowanych systemów bezpieczeństwa dopiero nastąpi. Biorąc pod uwagę dynamiczny rozwój branży dronów na rynku europejskim, można oczekiwać, że dokona się to już wkrótce.

Duży wkład będzie miał również rynek polski, od dawna prężnie działający w tym zakresie. Niedawno 16 listopada 2016 r., odbyło się spotkanie Grupy Założycielskiej Inicjatywy Dronowej, składającej się z kilkudziesięciu podmiotów o różnym statusie prawnym. Ich celem jest utworzenie koalicji na rzecz rozwoju polskiego rynku dronów. W tym roku Polska przejmie prezydencję w Komisji Stałej Europejskiej Organizacji ds. Bezpieczeństwa Żeglugi Powietrznej Eurocontrol.

Eltcrac System Sp. z o.o.
ul. Ruciana 3, 30-803 Kraków
tel. 12 292 48 60, faks 12 292 48 62
biuro@ecsystem.pl | **http://ecsystem.pl** | **http://dsdi.pl**

8 powodów, dla których platforma serwisowa DSDI poprawi jakość usług Twojej firmy

Zintegrowana platforma serwisowa DSDI Serwis została opracowana z myślą o specjalistach z zakresu instalacji. Ten nowatorski pakiet trzech narzędzi zapewnia pełen nadzór nad wykonywanymi serwisami.

Opiera się on na technologii *beacon*, czyli niewielkich rozmiarów urządzeniach bezprzewodowych, które można przymocować w dowolnym miejscu, np. w kasecie domofonowej, kamerze CCTV, czytniku kontroli dostępu, sygnalizatorze lub innych urządzeniach systemów zabezpieczeń. Działają one jak radiolatarnie, wysyłając sygnały radiowe BLT (*Bluetooth Low Energy*), które mogą być łatwo odbierane przez powiązaną aplikację na smartfonie użytkownika, a ich zasięg może być regulowany. Dzięki nim aplikacja DSDI Mobile na telefon z systemem Android, dostępna na platformie Google Play, monitoruje miejsce oraz dokładny czas rozpoczęcia i zakończenia serwisu, a także ułatwia znalezienie najkrótszej drogi do miejsca, w którym znajduje się serwisowane urządzenie.

Ponadto DSDI Mobile pozwala na bieżąco informować, jakie prace i kiedy zostały wykonane, katalogować, opisywać oraz fotografować urządzenia znajdujące się w danej lokalizacji beacona DSDI. Umożliwia również szybki dostęp do historii serwisowej danego systemu i weryfikację przyczyny jego awarii na podstawie przeprowadzonych napraw. Usprawnia proces serwisowania dzięki odbieraniu prac zleconych na dany dzień przez administratora.

Panel internetowy DSDI Manager, uruchamiany za pomocą przeglądarki internetowej, służy do zarządzania serwisem i zespołem serwisantów oraz pozwala odbierać zgłoszenia od firm zewnętrznych. Dzięki niemu można przydzielać pracownikom zadania na dany dzień, sprawdzać aktualny ich status i odbierać wszystkie dane wprowadzane za pomocą aplikacji DSDI Mobile. Panel udostępnia kompleksowe archiwum wykonywanych zleceń wraz z wymiarem czasu pracy poświęconego przez serwisanta na daną instalację. Udostępniając klientowi panel DSDI User, można też odbierać bezpośrednio zgłoszenia o zamawianych serwisach, naprawach oraz przeglądach.

Jeśli chcesz lepiej poznać rozwiązanie, zadzwoń pod numer: **530 788 866**
lub napisz e-mail: **pdorynek@ecsystem.pl**
Firma przygotuje odpowiednią prezentację i warunki współpracy.

Kamery w transporcie publicznym

Mam nieodparte wrażenie, że jeszcze 10 lat temu o bezpieczeństwie komunikacji zbiorowej myślało niewiele osób. Bolączką przewoźników były wszechobecne akty wandalizmu i agresji dokonywane na taborze i podróżnych.

Obraz 1. **Przykład kamery full HD o szerokim kącie obserwacji zamontowanej w autobusie [1]**

OKIEM PASAŻERA

Aż trudno uwierzyć, ale blisko dekadę temu „zapyziała", nieoświetlona stacja kolejowa nikogo nie dziwiła. Rodząca się świadomość dobra wspólnego ulegała pod naporem ogólnego braku zainteresowania stanem infrastruktury, głównie ze strony zarządcy i przewoźnika. Brakowało ławek, koszy na śmieci i tablic z rozkładem jazdy, a wraz z nimi podróżnych. Wprost proporcjonalnie do zniszczeń i liczby śmieci rosła liczba wystraszonych użytkowników komunikacji zbiorowej.
Podróż też nie należała do przyjemnych. Jakość podstawianych pociągów nie odbiegała bowiem od zapuszczonej infrastruktury (np. co trzeci wagon nie miał oświetlenia). Można było wysiąść w dowolnej chwili przez niezabezpieczone drzwi, z czego najchętniej korzystały szajki młodocianych, chcących uniknąć kar za terroryzowanie pasażerów.
Ludzie preferowali raczej własny transport lub korzystanie z usług prywatnych firm przewozowych niż zdewastowane autobusy, tramwaje czy podmiejską kolejkę. Na taki wybór wpływała niska ocena poziomu bezpieczeństwa zarówno w środkach transportu, jak i stosowanej infrastruktury.

Jan T. Grusznic

Całkiem nedawno przewoźnicy, zarządcy infrastruktury i inni zaangażowani w świadczenie usług przewozowych uzmysłowili sobie, że transport zbiorowy jest odbierany przez pasażerów jako całość – jako proces przemieszczania się „od drzwi do drzwi" za pomocą konkretnego środka lokomocji, ale również wszystkich elementów mu towarzyszących. Przewoźnik nie uzyska oczekiwanego zwiększenia liczby pasażerów, jeśli zainwestuje tylko w nowoczesny tabor, pozostawiając resztę niezmienioną, i odwrotnie. Dlatego zmiany powinny mieć – i z moich obserwacji wynika, że mają – charakter całościowy. Przewoźnik w transporcie publicznym ponosi odpowiedzialność za zapewnienie bezpieczeństwa swoim pasażerom, pracownikom oraz majątkowi, a także utrzymanie dobrej reputacji sieci transportowej. Pasażerowie, którzy nie czują się bezpiecznie w środkach komunikacji, nie będą chcieli korzystać z takich usług. Powszechnie zaś wiadomo że rola transportu publicznego w państwach, które mają ambicje rozwijać się w nowoczesny sposób, stale wzrasta dzięki redukcji nadmiernej kongestii[1)] i emisji spalin. Nie dziwią zatem kolejne inwestycje, których zadaniem jest wzrost poczucia bezpieczeństwa wszystkich użytkowników transportu zbiorowego. Dla przykładu PKP PLK do 2023 r. na ten cel przeznaczy 7–9 mld zł rocznie [1]. Transport zbiorowy w powszechnym przekonaniu jest uważany za jedną z najbezpieczniejszych form podróżowania, co znajduje potwierdzenie w statystykach [2]. Dlaczego zatem te ciągłe inwestycje w bezpieczeństwo? Ponieważ jak wynika z badań [3], osoba, która staje się świadkiem (również za pośrednictwem mediów) lub bezpośrednio uczestniczy w zdarzeniu niebezpiecznym, diametralnie zmienia swój pogląd na ryzyko. Pośrednio wpływa to na rezygnację z wyboru transportu zbiorowego. Obniżanie liczby niechcianych zdarzeń wpływa pozytywnie na postrzeganie tego segmentu usług i przekłada się na realny przychód. Stałe inwestycje w bezpieczeństwo są tym bardziej potrzebne, im częściej słychać o atakach terrorystycznych z wykorzystaniem infrastruktury komunikacji publicznej. Również zwiększająca się agresja w społeczeństwie odbija się na poczuciu bezpieczeństwa uczestników transportu publicznego. Nie dziwi zatem wprowadzanie przez przewoźników nowszych rozwiązań mających na celu zwiększenie poziomu bezpieczeństwa podróżnych.

Po wydarzeniach z 11 września 2001 r., kiedy to terroryści Al-Kaidy porwali w USA cztery samoloty, w wyniku czego zginęły 2973 osoby, w tym sześcioro naszych rodaków, wiele krajów (w tym Polska) zrewidowało swoją politykę bezpieczeństwa. Niedługo po tym wydarzeniu Federalna Administracja Lotnictwa wprowadziła nakaz montażu kamer obserwujących przestrzeń pasażerską oraz miejsce przed kabiną pilotów na pokładach samolotów znajdujących się w przestrzeni powietrznej Stanów Zjednoczonych. Dzisiaj takie kamery są na wyposażeniu każdego samolotu rejsowego, jednak obraz z nich nie jest w żaden sposób zapisywany i tym samym nie stanowi pomocy w wyjaśnieniu wydarzeń, do których doszło na pokładzie. Wynika to głównie z braku uregulowań prawnych dotyczących utrzymania prywatności załogi w ich miejscu pracy, jak również prawa do prywatności pasażerów. Pomocne są jednak w zarządzaniu przez załogę powstałymi sytuacjami kryzysowymi (np. awanturujący się pasażerowie). Najistotniejszym elementem tych urządzeń jest, oprócz zgodności elektromagnetycznej, ogniskowa obiektywu, która umożliwia uzyskanie obrazu o horyzontalnym kącie obserwacji 180°[2)]. Tak szeroki kąt uniemożliwia ukrycie się osobie zagrażającej załodze i pasażerom, jednocześnie pilot ma na bieżąco ogólny ogląd sytuacji w przestrzeni pasażerskiej.

Kamery hemisferyczne, pomocne w uzyskaniu ogólnego podglądu sytuacji w przestrzeni pasażerskiej, są interesujące również dla innych przewoźników (obraz 1). Jak zauważyli uczestnicy konferencji „Bezpieczeństwo w publicznym transporcie zbiorowym" zorganizowanej przez Kancelarię Senatu w 2012 r., jedną z głównych bolączek transportu publicznego jest dewastacja mienia [4]. Zgromadzeni wykazywali dużą przydatność monitoringu wizyjnego w szybkiej ocenie przebiegu zdarzenia oraz jako znaczącego elementu prewencyjnego. Dotychczasowe doświadczenia

[1)] Chroniczne zjawisko większego natężenia ruchu środków transportu od przepustowości wykorzystywanej przez nie infrastruktury.

[2)] Polecam lekturę dodatku specjalnego „SA" 4/2014 poświęconego takim kamerom. Do pobrania na www.systemyalarmowe.com.pl

przewoźników wykazały bowiem, że dzięki kamerom zainstalowanym na pokładach pojazdów zazwyczaj udawało się wykryć sprawców dewastacji pojazdów i przystanków, dzięki czemu te zdarzenia występują rzadziej [5].

Uczestnicy konferencji byli zgodni, że w system dozoru wizyjnego powinien być wyposażony docelowo każdy pojazd komunikacji zbiorowej i dozorem obejmować całą przestrzeń pasażerską oraz przestrzeń przed pojazdem. Podkreślono również istotę jakości uzyskanego obrazu, który w przypadku kolizji i stłuczek skraca procedurę ubezpieczeniową.

Niedawny incydent na Dolnym Śląsku związany z eksplozją improwizowanego ładunku wybuchowego pozostawionego we wrocławskim autobusie wykazał, ile są warte obrazy niskiej jakości. Te dostarczone przez przewoźnika i opublikowane przez dolnośląską policję (obraz 2) trudno uznać za użyteczne, choć niewątpliwie przyspieszyły ustalenie przebiegu wydarzeń. Policja, chcąc jak najszybciej rozpocząć poszukiwanie podejrzanego, zdecydowała się na publikację ujęć z kamery zainstalowanej w pobliżu Dworca Głównego, nie zaś tych z autobusu.

Również Państwowa Komisja Wypadków Kolejowych (PKWK), w nawiązaniu do zakończonych lub toczących się wówczas prac dochodzeniowych, już pod koniec 2011 r. nakazała stosowanie kamer rejestrujących tor jazdy pociągu [6]. Według PKWK *posiadanie zapisów obrazu przed pojazdem oraz zapisów głosów maszynistów powtarzających widoczny sygnał przyczyni się do usprawnienia ustalania przyczyn i okoliczności zdarzeń prowadzonych postępowań, w tym do sformułowania właściwych środków zapobiegawczych, jak również rozważania zasadności składanych raportów przez maszynistów, w których opisane są postępowania dyżurnych ruchu lub niewłaściwe sygnały wyświetlane przez sygnalizatory przytorowe*[3].

Powodem zalecenia są nieścisłości związane m.in. z katastrofą w Babach i wątpliwościami, czy do semafora został podany właściwy sygnał[4]. Proces instalacji kamer w lokomotywach spółki PKP Intercity zakończył się w 2014 r., czyli dopiero dwa lata po katastrofie kolejowej pod Szczekocinami, gdzie w wyniku zderzenia dwóch pociągów pospiesznych zginęło 16 osób, 57 zostało rannych.

Obraz 2. **Ujęcie z kamery pokładowej zainstalowanej w autobusie ukazujące postać zamachowca.**

Dla porównania PKP Cargo dysponująca ponad 2500 lokomotyw (PKP Intercity posiada ich ok. 450) dopiero niedawno odebrała pierwszą zmodernizowaną lokomotywę z instalacją przeciwpożarową i kamerami zapisującymi obraz szlaku przed pojazdem [7]. Według zapewnień PKP Intercity oraz PKWK nagrany materiał służy do szybkiego określenia przyczyn wypadków kolejowych oraz do celów szkoleniowych. Co istotne, nie może być przekazywany osobom innym niż wymienione w zaleceniu.

Przyczyną opóźnień we wdrażaniu tzw. kamer szlakowych w PKP Cargo są prawdopodobnie problemy spowodowane zastosowaniem rozwiązań niedostosowanych do instalacji w pojazdach szynowych. Według informacji przekazanych podczas konferencji „Bezpieczeństwo w publicznym transporcie zbiorowym" zamontowane urządzenia *powodowały zakłócenia radiowe i zakłócały system radiołączności pociągowej* [8]. Ujawnione trudności są wywoływane przez sprzęt niezgodny z EN 50121-4:2015 (Emisja i odporność elektromagnetyczna urządzeń sterowania ruchem kolejowym oraz telekomunikacji). Norma ta określa dopuszczalne poziomy emisji i odporności oraz podaje kryteria działania aparatury sterowania ruchem kolejowym i telekomunikacji (S&T), łącznie z systemami zasilania należącymi do S&T, które mogłyby zakłócać inną aparaturę pracującą w środowisku kolei lub zwiększać emisję całkowitą środowiska kolejowego, stwarzając tym samym niebezpieczeństwo zakłóceń elektromagnetycznych (EMI) aparatury znajdującej się poza systemem kolejowym.

Kamery instalowane wewnątrz taboru oprócz zgodności elektromagnetycznej muszą sprostać wielu nietypowym problemom, takim jak ciągła zmiana oświetlenia, stosunkowo szybkie zmiany temperatury, sezonowo wysoki poziom wilgoci w pojazdach czy akty wandalizmu. W przypadku oświetlenia większymi problemami są jego zmienność i nierówne pokrycie sceny. W tradycyjnej konfiguracji kamer silne oświetlenie z zewnątrz powoduje dopasowanie parametrów naświetlania do dominanty oświetlenia, tym samym obniżając czytelność szczegółów w części sceny gorzej doświetlonej.

Problem silnego oświetlenia niegdyś zupełnie niezamierzenie rozwiązywały reklamy wielkoformatowe umieszczane w oknach pojazdów komunikacji miejskiej. Jednak wielu przewoźników zrezygnowało z tego rozwiązania ze względów bezpieczeństwa. Usunięcie reklam z szyb ułatwiło policji sprawdzenie na ujęciach z monitoringu miejskim, co się dzieje wewnątrz pojazdów.

Problem silnego oświetlenia rozwiązuje się obecnie, stosując kamery z funkcją rozszerzonej dynamiki WDR. Dzięki wielokrotnej ekspozycji i łączenia obrazów takie kamery dostarczają użyteczny obraz z miejsc zarówno silnie oświetlonych, jak i zacienionych. Zastosowanie funkcji WDR ma też wady. Ze względu na wielokrotną ekspozycję i różny czas naświetlania może się okazać, że złożony finalny obraz zawiera artefakty – błędy wynikające z nieprawidłowego zaklasyfikowania części obrazów, np. zwielokrotnienie niektórych obiektów w obrazie lub półprzezroczyste obiekty, spod których przebija tło sceny [9]. Chęć posiadania wiernego materiału bez powyższych błędów wymusza zastosowanie innych technik, np. odpowiednie dopasowanie poziomu kontrastu pomiędzy najjaśniejszymi a ciemniejszymi scenami, którego efekt można zobaczyć na obrazie 1.

Wysoka czułość przetworników w obecnie stosowanych kamerach spowodowała, że po zmierzchu dozór wnętrza pojazdu nawet podczas postoju na pętli nie stanowi już takiego problemu, jak jeszcze kilka lat temu. W warunkach nocnych oświetlenie w przestrzeni pasażerskiej jest na ogół utrzymywane na poziomie 100 lx (mierząc 85 cm od podłogi) [10], w przypadkach awaryjnych nie powinien spaść poniżej 10 lx (mierząc 75 cm od podłogi) [11]. Dostępne na rynku kamery bez przeszkód pozwalają uzyskać użyteczny kolorowy obraz ze sceny zarówno o takim poziomie oświetlenia, jak i zdecydowanie niższym.

Obraz 3. **Przykład obrazu zestawionego z dwóch naświetlań przy działającej funkcji WDR w kamerze przy niskim poziomie oświetlenia sceny**

Z kolei dla kamer szlakowych do obserwacji trasy pojazdu wyzwaniem jest jednoczesna obserwacja drogi i sygnałów świetlnych w warunkach nocnych. Funkcja WDR nie spełni swojego zadania, ponieważ z założenia ma ona kompensować nadmiar oświetlenia w scenie, gdy sumaryczny poziom naświetlenia przetwornika jest duży. W przypadku wykorzystania funkcji WDR w kamerze, gdy poziom oświetlenia sceny jest niski, na obrazie ujawnia się okresowy szum wynikający z dodatkowego wzmocnienia sygnału kompensującego zbyt szybki czas naświetlania.

Dotyczy to tylko tych części obrazu, które zostały zaklasyfikowane przez funkcję jako jaśniejsze i potraktowane krótszym czasem otwarcia migawki. Efekt po złożeniu dwóch obrazów (naświetlanych odpowiednio dłużej i krócej) przedstawiono na obrazie 3.

Uwaga, podanie 25 obrazów/s wymaga od kamery podaży jednego obrazu w czasie 40 ms (1/25 s). Oznacza to, że najdłuższy czas migawki nie może być dłuższy niż 1/50 s, a bardzo często jest krótszy. Przetwornik musi bowiem wykonać dwa sczytania danych, a układ przetwarzania

[3] Część treści uzasadnienia PKBWK-076-305/RL/R/11, Warszawa, 22 listopada 2011 r.

[4] W wyniku zbyt dużej prędkości doszło do wykolejenia się pociągu, w wyniku czego dwie osoby poniosły śmierć, a 81 zostało rannych. „Z Biegiem Szyn" nr 3 (59), maj-czerwiec 2012.

sygnałów wymaga czasu, aby złożyć obrazy ze sobą. Zatem do obserwacji szlaku w warunkach słabego oświetlenia w optymalnym układzie będą wymagane dwie kamery: jedna do obserwacji sygnałów świetlnych na sygnalizatorach (obraz 4), druga obserwująca przestrzeń przed pojazdem, wykazująca się lepszą obserwacją otoczenia (obraz 5).
Obie kamery, jeśli są instalowane wewnątrz środka lokomocji, powinny być odizolowane od oświetlonej części kabiny, aby wyeliminować powstawanie odbić na szybie, które skutecznie obniżą użyteczność obrazu.
Pewną nowością w pojazdach transportu publicznego mogą być kamery zliczające. Umieszcza się je na ogół w przejściu w celu zliczania wchodzących i wychodzących pasażerów. Dzięki temu można skutecznie badać efektywność rozkładów jazdy, przebiegu tras linii i wykorzystania taboru. Dotychczas dane zbierali ręcznie pracownicy przewoźnika, którzy liczyli pasażerów na wyselekcjonowanych przystankach. Dzięki zautomatyzowaniu całego procesu można odpowiednio zagospodarować tabor.
Kamery zliczające opierające się na efekcie stereoskopii są montowane nad drzwiami wejściowymi. Poziom skuteczności, zależnie od dostępnych testów, szacuje się na 96–99 proc. Tak wysoka skuteczność jest możliwa dzięki tworzonym mapom głębokości (obraz 3D), które system analizujący tworzy przez wyselekcjonowanie różnic w obrazach dostarczanych przez każdą z kamer. Innymi słowy takie rozwiązanie „wie", co jest tłem, a co obiektem na tym tle. Eliminuje również problemy związane ze zmianami oświetlenia wynikającymi z poruszania się pojazdu, które poważnie ograniczały wykorzystanie typowych systemów zliczających[5].

System

Transport publiczny to nie tylko tabor, to także wszelka infrastruktura towarzysząca: przystanki, pętle, porty czy dworce – miejsca istotne z punktu widzenia utrzymania ciągłości usług transportu publicznego, wpływające na jakość świadczonych usług. Od początku XXI w. właśnie te miejsca ze względu na fakt gromadzenia się znacznej liczby ludzi są

[5] W dodatku *Video Content Analysis* do „Systemów Alarmowych" są dostępne artykuły wybranych firm mających w swoim portfolio systemy zliczania.

Obraz 4. **Kamera z załadowanymi ustawieniami do obserwacji sygnałów świetlnych**

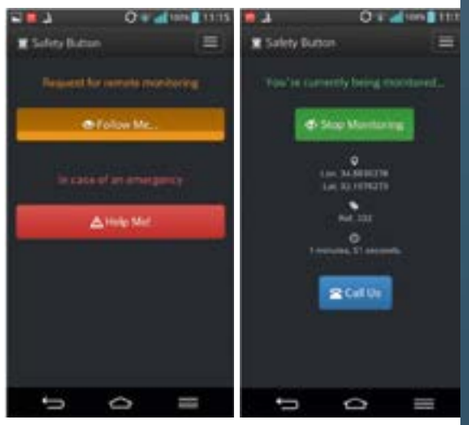
Obraz 5. **Kamera z załadowanymi ustawieniami do obserwacji szlaku**

w kręgu zainteresowania skrajnych organizacji, które chcąc osiągnąć swój cel, nie wahają się wykorzystać elementu terroru. Przykładem mogą być chociażby wydarzenia w moskiewskim metrze w 2004 r., gdzie dokonano zamachu podczas przejazdu pociągu ze stacji Pawieleckaja na stację Awtozawodskaja. Zginęło 41 osób, a ponad 100 zostało rannych.
Sześć lat później, 29 marca 2010 r. doszło do dwóch wybuchów na stacjach metra w centrum Moskwy: Łubianka i Park Kultury. W wyniku eksplozji bomb, które zostały zdetonowane przez dwie kobiety-samobójczynie, zginęło co najmniej 39 osób, a 102 zostały ranne. Z kolei 7 lipca 2005 r.w godzinach porannego szczytu w londyńskim metrze eksplodowały trzy bomby. Terroryści zabili 52 osoby, a około 700 zostało rannych. Przytoczone wydarzenia, poczynając od 11 września 2001 r., przyczyniły się do zmiany procedur bezpieczeństwa i doposażenia technicznego systemami wspomagającymi utrzymanie bezpieczeństwa głównie w portach lotniczych. Obecnie w powszechnym użyciu są detektory do wykrywania śladowych ilości materiałów wybuchowych i kontroli płynów, skanery RTG oraz stacjonarne monitory promieniowania jonizującego. Zaostrzono również procedury związane z kontrolą dostępu, wprowadzając jednocześnie elektroniczne systemy zarządzania przemieszczaniem się osób. Rozbudowano systemy telewizji dozorowej w strefach ogólnodostępnej[6], zastrzeżonej[7] i krytycznej[8], zwiększając tym samym poziom pokrycia terenu obserwowanego m.in. przez SOL.
Pomimo poniesionych kosztów nie udało się powstrzymać eksplozji ładunków wybuchowych w hali odlotów na lotnisku międzynarodowym w Brukseli, do którego doszło w marcu 2016 r. Po przeanalizowaniu tego zdarzenia jako jeden z powodów wskazano brak reakcji na wykrycie anomalii lub zignorowanie informacji przekazanych przez służby wywiadowcze. Wykazano również, że systemy dozoru wizyjnego podają informację, ale nie analizują jej pod względem wizerunkowym, co oznacza, że osoby posługujące się fałszywymi dokumentami przy odrobinie szczęścia mogą przemieszczać się na całym świecie. A przecież są zmuszone do korzystania z istniejącej sieci transportu publicznego, w której działają tysiące kamer, zatem ich schwytanie nie powinno stanowić większego problemu.
Tymczasem problematyka związana z rozpoznawaniem osób zgromadzonych w miejscach publicznych na podstawie biometrii twarzy stoi w kontrze do prawa do prywatności. Aby wyszukać w tłumie osobę poszukiwaną, wszyscy dobrowolnie lub przy nakazie wynikającym z przepisów (których w Polsce na razie brak) musieliby poddać się takiej powszechnej inwigilacji. Zgodnie z literą prawa [12] wizerunek osób przetwarzany przez systemy zarządzające obrazami z kamer nie jest w żaden sposób łączony z innymi danymi, które indywidualizują osobę, a zatem nie stanowi w jego rozumieniu danej osobowej. Inaczej gdy porównuje się dane wizerunkowe na podstawie danych biometrycznych lub innych, gdy potrzebujemy ich do uzyskania wyniku zestawienia dwóch zbiorów danych.
Wydaje się, że troska o bezpieczeństwo obywateli weźmie górę nad prywatnością i przy coraz częstszych próbach atakowania ładu w Europie i na świecie rządzący zdecydują się na wprowadzenie prawa do powszechniejszej inwigilacji społeczeństwa. Być może przekonujące będzie to, że takie prawodawstwo ułatwiłoby wprowadzenie systemów rozpoznawania wizerunku, dzięki czemu interwencja na lotnisku w Brukseli nie byłaby spóźniona i nie zginęłoby 11 osób.
Rząd w Czechach zaaprobował już system do rozpoznawania twarzy zainstalowany na lotnisku w Pradze im. Vaclava Havla w ramach projektu rozbudowy systemu dozoru wizyjnego. Podobne rozwiązania mają zostać wprowadzone na pozostałych lotniskach: w Brnie i Karlowych Warach. Kwestią czasu jest zastosowanie podobnych rozwiązań w innych portach lotniczych, a także w systemach instalowanych na dworcach, pętlach autobusowych i przystankach.

[6] Strefa ogólnodostępna to teren lotniska i jego budynki, do których dostęp nie wymaga posiadania karty identyfikacyjnej (przepustki).
[7] Strefa zastrzeżona to teren lotniska, do którego dostęp ze względów bezpieczeństwa mają wyłącznie osoby uprawnione.
[8] Część krytyczna strefy zastrzeżonej to ta część strefy zastrzeżonej lotniska, do której dostęp osób lub przedmiotów wymaga poddania się kontroli bezpieczeństwa i posiadania dokumentów uprawniających do przebywania w tej strefie.

PARADOKS?

Brak uregulowań prawnych w Polsce prowadzi niekiedy do nietypowego uzasadniania celowości posiadanego systemu dozoru wizyjnego. Według PKP SA kamery zainstalowane na dworcach nie służą dobru publicznemu: „Cel monitoringu wizyjnego jest ukierunkowany na interes gospodarczy spółki, a nie zapewnienie porządku czy bezpieczeństwa publicznego". Chodzi jedynie o „zwiększenie dyscypliny i wydajności pracy" oraz „usprawnienie procesów zarządzania" [13].



Obraz 6. **Przykładowe zrzuty ekranu z telefonu z uruchomioną aplikacją Follow Me firmy NICE**

Utrzymanie bezpieczeństwa w transporcie publicznym stanowi nie lada wyzwanie ze względu na skalę systemu i agregację danych. Żaden z elementów systemu nie może zakłócać działania innych systemów funkcjonujących w obrębie czynnej infrastruktury zarządzania taborem. Wielkość całego systemu determinuje zarówno wybór technologii, która powinna być otwarta, by umożliwić skalowalność, jak i dobór dowolnych elementów spełniających odpowiednie standardy. Dzięki temu stanie się możliwe stosowanie oprogramowania i urządzeń różnych producentów.

Ze względu na liczbę kamer i przetwarzanych strumieni wizyjnych istotne okaże się wykorzystanie analizy zawartości obrazu (VCA), która umożliwi odpowiednie zarządzenie zdarzeniem przez operatora. Obecnie dostępne algorytmy działają raczej w zakresie wykrywania anomalii w scenie, zatem wskazane jest, aby potencjalne scenariusze zdarzeń były w ten sposób skonstruowane. VCA działa najlepiej, gdy mamy skanalizowany ruch lub określone procedury (np. ruch drogowy, kolejowy), gdzie wykrycie zdarzeń spoza regulaminowego ruchu jest stosunkowo proste. W przypadku detekcji zdarzeń w tłumie uzyskanie niskiego stopnia alarmów fałszywych będzie wyjątkowo trudne.

Dozór przystanków komunikacji miejskiej jest na ogół realizowany przy współpracy z miejskim systemem monitoringu. Tylko w niewielu lokalizacjach zdecydowano się na stworzenie odrębnego systemu na potrzeby utrzymania bezpieczeństwa pasażerów. Przykładami mogą być szybki tramwaj w Łodzi i projekt BiT City w Toruniu. Z kolei PKP PLK wyposażyła już przystanki i perony należące do tzw. Warszawskiego Węzła Kolejowego w system dozoru wizyjnego. W ramach wdrażania pierwszego w Polsce dużego systemu kolejowego kamery pojawiły się już na odcinku Warszawa Płudy – Nasielsk. Zamontowanie kamer zmniejszyło liczbę aktów wandalizmu, na czym najbardziej zależało zarządcy. Brakuje jeszcze słupków przywoławczych SOS dla pasażerów, które coraz chętniej są stosowane jako element proaktywny systemu, umożliwiając szybkie zgłaszanie zdarzeń lub nieprawidłowości.

Takie rozwiązania z sukcesem zostały wdrożone na stacjach zmodernizowanej linii SKM w Trójmieście. W państwach Europy Zachodniej oraz USA dla pasażerów komunikacji miejskiej opracowano specjalną aplikację na urządzenia mobilne (obraz 6), która błyskawicznie wysyła powiadomienie do operatora monitoringu wraz z koordynatami GPS. Dzięki temu operator wie, której kamery użyć w celu weryfikacji zgłoszenia.

***

Uruchomione środki z unijnego programu Infrastruktura i Środowisko 2014–2020 niewątpliwie przyczynią się do nowych inwestycji w zakresie rozwoju publicznego transportu zbiorowego. Już wiadomo że są przygotowywane kolejne projekty na kolei związane z poprawą bezpieczeństwa.

Zbliża się gorący okres dla branży elektronicznych systemów zabezpieczeń zarówno w zakresie potencjalnych zysków, jak i pośpiechu z dopasowaniem portfolio do szybko zmieniających się wymagań rynkowych. Podczas gdy rozdzielczość full HD stała się obecnie standardem, producenci będą przekonywać do wyższych rozdzielczości, które też mają swoje ograniczenia, podobnie jak jeszcze kilka lat temu kamery 2 Mpix. Wraz ze zwiększaniem się liczby pikseli na przetworniku zostaną wprowadzone nowe algorytmy optymalizacji strumienia danych przy próbach zachowania użytecznego obrazu. Coraz większa liczba przetwarzanych danych wizyjnych wymusi wprowadzenie efektywniejszych algorytmów analizujących obrazy, opartych na głębokim uczeniu *(Deep Learning)*, w celu skrócenia czasu reakcji na zdarzenie. W dobie tak dużych inwestycji zostanie również potwierdzona zasadność stosowania otwartych protokołów jako gwarancji możliwości dalszej rozbudowy systemów i zwiększenia ich interoperacyjności. Istotne staną się czynniki, obecnie w wyborze urządzeń pomijane: rozbudowana diagnostyka, niska awaryjność i bezpieczeństwo informacji. A wszystko po to, byśmy czuli się bezpieczni.

Literatura

[1] Źródło obrazów wykorzystanych w tekście (z pominięciem obrazu nr 2): Axis Communications AB

[2] Komunikacja publiczna nr 1/2011

[3] Elvik R., Bjornskau T., *How accurately does the public perceive differences in transport risks? An exploratory analysis of scales representing perceived risk?*, Accident Analysis and Prevention 37, Elsevier 2005.

[4] *Bezpieczeństwo w publicznym transporcie zbiorowym*, Konferencja Senackiego Zespołu Infrastruktury 15 października 2012 r., Kancelaria Senatu 2013, zeszyt 15/2013.

[5] *Secure Public Transport in a Changeable World*, November 2010, UITP.

[6] PKBWK-076-305/RL/R/11, Warszawa, 22 listopada 2011 r.

[7] www.pkpcargo.com/pl/aktualnosci/

[8] *Bezpieczeństwo w publicznym transporcie zbiorowym*, Konferencja Senackiego Zespołu Infrastruktury 15 października 2012 r., Kancelaria Senatu 2013, zeszyt 15/2013.

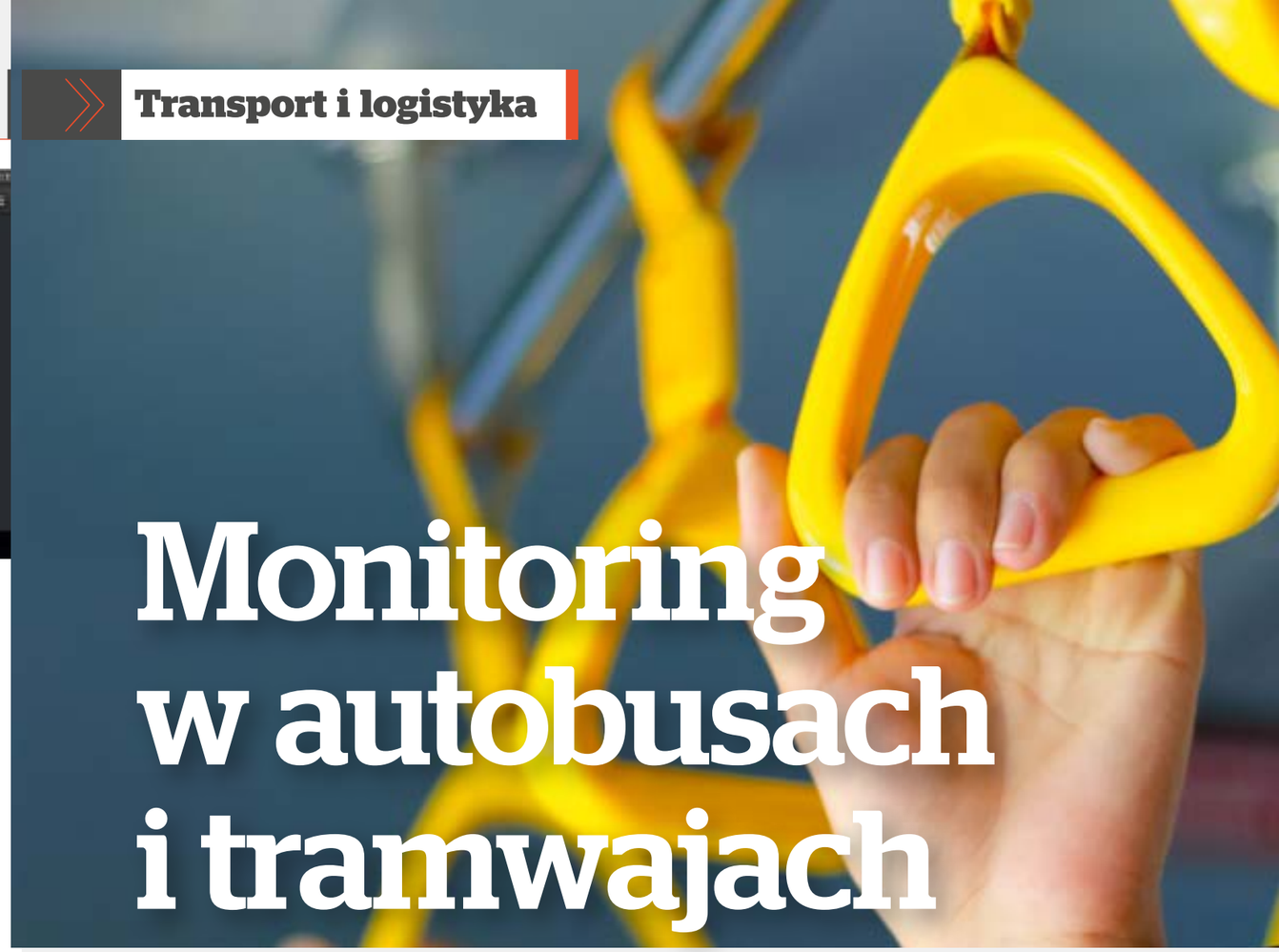
[9] Grusznic J. T.: *WDR w praktyce*, „Systemy Alarmowe" nr 4/2013.

[10] *Rozporządzenie Ministra Infrastruktury z 2 marca 2011 r. w sprawie warunków technicznych tramwajów i trolejbusów oraz zakresu ich niezbędnego wyposażenia*, DzU 2011, poz. 65, poz. 344.

[11] *Jednolite przepisy dotyczące homologacji pojazdów kategorii M2 lub M3 w odniesieniu do ich budowy ogólnej [2015/922]*, Regulamin nr 107 Europejskiej Komisji Gospodarczej Organizacji Narodów Zjednoczonych (EKG ONZ).

[12] *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*, Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 17 grudnia 2013 r. w sprawie ogłoszenia jednolitego tekstu ustawy – Kodeks cywilny, Dz.U. 2014 poz. 121.

[13] https://panoptykon.org/wiadomosc/pociag-do-nadzoru.



Monitoring w autobusach i tramwajach

Zdecydowana większość nowoczesnych pojazdów komunikacji miejskiej jest wyposażona w systemy monitoringu wizyjnego. Dzieje się tak głównie ze względu na chęć ograniczenia aktów wandalizmu oraz zwiększenie poczucia bezpieczeństwa wśród pasażerów. Jednocześnie dowód w postaci wysokiej jakości nagrań może szybko rozstrzygać spory na linii pasażer – operator. Efektywność i użyteczność mobilnych systemów CCTV zależy jednak od zastosowanego rozwiązania i parametrów urządzeń. Autor opisuje te parametry w sposób pozwalający na sprecyzowanie oczekiwań zamawiającego tabor komunikacyjny w dokumentacji przetargowej.

Jakub Adamczyk
Polgard

Funkcjonalność systemu w pojeździe

Podstawową funkcją systemu monitoringu wizyjnego w pojeździe jest rejestrowanie i wyświetlanie obrazu z kamer. Czas zapisu zależy od indywidualnych wymagań klienta, ale z reguły nie powinien być krótszy niż 14 dni. Akceptowalne parametry nagrywania powinny być nie gorsze niż w przypadku rozdzielczości 1920 x 1080 przy 15 kl./s dla kamery czołowej oraz 1280 x 720 przy 10 kl./s dla pozostałych kamer. Aby obraz z kamer wyświetlany na monitorze dotykowym był czytelny, przekątna urządzenia powinna mieć minimum 8 cali. Ważne jest też umożliwienie skonfigurowania dowolnej matrycy wyświetlania kamer[1] oraz podglądu schematu pojazdu z naniesionymi urządzeniami. Wtedy prowadzący pojazd będzie mógł, klikając ikony na schemacie, uruchomić podgląd z wybranej kamery.

Istotną funkcją systemu jest reakcja na sygnały z pojazdu, np. wyświetlanie obrazu z kamery cofania po wrzuceniu biegu wstecznego lub podgląd z kamery lusterkowej po

[1] Matryca wyświetlania kamer oznacza sposób ich wyświetlania na ekranie – pozwala na optymalne zasady podziału, aby maksymalnie wykorzystać przekątną ekranu. Ponadto jest możliwość wyświetlenia, np. tylko obrazów z kamer wewnątrz pojazdu.

otwarciu drzwi. Informacje te mogą być także oznaczone na wyświetlanym materiale (np. w postaci ikony zamkniętych/otwartych drzwi na nagraniach z kamery lusterkowej). Prowadzący pojazd powinien też mieć możliwość podglądu statusu systemu i komponentów (nagrywanie, kamery, stan dysków itp.). Konieczne jest również zapewnienie zaawansowanego systemu zabezpieczeń i zarządzania użytkownikami – administratorowi należy przydzielić dostęp do wszystkich ustawień systemu, ale np. kierowca lub motorniczy nie powinni mieć dostępu do nagrań.

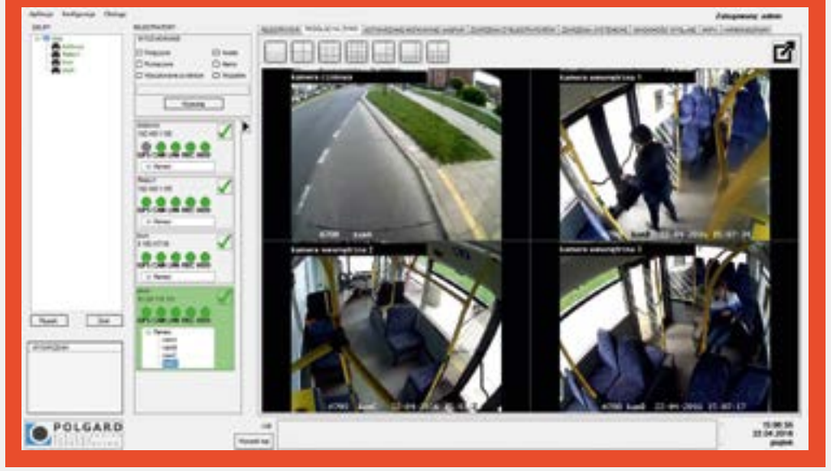
Funkcjonalność systemu zarządzania

Ideą nowoczesnych systemów monitoringu mobilnego jest zarządzanie nimi bez konieczności wchodzenia do pojazdu. Pobieranie nagrań, podgląd na żywo statusu systemu, jego komponentów oraz obrazów z kamer następuje poprzez sieć bezprzewodową. Dlatego wskazane jest wyposażenie systemu w router z obsługą sieci 4G, który automatycznie przełączy sieć GSM na Wi-Fi, gdy pojazd znajdzie się w zajezdni. W celu ułatwienia obsługi warto, aby system zdalnego zarządzania posiadał harmonogram pobieranych nagrań, tj. możliwość zaprogramowania przyszłego zgrywania nagrań, które rozpocznie się automatycznie, gdy pojazd zjedzie do zajezdni i będzie w zasięgu Wi-Fi (tak aby nie było konieczności oczekiwania na autobus lub wykorzystywania nadmiernej ilości danych GSM).
Pobrane materiały powinny być kodowane (mieć znak wodny) oraz zapisane w popularnym formacie wideo (np. mp4), aby było możliwe ich odtwarzanie w powszechnie dostępnych programach.
Z kolei w odtwarzaczach systemu monitoringu standardem jest funkcja stop-klatki, przewijania przód/tył z różnymi prędkościami i wyszukiwania nagrań np. po współrzędnych GPS lub tekście.
System zarządzania CCTV w pojazdach warto wyposażyć w dodatkowe funkcje, takie jak ich wizualizacja na mapie. Wyświetlanie położenia pojazdów powinno być połączone z możliwością łatwej identyfikacji ich statusów (np. szary – nieaktywny, zielony – aktywny i sprawny, czerwony – aktywny i niesprawny). Warto też zapewnić w systemie monitoringu możliwość dwustronnej komunikacji między prowadzącym a operatorem (za pomocą wiadomości lub połączenia głosowego). Grupowanie pojazdów pozwoli z kolei na łatwy podział według marki/typu pojazdu.

Sposób rozmieszczenia urządzeń w pojeździe

Trzeba zadbać o to, by kamery były umieszczone w sposób zapewniający optymalne objęcie przestrzeni pasażerskiej, by wyeliminować powstawanie martwych stref. Strategicznymi miejscami z punktu widzenia identyfikacji osób są niewątpliwie drzwi wejściowe i kabina prowadzącego pojazd oraz ich najbliższe otoczenie, z powodu występowania częstych incydentów w tych obszarach. Liczba kamer ze względu na koszty oraz możliwości montażowe jest często ograniczona, stąd też warto stosować obiektywy o szerokim kącie widzenia, aby maksymalnie wykorzystać ich możliwości (np. o długości ogniskowej 2,8 mm).
Następnym ważnym obszarem do monitorowania jest przestrzeń poza pojazdem, a mianowicie tył, przód oraz drzwi na zewnątrz, w przypadku pojazdów wykorzystujących sieć trakcyjną – kamery obserwujące pantografy. Są to miejsca, których obserwacja pozwala niejednokrotnie na skuteczną ocenę zaistniałych zdarzeń. Kamery zamontowane w tych miejscach nieraz przyczyniły się do oceny ustalenia sprawcy kolizji, są pomocne przy cofaniu w przypadku kamery zamontowanej z tyłu pojazdu oraz działają jako lusterko boczne pozwalające dodatkowo obserwować osoby wsiadające.
Rejestrator powinien być zamontowany w zamkniętej szafce, która uniemożliwia dostęp pasażerom i kierowcom. Wskazane, aby przestrzeń, w której się znajduje, zapewniała odpowiednią wentylację, ponieważ każde urządzenie ma określoną maksymalną temperaturę pracy, powyżej której może ulec awarii.

> Ideą nowoczesnych systemów monitoringu mobilnego jest zarządzanie nimi bez konieczności wchodzenia do pojazdu.



> System monitoringu wizyjnego w pojazdach warto wyposażyć w dodatkowe funkcje, takie jak wizualizacja na mapie, która wyświetla aktualne położenie pojazdów.

Parametry urządzeń

W skład systemu monitoringu w pojazdach wchodzą:
- **rejestrator,**
- **kamery,**
- **monitor umieszczony w kabinie kierowcy,**
- **moduł komunikacyjny,**
- **urządzenia pomocnicze (przełączniki, przetwornice napięcia, UPS).**

Parametry rejestratora, który jest najważniejszym urządzeniem całego systemu, należy dobrać, biorąc pod uwagę kilka czynników. Należy wyposażyć go w dyski o odpowiedniej pojemności, aby umożliwić zapis materiału przez wystarczająco długi okres i przy zachowaniu odpowiednich parametrów. Przykładowo w autobusie z 6 kamerami oraz wymaganym zapisem minimum 14 dni łączna pojemność dysków nie powinna być mniejsza niż 2 TB. Z kolei pojazd wyposażony w 8 kamer, aby zapewnić czas zapisu w dobrej jakości przez 30 dni, powinien mieć łącznie ok. 6 TB przestrzeni dyskowej. Dyski, na których będą zapisywane nagrania, powinny być przeznaczone do ciągłej pracy oraz umieszczone w kieszeniach zamykanych na klucz i mających absorbery drgań. Warto również skorzystać z funkcji backup rejestratora, która umożliwi nagrywanie na dwóch dyskach jednocześnie, co pozwoli na zachowanie nagrań w przypadku awarii jednego z nośników. Wykonawca systemu monitoringu powinien dostarczyć stację dokującą do dysków, aby w razie potrzeby zapewnić szybką ich wymianę. Rejestrator musi być urządzeniem przeznaczonym do zastosowania w pojazdach, czyli mieć odpowiednią budowę, zakres temperatury pracy od -30° do 60° oraz wydajny procesor umożliwiający wykonywanie wymaganych przez operatora funkcji i dalszą rozbudowę.
Zastosowane **kamery wewnętrzne** także muszą być przystosowane do zastosowań w pojazdach – spełnianie wymagań normy EN 50155:2007, brak ostrych krawędzi, posiadanie obudowy o wysokiej wytrzymałości mechanicznej (co najmniej IK08), konstrukcja uniemożliwiająca ich otwarcie przez osoby niepowołane. Muszą obsługiwać rozdzielczość co najmniej full HD (1920 x 1080), mieć funkcję WDR i być wyposażone we wbudowany oświetlacz podczerwieni w celu umożliwienia obserwacji nawet w ciemności. Zaleca się zastosowanie obiektywów o maksymalnej długości ogniskowej 2,8 mm, by osiągnąć szeroki kąt widzenia kamer.
Kamery zewnętrzne, oprócz spełnienia wymogów do zastosowania w pojazdach (norma EN 50155:2007, brak ostrych krawędzi), powinny wyróżniać się jeszcze większą wytrzymałością mechaniczną (najlepiej IK10), wodoszczelnością (IP 68) i mieć wbudowaną grzałkę. Muszą obsługiwać rozdzielczość co najmniej full HD (1920 x 1080), posiadać funkcję WDR i być wyposażone we wbudowany oświetlacz podczerwieni o większym zasięgu (do 30 m). Podobnie jak w przypadku kamer wewnętrznych, ze względu na chęć osiągnięcia szerokiego kąta widzenia kamer, zalecane jest zastosowanie obiektywów o maksymalnej długości ogniskowej 2,8 mm.
Ważnym, lecz często pomijanym (np. w systemach analogowych) urządzeniem jest UPS. Służy on do podtrzymania napięcia rejestratora w celu umożliwienia bezpiecznego wyłączenia systemu i poprawnego zamknięcia np. plików z nagraniami. UPS systemu monitoringu wizyjnego powinien zapewnić podtrzymanie zasilania rejestratora systemu w zaprogramowanym czasie po wyłączeniu głównego zasilania w pojeździe.

Obsługa i serwis systemu

Zapewnienie łączności bezprzewodowej umożliwia prowadzenie dozoru nad działaniem systemu przez jego dostawcę. Firma odpowiedzialna za monitoring w autobusie czy tramwaju powinna stale zdalnie sprawdzać funkcjonowanie CCTV. Po uruchomieniu pojazdu rejestrator musi ponadto sprawdzić swoją wersję oprogramowania na serwerze dostawcy i automatycznie pobrać aktualizację, gdy jest ona dostępna.

Wszystkie przedstawione funkcje i parametry, które powinny cechować nowoczesne systemy monitoringu wizyjnego w komunikacji miejskiej, zostały opracowane na podstawie wieloletniego doświadczenia firmy Polgard, opinii i analiz potrzeb klientów. Każdy przewoźnik ma jednak własne wymagania zgodnie ze specyfiką prowadzonej przez siebie działalności. Aby je spełnić, konieczne jest opracowanie przez dostawcę systemów szytych na miarę. Można to osiągnąć, tylko posiadając własne oprogramowanie i je rozwijając.

Hanwha Techwin Europe
ul. 1-go Maja 38/39
71-627 Szczecin
www.hanwha-security.eu

Bezpieczny transport dzięki Hanwha WiseNet

W świecie pełnym zagrożeń szeroko rozumiane bezpieczeństwo jest odmieniane przez wszystkie przypadki. Nadzór nad środkami transportu ma w tym aspekcie szczególne znaczenie. Wychodząc naprzeciw wyzwaniom, Hanwha Techwin (dawniej Samsung Techwin) oferuje kompleksowe, gotowe rozwiązania zwiększające bezpieczeństwo logistyki, transportu osób i towarów oraz infrastruktury drogowej i kolejowej.

KAMERY

PNF-9010RVM to wandaloodporna kamera hemisferyczna 4K

Obraz wysokiej jakości wymaga również kamer dobrej jakości. Hanwha Techwin posiada w ofercie modele dedykowane do zastosowań transportowych. Oprócz znanej już klientom polskim wandaloodpornej kamery kopułkowej o rozdzielczości full HD typu SNV-6012M wprowadzono nowe modele: SNV-L6013RM, także full HD, z wbudowanym promiennikiem podczerwieni oraz bliźniaczy SNV-L6014RM o tych samych parametrach, ale dodatkowo z wbudowanym mikrofonem i złączem M12.

Na uwagę zasługuje model PNF-9010RVM. To wandaloodporna kamera hemisferyczna 360° o rozdzielczości 4K z wbudowanym promiennikiem podczerwieni, mikrofonem i złączem M12. Wbudowana analityka obrazu obsługuje m.in. zliczanie osób oraz mapowanie gęstości ruchu (*heatmap*).
Wszystkie te kamery mają certyfikat odporności udarowej IK10, większość z nich także certyfikat „kolejowy" na zgodność z normą EN-50155 dopuszczający instalację wewnątrz i na zewnątrz wagonów kolejowych, metra, tramwajowych itp.

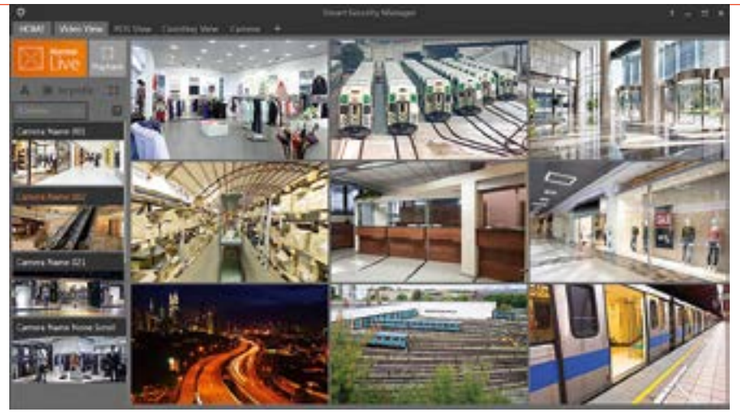
REJESTRACJA

Zapis obrazu w rozwiązaniach transportowych Hanwha Techwin można prowadzić bezpośrednio na kartach SD zainstalowanych w kamerach, na serwerze z oprogramowaniem SSM Transportation lub na dedykowanym rejestratorze SRM-872. To model 8-kanałowy (wizja + dźwięk) z wbudowanymi portami PoE, serwerem DHCP i techniką podłącz i pracuj (*plug & play*). Uruchomienie i konfiguracja systemu trwa kilka minut, a kamerom automatycznie zostają przypisane kanały i adresy IP. Rejestrator jest zgodny ze standardem EN-50155. Odporność udarową i elektromagnetyczną potwierdzają dwa certyfikaty wojskowe, wymagane m.in. przez NATO.

SRM-872 – rejestrator IP z portami PoE

ŚLEDZENIE I POWIADAMIANIE

W komplecie z rejestratorem SRM-872 jest dostępna antena z odbiornikiem GPS, co pozwala na śledzenie pozycji pojazdu w czasie rzeczywistym. System uzupełnia akcelerometr 3-osiowy, rejestrujący przeciążenia w momencie kolizji lub innych zdarzeń drogowych, umożliwiając późniejszą analizę, np. kierunku i siły zderzenia, a co ważniejsze powiadomienie centrum nadzoru bezpośrednio w trakcie zdarzenia. Kierowca pojazdu może mieć także zainstalowany w kabinie przycisk „Panic" pozwalający na uruchomienie zapisu alarmowego i bezpośrednie powiadomienie centrum nadzoru lub policji, np. w razie zaobserwowania w pojeździe aktów wandalizmu, przemocy itp.



ZARZĄDZANIE

Wszystkie elementy monitoringu transportu integruje oprogramowanie SSM Transportation. To dedykowana wersja dobrze znanego klientom polskim pakietu SSM (*Smart Security Manager*). Uproszczony interfejs gwarantuje łatwość obsługi, integracja z mapami Google pozwala na śledzenie ruchu pojazdu w czasie rzeczywistym, z podaniem aktualnej pozycji, prędkości, a także informacji o pojeździe i kierowcy. Zintegrowany serwer archiwizacji pozwala na pobranie zapisanych zdarzeń przez sieć Wi-Fi, np. w momencie, gdy pojazd pojawi się w zajezdni po wykonaniu kursu. Obsługa zapisu awaryjnego umożliwia łatwe odzyskanie zapisu z kart SD zainstalowanych w kamerach, np. w przypadku ewentualnego uszkodzenia rejestratora. Nieskomplikowana integracja z kamerami do rozpoznawania numerów tablic rejestracyjnych (np. SNO-6095RH) zapewnia gromadzenie i wyszukiwanie danych o konkretnych pojazdach poruszających się na chronionym obszarze. Ponadto jest możliwa integracja z systemami parkingowymi.

TRANSMISJA

Rejestrator SRM-872 może być wyposażony w modem LTE/4G i moduł Wi-Fi. Technologia LTE zapewnia łączność z pojazdem w czasie rzeczywistym, pozwalając na transmisję obrazu i dźwięku oraz lokalizację pojazdu. Moduł Wi-Fi natomiast zapewnia transmisję danych do centrum, gdy pojazd znajdzie się w zasięgu tej sieci, np. gdy wróci do zajezdni.

Honeywell Building Solutions
ul. Domaniewska 39
02-672 Warszawa
www.honeywell.com.pl

Automatyka wysokich lotów

Technika Honeywell zastosowana w terminalu T2 Portu Lotniczego w Gdańsku spełnia wszystkie wymagania nowoczesnego lotniska i zapewnia wymierne oszczędności energii. **Inteligentny system zarządzania przynosi korzyści zarówno pracownikom portu lotniczego, jak i podróżnym. Całym obiektem można sterować z jednego stanowiska kontrolnego, dbając tym samym o komfort i bezpieczeństwo pasażerów.**

Dzięki ukończonej w 2015 r. rozbudowie terminalu T2 z gdańskiego lotniska może korzystać 5 mln pasażerów rocznie. Tak duży obiekt wymaga zautomatyzowania procesów zarządzania. Inteligentny system nadzoru, kontroli i sterowania zaprojektowali, zainstalowali i zaprogramowali specjaliści z Honeywell.

Aby zagwarantować bezpieczeństwo pasażerów i sprawne zarządzanie obiektem, zainstalowano pełen pakiet nowoczesnych systemów automatyki.

Mózgiem jest zintegrowany system BMS *Enterprise Building Integrator R410.2*, umożliwiający monitorowanie i zarządzanie całą infrastrukturą bezpieczeństwa, wszystkimi urządzeniami automatyki budynku oraz monitoringiem elektroenergetycznym. Informacje płynące z całego budynku są zbierane z ponad 20 tys. punktów i 600 czytników biometrycznych, a następnie gromadzone w jednym miejscu. Dwa systemy BMS EBI R410 (jeden w terminalu T1, drugi w T2) monitorują, kontrolują i sterują całą infrastrukturą lotniska oraz przyległych obiektów rozproszonych (oddalonych nawet o 30 km od portu lotniczego), podłączonych do infrastruktury przez rozległą sieć CISCO.

System jest nadzorowany przez dwa redundantne centra operacyjne, w których symultanicznie ma do niego dostęp ponad 30 przedstawicieli różnych służb. Możliwość wydzielania i segregacji logicznej informacji, m.in. kamer dla dedykowanych operatorów i służb bezpieczeństwa, pozwala na wnikliwe analizowanie danych z dużą rozdzielczością.

Zapewnia to optymalne zużycie energii, poprawę funkcjonalności, komfortu i bezpieczeństwa. System jest modułowy, dzięki czemu można go łatwo rozbudować, a w przypadku awarii lub konieczności konserwacji - wyłączyć tylko niektóre jego elementy.

Ruch w terminalu T2 jest stale obserwowany przez zintegrowane programowo z BMS EBI cyfrowe kamery dozorowe. Wchodzą one w skład drugiego ważnego systemu Honeywell – zarządza nimi *Digital Video Manager R400*. System telewizji dozorowej IP zawiera ponad 500 kamer Axis, 16 serwerów oraz pamięci masowe 200 TB, zapewniając dostęp do wszystkich nagrań przez ponad miesiąc. System *Digital Video Manager* wdrożony na lotnisku wspiera sieciowy protokół danych multicast, umożliwiający obniżenie zajmowanego pasma sieciowego o 30 do 50 proc.

Na uwagę zasługuje czynne uczestnictwo służb IT lotniska i certyfikowanych przez firmę CISCO inżynierów Honeywell w tuningu systemu sieciowego, by dostosować go do potrzeb platformy DVM.

W system dozoru wizyjnego wbudowano analitykę wideo opartą na algorytmach serwerowych behawioralnych, wykrywających różne zagrożenia, zdefiniowane obiekty oraz osoby za pomocą DVM *Alert Premium View.*

O dobry „klimat" w terminalu dba zainstalowany system HVAC oparty na sterownikach ExcelWEB. Zarządza on ogrzewaniem, wentylacją i klimatyzacją, nie dopuszczając m.in. do sytuacji, w których urządzenia grzewcze i chłodzące działają równocześnie.

W takim newralgicznym obiekcie jak lotnisko efektywny nadzór nad dostępem do wydzielonych pomieszczeń wymagał wdrożenia zaawansowanego systemu kontroli dostępu. Pozwala on na przydzielenie poszczególnym grupom pracowników i współpracowników lotniska określonych praw dostępu do wyznaczonych stref. Optymalnym rozwiązaniem okazał się nowoczesny system kontroli dostępu oparty na sterownikach Honeywell.

Zainstalowany system sygnalizacji pożarowej jest zbudowany na bazie wysokowydajnych central pożarowych Honeywell Esser. Niezawodną ochronę przeciwpożarową gwarantuje aż 5 tys. detektorów współpracujących z pięcioma centralami pożarowymi.

Port lotniczy wymaga również skutecznych zabezpieczeń na wypadek włamania i napadu. Wdrożone rozwiązanie pracuje na centralach Honeywell Galaxy i spełnia najostrzejsze wymogi bezpieczeństwa dużych obiektów o wzmożonym ryzyku. Wykorzystanie najnowszych technik komputerowych, otwarta architektura sprzętowa i programowa oraz rozbudowany zestaw kodów dostępu sprawiają, że system Galaxy jest idealnym rozwiązaniem dla tak wymagającego obiektu, jakim jest terminal lotniczy.

W budynku działa również system monitoringu elektrycznego, składający się z około 2,5 tys. punktów pomiarowych. Komunikują się one z pozostałymi systemami poprzez protokół MODBUS przy użyciu sterowników Schneider Electric.

O dobre samopoczucie pasażerów i pracowników dba system komfortu pomieszczeń, zbudowany na sterownikach Excel WEB i fancoili, które zintegrowano z systemem EBI za pomocą protokołu MODBUS.

> Mózgiem jest zintegrowany system BMS, który umożliwia monitorowanie i zarządzanie całą infrastrukturą bezpieczeństwa, urządzeniami automatyki oraz monitoringiem elektroenergetycznym.

Drugim ważnym systemem jest oprogramowanie *Digital Video Manager* do zarządzania, nagrywania oraz przetwarzania obrazu z ponad pół tysiąca cyfrowych kamer IP firmy Axis. Ostatnim elementem tego ogniwa jest oprogramowanie *Honeywell Active Alert*. Analizuje ono w czasie rzeczywistym obrazy pobierane z serwerów systemu DVM i poddaje je obróbce pod kątem ściśle zdefiniowanych zachowań.

Można tu wyróżnić następujące algorytmy analizy wizyjnej:

- pozostawienie bagażu bez nadzoru,
- wrzucenie obiektu w strefę zakazaną,
- przekroczenie linii przez obiekt, pojazd lub osobę,
- zmiana kierunku ruchu obiektu, pojazdu lub osoby,
- wspinanie się po ogrodzeniu,
- wtargnięcie obiektu, pojazdu lub osoby w strefę wydzieloną,
- wałęsanie się w strefie,
- liczenie osób w zdefiniowanych kierunkach,
- liczenie osób w strefach ewakuacji,
- parkowanie pojazdów w strefach zakazanych,
- pozostawianie pojazdów powyżej zdefiniowanego czasu,
- zawracanie pojazdu w niedozwolonym miejscu,
- jazda w złym kierunku,
- nadzorowanie stref sterylnych dla systemów ochrony obwodowej.

Lista algorytmów jest bogata i zależy od licencji oprogramowania.

System współpracuje również z kamerami termowizyjnymi oraz systemami radarowymi śledzenia obiektów i ludzi. Wykrycie jakiegokolwiek zachowania powoduje w trybie alarmowym przekazanie informacji do systemu BMS EBI oraz DVM i rozpoczęcie zdefiniowanych procedur bezpieczeństwa, np. nagrywanie obrazu z buforem czasowym, wyświetlenie obrazu na monitorach stacji komputerowych, interakcje programowe z systemem kontroli dostępu.

Ponieważ wszystkie zależności są budowane na drodze programowej, w każdej chwili istnieje możliwość zmiany procedur i dostosowanie ich do potrzeb służb ochrony oraz zmieniających się sytuacji. Ma to oczywiście duży wpływ na poprawę bezpieczeństwa obiektu nie tylko podczas normalnych operacji lotniczych, ale także w sytuacjach podwyższonego zagrożenia atakami terrorystycznymi.

Atutem rozwiązania *Honeywell Active Alert* jest możliwość czerpania informacji statystycznych z bazy zarejestrowanych zdarzeń w celach marketingowych, na podstawie badania natężenia ruchu ludzi i pojazdów w rejonie terminalu. Honeywell dostrzega duże możliwości rozwoju na tym polu i szuka dalszych obszarów zastosowań komercyjnych oraz wojskowych.

Bosch Security Systems
ul. Jutrzenki 105
02-231 Warszawa
http://pl.boschsecurity.com

Ochrona obwodowa

więcej niż można dostrzec gołym okiem

Porty lotnicze są bardzo złożonymi projektami obejmującymi niemal wszystkie rodzaje obiektów: od parkingów i terminali, przez centra handlowe i poczekalnie, aż po płyty postojowe i pasy startowe.

W każdym obiekcie portu lotniczego występują zagrożenia związane z obsługą lotów oraz obsługą ruchu pasażerskiego i towarowego, takie jak pożar, akty terroryzmu, przemyt, nielegalna imigracja czy kradzieże. Procedury zabezpieczenia stanowią ogromne wyzwanie ze względu na konieczność monitorowania wielu różnych obszarów – rozległych terenów, parkingów, terminali pasażerskich, płyt postojowych, pasów startowych itp. Jednym z podsystemów, które w największym stopniu przyczyniają się do podniesienia standardu bezpieczeństwa zewnętrznych granic obiektu, są sieciowe systemy dozoru wizyjnego. Najważniejsza jest wysoka jakość przekazywanego obrazu. Wciąż rośnie zapotrzebowanie na obraz o dużym stopniu szczegółowości. Branża przemysłowa jednak zbyt duży nacisk kładzie na wyższą rozdzielczość, która oczywiście zapewnia także większą szczegółowość obrazu. W tym przypadku więcej szczegółów to więcej pikseli i więcej danych, co w konsekwencji oznacza większe nakłady na archiwizację oraz większe obciążenie sieci. Mimo że obraz szczegółowy oczywiście ułatwia rozróżnienie osób lub drobniejszych detali, należy dążyć do zredukowania wymagań w zakresie archiwizacji oraz zmniejszenia obciążenia sieci. Ale to nie wszystko. Zwiększa się także oferta kamer dostępnych na rynku. Nawet jeśli uda się zredukować wymagania w zakresie archiwizacji oraz ograniczyć obciążenie sieci, wciąż pozostaje problem ogromnej ilości danych wymagających pokaźnych zasobów obliczeniowych. W związku z tym trzeba rozwiązać kwestię zarządzania i dostępu do materiałów wideo.

Zarządzanie i dostęp do materiałów wideo

Głównym zadaniem personelu ochrony oraz operatorów systemu dozoru wizyjnego jest powiadamianie o wszystkich podejrzanych zdarzeniach. Wbudowana w kamerę funkcja analizy wideo firmy Bosch analizuje obraz w czasie rzeczywistym i wykrywa podejrzane zdarzenia na podstawie zdefiniowanych wcześniej reguł alarmowych. Umożliwia to operatorom i personelowi ochrony skoncentrowanie się na innych zadaniach i reagowanie tylko w przypadku istotnych zdarzeń. W razie ich wykrycia operatorzy lub personel ochrony mogą przeszukać zapis wideo w celu znalezienia niezbitych dowodów. Znając dokładny czas i miejsce zdarzenia, staje się to jeszcze łatwiejsze, ponieważ w materiale wideo są zapisane znaczniki czasowe. Gdyby jednak użytkownik chciał poznać i przeanalizować trasę ucieczki intruza na podstawie nagrań z wielu kamer, szybkie wykonanie takiego zadania byłoby niemożliwe ze względu na dużą ilość danych.

Pomocne byłoby, gdyby kamery sieciowe „rozumiały" obraz, który rejestrują. Innymi słowy, gdyby nadawały danym wideo „sens i porządek". Ułatwiłoby to zarówno zarządzanie, jak i dostęp do istotnych fragmentów nagrań. Wbudowane funkcje analityczne Bosch realizują wszystko (i jeszcze więcej) w zastępstwie użytkownika. W przypadku zastosowań newralgicznych, takich jak ochrona obwodowa lotnisk, jest dostępna funkcja *Intelligent Video Analysis.*

Inteligencja wbudowana w kamery

Bosch gwarantuje najwyższą jakość i niezawodność funkcji analitycznych. Dzięki temu każda kamera sieciowa z funkcją *Intelligent Video Analysis (IVA)* lub *Essential Analytics* może pracować niezależnie i bez wsparcia centralnego serwera analitycznego. Nie ma więc ryzyka awarii kluczowego elementu systemu. Taka koncepcja jest określana mianem inteligencji rozproszonej. Awaria jednej z kamer lub któregoś z urządzeń kodujących nie wpływa na wydajność pozostałych elementów systemu. Ułatwia to także ewentualną rozbudowę o kolejne urządzenia. Obciążenie sieci i nakłady na archiwizację można zmniejszyć dzięki przesyłaniu tylko istotnych danych, analiza obrazu odbywa się bowiem w kamerze. System jest więc bardziej odporny i elastyczny, a koszty eksploatacji – niższe.

Alarm? Tylko wtedy, gdy to konieczne

Kamery sieciowe z wbudowanymi funkcjami analitycznymi można skonfigurować w taki sposób, aby automatycznie identyfikowały warunki wzbudzenia alarmu, np. osoby zbliżające się lub próbujące sforsować ogrodzenie, a przy tym odróżniały człowieka od zwierzęcia zarejestrowanego przez kamerę. Kryteria wzbudzenia alarmu uwzględniają także przekroczenie jednej lub kilku zdefiniowanych linii, śledzenie określonej trajektorii ruchu oraz zmianę prędkości poruszania się (bieg), kształtu (przykucnięcie) lub proporcji (upadek). Przetwarzanie danych w czasie rzeczywistym bezpośrednio przez kamerę można wykorzystać także do wzbudzania alarmów w przypadku niepożądanego gromadzenia się osób lub wykrywania pozostawionych obiektów. Personel ochrony uzyskuje wszystkie informacje potrzebne do zareagowania i szybkiego podjęcia właściwych działań.

Automatyczne śledzenie poruszających się obiektów może pomóc w weryfikacji lub anulowaniu alarmów, powiadamiając operatora w odpowiedni sposób. Funkcję śledzenia można aktywować, klikając obiekt, lub wcześniej zdefiniować reguły automatycznego śledzenia. Po zintegrowaniu z systemami sygnalizacji włamania i napadu lub kontroli dostępu funkcję inteligentnej analizy wideo można wykorzystać także do automatycznego weryfikowania alarmów generowanych przez te systemy lub do dodatkowego sprawdzenia tożsamości osoby przedstawiającej przy bramie dokument uprawniający do wstępu.

> Ogromnym wyzwaniem jest konieczność monitorowania wielu różnych obszarów: terminali pasażerskich, parkingów, płyt postojowych, pasów startowych...

Analiza obrazu wideo w warunkach ekstremalnych

Przed zewnętrznymi systemami dozoru wizyjnego stoi wiele wyzwań. Mogą to być zmieniające się warunki oświetlenia. O ile niektóre z nich można przewidzieć, np. pora dzienna i nocna, o tyle inne, np. oślepienie kamery światłami przejeżdżającego samochodu lub światło rozproszone przez chmury, są nieprzewidywalne. Kamery sieciowe Bosch ze zintegrowaną funkcją analizy wideo mogą wykrywać zmieniające się warunki oświetlenia i dostosowywać do nich swoje ustawienia w czasie rzeczywistym, co gwarantuje najwyższą jakość obrazu o każdej porze. Inteligentne algorytmy są także pomocne w przypadku niekorzystnych warunków atmosferycznych. Kamery sieciowe ze zintegrowaną funkcją IVA, np. DINION IP starlight 8000 MP firmy Bosch, zostały zaprojektowane w taki sposób, aby zapewniać maksymalnie niezawodną (minimalna liczba fałszywych alarmów) analizę wideo w najbardziej ekstremalnych sytuacjach. Bez problemów wykrywają różnicę między deszczem lub śniegiem a ważnym z punktu bezpieczeństwa obiektem, co ogranicza liczbę fałszywych alarmów wywołanych czynnikami naturalnymi, takimi jak spływająca woda, spadające liście czy poruszające się gałęzie drzew. Inną ważną funkcją jest *Intelligent Defog* poprawiająca wyrazistość obrazu w warunkach mgły, oparów lub zanieczyszczenia powietrza. Funkcja usuwa zmętnienie obrazu, poprawiając widoczność i wydobywając szczegóły poprzez podniesienie kontrastu i nasycenia barw.

Szybkie pozyskiwanie potrzebnych danych

Analizowanie nagranych materiałów wideo to zajęcie nie tylko czasochłonne, ale także obciążone ryzykiem błędu. Kamery sieciowe z wbudowaną funkcją analizy wideo mogą znacznie obniżyć nakłady i przyspieszyć pracę poprzez wprowadzenie pewnego poziomu abstrakcji. Mogą generować metadane w formie prostych tekstów opisujących istotne szczegóły na obrazie, takie jak obiekty czy ruch. Metadane zajmują niewiele miejsca w porównaniu do zapisywanego obrazu, a więc nie zwiększają wymagań w zakresie szerokości pasma transmisji czy przestrzeni dyskowej. Mają jednak ogromną zaletę, ponieważ można je przeszukiwać automatycznie. Przy typowym ustawieniu wystarczy 20 s, aby z wykorzystaniem metadanych z czterogodzinnego nagrania odfiltrować wszystkie istotne sekwencje wideo.

Wytrzymałe kamery do pracy w trudnych warunkach środowiskowych

Bez względu na to, czy jest silny wiatr, pada deszcz, panuje upał, czy temperatura spada poniżej zera, oprócz funkcji analizy wideo kamery stosowane w obszarze ochrony obwodowej muszą sprostać wielu wyzwaniom środowiskowym, zapewniając wysoką jakość obrazu nawet w najtrudniejszych warunkach. Bosch opracował nową linię kamer sieciowych PTZ, wkładając w ich rozwój całą swoją wiedzę i doświadczenie z dziedziny mechaniki oraz sieciowych systemów dozoru wizyjnego. Inteligentne kamery sieciowe MIC IP starlight 7000 HD oraz MIC IP dynamic 7000 HD łączą niemal niezniszczalną obudowę z funkcją automatycznego czyszczenia.

Optex Security
ul. Bitwy Warszawskiej 1920 r. 7b
02-366 Warszawa
www.optex.com.pl

REDSCAN
Laserowa czujka skanująca

Zapewnienie bezpieczeństwa w obiektach i środkach komunikacji publicznej stanowi coraz bardziej istotny obszar dla branży security w Polsce.

Marlena Witkowska
OPTEX Security

Bezpieczeństwo na lotniskach i w obiektach infrastruktury kolejowej zapewnia laserowa czujka skanująca REDSCAN.

Technologia

REDSCAN wykorzystuje technologię skanowania przestrzeni wiązką lasera IR (dł. fali 905 nm, kl. bezp. 1). Promień lasera jest kierowany w określony punkt za pomocą lustra obracającego się z dużą prędkością. Rozdzielczość skanowania wynosi 0,25 lub 0,125 stopnia. Bazowym parametrem do analizy jest „czas przelotu", czyli czas od momentu emisji każdej wiązki do jej powrotu do odbiornika po odbiciu od przeszkody. Analiza zależności kąta, czasu i odległości dla każdej wiązki pozwala obliczyć rozmiary intruza lub przedmiotu (powyżej 2,5 cm), jego położenia i pokonanego dystansu. Stanowi to podstawę do wysłania sygnału alarmowego generowanego przez obiekt o określonych wymiarach, poruszający się z różną prędkością. Wszystkie procesy obliczeniowe odbywają się w układach elektronicznych czujki i nie wymagają wsparcia przez komputer zewnętrzny.

Charakterystyka pracy

Zewnętrzna czujka REDSCAN jest wyposażona w algorytmy wykrywania dostosowane do sposobu montażu: pion, poziom, pod kątem. Zależnie od aplikacji można wybrać predefiniowane ustawienia lub zdefiniować parametry w zależności od sytuacji, np. wielkość przerzucanego przedmiotu lub czas przebywania w określonym miejscu. Obszar działania jest niewidzialną taflą, której kształt można dopasować do wymagań. Analogicznie można zabezpieczyć całą fasadę budynku. Czujka jest wyposażona w algorytm kompensacji mgły, opadów deszczu i śniegu, a przekroczenie brzegowych warunków przejrzystości powietrza wywołuje alarm o zakłóceniach środowiskowych.

Obszar detekcji jest podzielony na strefy, co pozwala na skierowanie kamery dokładnie na scenę, z której pochodzi sygnał alarmowy. Sygnały alarmowe są wysyłane przez wyjścia przekaźnikowe NO lub połączenia Ethernet. REDSCAN mini RLS-2020S może przyjmować sygnały NO/NC poprzez terminal wejściowy. Dopasowanie kształtu obszaru detekcji do wymagań użytkownika, rozmieszczenie stref alarmowych, wybór algorytmu pracy wykonuje się za pomocą dedykowanego oprogramowania. Strefa alarmowania może obejmować obszary zwarte i rozproszone, można także ustawić kilka schematów rozmieszczenia stref w jednym urządzeniu (np. strefa „dzień/noc", „otwarcie bramy", „trasa obchodu" itp.). i sterować nimi poprzez sieć komputerową.

Precyzyjne wyznaczenie granicy zasięgu (pochylenia czujki) czy sprawdzenie poziomu tafli (instalacja w poziomie) nad nierównym podłożem ułatwia detektor wiązki lasera.

Zasłonięcie części okna czujki, zabrudzenie lub przemieszczenie korpusu czujki widziane jako zmiana rozmieszczenia stałych obiektów w przestrzeni jest sygnalizowane jako sabotaż.

1. Zabezpieczenie przejazdów kolejowych

Technologia laserowa dzięki możliwościom integracji z innymi systemami znalazła szerokie zastosowanie w środkach komunikacji publicznej. Przykładowo brytyjski Network Rail, chcąc zwiększyć bezpieczeństwo na przejazdach kolejowych, zastosował dodatkowy system wykrywania przeszkód współpracujący równolegle z systemem RADAR i urządzeniami nadzorującymi. RADAR wykrywa pojazdy lub duże przedmioty, które mogą spowodować uszkodzenia pociągu i zagrażać bezpieczeństwu pasażerów (*rys. 1*).

Z kolei system LIDAR jest przeznaczony do ochrony pieszych i rowerzystów, którzy mogą zostać uwięzieni pomiędzy barierami. Wyzwaniem było zaprojektowanie systemu wystarczająco czułego, aby wykryć stojącego, leżącego lub przechodzącego przez tory dziecka, a także sprostanie rygorystycznym wymaganiom Network Rail. Zaprojektowano w pełni zautomatyzowany system wykrywania oparty na technologii laserowej OPTEX i zintegrowano go z systemem sygnalizacji kolejowej. System LIDAR informuje, gdy przejazd kolejowy jest aktywny, a system wykrywania skanuje obszary przejścia i wewnątrz barier. Jeżeli przejście jest wolne, kolor sygnału zmienia się na zielony i pociąg może bezpiecznie przejechać. Gdy zostanie wykryty obiekt, bariery są podnoszone, umożliwiając obiektowi (pojazdowi lub pieszemu) opuszczenie terenu przed przejazdem pociągu. Jeśli obiekt jest statyczny, a system przeszedł trzy cykle, komunikat jest wysyłany do maszynisty pociągu, który może zmniejszyć prędkość jazdy, aby określić, co utrudnia przejazd.

Opracowano także specyficzne algorytmy do analizy poszczególnych przeszkód naturalnych, jak piętrzący się śnieg na torach czy chwasty. Podobne systemy są testowane przez koleje niemieckie, szwajcarskie i portugalskie.

2. Wykrywanie ludzi i obiektów znajdujących się na torowisku

Innym przykładem zastosowania technologii laserowej OPTEX jest wykrywanie osób, które przez przypadek bądź celowo przeszły z peronu na tory, lub alarmowanie o obiektach pozostawionych na peronach czy torach. Wyzwaniem było dostosowanie do warunków oświetleniowych (światło pociągu, olśnienia czy refleksy, praca w nocy). Sam monitoring wizyjny nie zdawał egzaminu, powstawało bowiem zbyt dużo fałszywych alarmów.

Obszar detekcji REDSCAN został zdefiniowany do wykrywania ludzi i przedmiotów o określonej wielkości, a przejeżdżające pociągi nie wywoływały alarmów. System może być zintegrowany z CCTV i podłączony do systemu sygnalizacji ruchem (*rys. 2*).

3. Ochrona tunelu metra

Wandalizm, graffiti i kradzieże miedzi powodują duże straty. Aby im zapobiegać, zaprojektowano system monitorujący wejście do tunelu. Aplikacja wymagała takiej konfiguracji systemu, aby sygnał alarmowy o wejściu do tunelu był generowany nawet, gdy jednocześnie przejeżdża pociąg. Największym problemem było poradzenie sobie z trudnymi warunkami oświetleniowymi (światła pociągu, cienie, refleksy). Zastosowanie monitoringu wizyjnego nie przyniosło efektu, ponieważ generował zbyt wiele fałszywych alarmów. Skutecznym rozwiązaniem okazało się zastosowanie technologii laserowej OPTEX. Za pomocą czujki RLS-3060 utworzono obszar detekcji w kształcie wirtualnej ściany w płaszczyźnie wejścia do tunelu (*rys. 3*) tak skonfigurowany, żeby przejeżdżające pociągi nie powodowały alarmu. System alarmuje jedynie wtedy, gdy człowiek przekracza linię wejścia do tunelu. System można zintegrować z CCTV i przekazywać sygnały alarmowe operatorowi.

4. Wykrywanie „przerzucania paszportów" na lotniskach

Jednym z najważniejszych elementów w systemie ochrony portów lotniczych jest kontrola paszportowa. Możliwość przekazania dokumentów osobistych innej osobie ponad istniejącymi przegrodami w celu nieuprawnionego przekroczenia granicy należy do głównych problemów, z którymi mają do czynienia organy kontrolne.

Na lotnisku w Grecji zastosowano czujki REDSCAN oraz dwie 5-megapikselowe kamery do weryfikacji. Czujki wyposażono w specjalnie przygotowane oprogramowanie analityczne i umieszczono na wysokości górnej krawędzi przegrody (*rys. 4*). Obszar detekcji miał postać wirtualnego sufitu ponad strefą kontroli paszportowej. Zadaniem detektora jest wykrycie paszportu „przecinającego" linię sufitu w czasie przerzucania go do strefy i poza strefę. Specjalne oprogramowanie w wersji „airport" wykrywa obiekty niewielkich rozmiarów poruszające się z dużą prędkością. Istotne znaczenie ma odległość strefy detekcji od miejsca zamontowania skanerów REDSCAN. Oprócz sygnału alarmowego do kamery lub oprogramowania do dozoru wizyjnego są przekazywane współrzędne *xy* miejsca zdarzenia. Pozwala to precyzyjnie zlokalizować przedmiot na obrazie. Użycie kamer wysokiej rozdzielczości z cyfrowym zoomem ułatwia identyfikację osoby wykonującej zabronioną operację. Zadaniem dodatkowego skanera jest monitorowanie obszaru poza strefą kontroli w celu zwiększenia skuteczności działania systemu.

Przeprowadzone próby rozmieszczenia skanerów oraz dopasowanie parametrów detekcji pozwoliły na uzyskanie 100-procentowej skuteczności wykrywania.

Rys. 1. Regulacje brytyjskie wymagają zastosowania dwóch czujek. Aby spełnić wymagania kolei niemieckich, wystarczy jedna czujka.

Rys. 2. Czujka umieszczona poziomo wykrywa obiekty znajdujące się na torowisku i wysyła sygnały do systemu CCTV i sterowania ruchem.

Rys. 3. Charakterystyka detekcji REDSCAN umożliwia wykrywanie człowieka także w czasie, gdy przejeżdża pociąg.

Rys. 4. Czujka wysyła współrzędne miejsca zdarzenia, a kamera megapikselowa zapewnia dokładną identyfikację sprawcy.

SATEL
ul. Budowlanych 66
80-298 Gdańsk
www.satel.pl

Kontrola dostępu w służbie ochrony podróżnych

Bezpieczeństwo podróżnych jest priorytetem każdego przewoźnika. W jaki sposób można o nie zadbać? Korzystając z nowoczesnej technologii!

Dworzec, lotnisko czy stacja metra to miejsca, gdzie codziennie przemieszczają się tysiące ludzi. Ze względów bezpieczeństwa dostęp do pomieszczeń służbowych, korytarzy technicznych czy nieczynnych na co dzień przejść ewakuacyjnych musi więc być ściśle nadzorowany. Konieczne jest zapewnienie jak najszybszego dostępu osobom uprawnionym, z kolei przy próbach nieautoryzowanego przejścia – jego skuteczne uniemożliwienie. Z tego powodu miejsca te wymagają zastosowania zaawansowanych instalacji kontroli dostępu, takich jak system ACCO NET firmy SATEL zbudowany z użyciem wyspecjalizowanych modułów mikroprocesorowych.

Budowa systemu

ACCO NET to system kontroli dostępu o architekturze rozproszonej umożliwiający obsługę dziesiątek tysięcy użytkowników. Jest oparty na centralach ACCO-NT współpracujących z ACCO Server za pośrednictwem komunikacji sieciowej z protokołem TCP/IP. Dzięki skalowalności, tj. możliwości dołączania do jednego systemu nieograniczonej liczby central, może zapewnić nadzór nad bardzo dużym obiektem. Doskonale sprawdzi się także w zarządzaniu bezpieczeństwem grupy budynków, np. sieci dworców czy stacji metra.
Pojedyncza centrala ACCO-NT umożliwia utworzenie do 255 stref obejmujących m.in. grupy drzwi, bramek dwukierunkowych, tripodów czy wind. W każdej nadzorowanej strefie mogą się znajdować urządzenia wykonawcze: kontrolery przejść ACCO-KPWG oraz ACCO-KP. Do nich są podłączane terminale użytkowników: czytniki kart, np. CZ-EMM, manipulatory ACCO-KLCDR, klawiatury ACCO-SCR-BG oraz inne czytniki obsługujące protokół WIEGAND 26. Rozbudowa systemu o moduły rozszerzeń umożliwia obsługę wejść i wyjść, a także pilotów.
W przypadku wystąpienia problemów z komunikacją nadzór nad kontrolowanym przejściem zostanie zachowany. Dotyczy to zarówno szyfrowanego połączenia TCP/IP z serwerem, jak i komunikacji centrala–kontroler–terminal. W pamięci ACCO-NT można zapisać do miliona zdarzeń własnych oraz do 100 tys. zdarzeń z każdego kontrolera, w tym informacje o nawet 8 tys. aktywnych użytkownikach. Po odzyskaniu połączenia wszystkie dane są przesyłane do serwera.

Zarządzanie i obsługa

Do konfiguracji systemu służy oprogramowanie ACCO Soft. Administrator może budować w nim schematy dostępu dla poszczególnych użytkowników lub grup, łącznie z czasowymi harmonogramami i ustalaniem ścieżek (tras), określając hierarchię dostępu do przejść. Przykładowo możliwość otwarcia kolejnych drzwi użytkownik może uzyskać dopiero po zalogowaniu się we wcześniej zdefiniowanym terminalu.
Istotną cechą ACCO NET jest funkcja *anti-passback* blokująca autoryzację identyfikatorów danego użytkownika do wszystkich wejść do strefy (nie tylko pojedynczego przejścia), jeśli jej nie opuścił. W ten sposób zapobiega się wejściu przy użyciu np. skopiowanej karty lub skradzionego kodu.
Do obsługi systemu służy aplikacja internetowa ACCO Web umożliwiająca przeglądanie wielopoziomowych map nadzorowanych obiektów, a także przełączanie się między obiektami, centralami i pojedynczymi strefami, co zapewnia szybki dostęp do informacji o ich stanie. Z poziomu mapy można też zdalnie obsługiwać pojedyncze przejścia i mieć podgląd z kamer IP w czasie rzeczywistym.
ACCO Web pozwala także na tworzenie raportów dotyczących obecności użytkowników m.in. ze zliczaniem czasu ich pracy, monitorowaniem lokalizacji i weryfikacją ścieżek, którymi się przemieszczali.

Axis Communications Poland
ul. Domaniewska 39A
02-672 Warszawa
www.axis.com/pl

Wizyjna kontrola przesyłek gwarantuje efektywne dostawy

Patrik Anderson
Director Business Development Transportation, Axis Communications

Klienci z segmentu transportu i logistyki nieustannie mierzą się z trudnościami w przesyłaniu towarów z punktu A do B. Ten proces jest skomplikowany i pełen wyzwań.

Ataki i wypadki

Patrząc na globalny rynek logistyki pod kątem bezpieczeństwa, można zaobserwować nasilenie się ataków na przewoźników w coraz większej liczbie regionów oraz w kolejnych rodzajach środków transportu. Organizacje i instytucje rządowe publikują alarmujące statystyki. Przewożone towary stają się celem zorganizowanych grup przestępczych, co przy zwiększającej się fragmentacji łańcucha logistycznego stawia przed nieznanymi wcześniej wyzwaniami. Rosną również wymagania stawiane poszczególnym ogniwom systemu dostaw.
Jak sobie poradzić ze zwiększającą się liczbą tego typu incydentów? Jak pomóc w podniesieniu bezpieczeństwa zarówno kierowców, jak i zatowarowanych ciężarówek czy przyczep?

Sprawne wyszukiwanie i śledzenie

Jednym ze sposobów jest zastosowanie różnych metod telemetrycznych do wyszukiwania i śledzenia towarów na trasie przewozu. Niektórzy przeprowadzają taką weryfikację po incydencie, żeby sprawdzić trasę, jaką pokonały towary. Inni natomiast w ten sposób monitorują i kontrolują zarówno floty, jak i transportowane towary w czasie rzeczywistym.
Druga metoda bazuje na identyfikacji przewożonych dóbr poprzez skanowanie kodów kreskowych lub zbliżeniowych RFID w magazynach, centrach logistycznych czy przeładunkowych. Jednak ten sposób nie pozwala zobaczyć, co wydarzyło się z daną przesyłką ani jaki jest bieżący status towarów. Nie można określić, kto i co zrobił, kiedy, dlaczego i jak to wpłynęło na produkty.

Widoczność bez śledzenia

Jak zatem można uzyskać klarowny podgląd sytuacji, unikając kosztownej i czasochłonnej kontroli podczas prowadzonych postępowań wyjaśniających (wypadki, roszczenia, ataki na transport i towary)? Co zrobić, by uzyskać wyraźny obraz z dowolnego magazynu, stacji przeładunkowej, centrum logistycznego, ciężarówki, przyczepy czy samochodu dostawczego?
Pierwszym krokiem jest wyposażenie wszystkich lokalizacji i środków transportu w nowoczesne sieciowe kamery dozoru wizyjnego. Urządzenia nie tylko dostarczą wysokiej jakości obraz niezależnie od warunków oświetlenia i temperatury, ale dzięki wbudowanej analizie obrazu będą w stanie wykryć niepożądane działania. Kamery Axis współpracują ze skanerami kodów kreskowych i zbliżeniowych, wykorzystując istniejące okablowanie strukturalne i zapewniając efektywną obserwację rozległych obszarów zarówno wewnątrz, jak i na zewnątrz budynków. Ale czy to wystarczy? Jak szybko można znaleźć daną przesyłkę wśród milionów zarejestrowanych? Czy można opracować system śledzenia konkretnego towaru wśród innych?

Przejrzysta i bezpieczna logistyka w każdym momencie

Aby opracować przejrzyste narzędzie, które umożliwi weryfikację każdego incydentu dotyczącego określonego towaru, należało zintegrować śledzenie i metody wyszukiwania z obrazem. Obecnie każdy system WMS (*Warehouse Management System*) i ERP (*Enterprise Resource Planning*) zbiera dane identyfikujące towary. Każdy system telemetryczny i zarządzania flotą nieustannie śledzi miejsce przebywania pojazdów. Łącząc nagrania ze śledzeniem i danymi przesyłki w jeden spójny system, otrzymujemy idealne rozwiązanie.
Dzięki systemowi wizyjnego śledzenia towarów firmy Axis i jej partnerów stan przesyłki znany jest na każdym etapie. Szybko można też uzyskać jego weryfikację na obrazie.
Rozwiązanie integruje systemy WMS i AIDC (*Automatic Identification and Data Capture*) z kamerami sieciowymi i systemem zarządzania obrazem, umożliwiając nadzór nad pełną procedurą obsługi przesyłek. Po wprowadzeniu numeru paczki można więc prześledzić obraz jej „wędrówki" w firmie. W razie skargi klienta lub wykrycia nieprawidłowości można poznać ich przyczyny i przedstawić je jako materiał dowodowy. W branży, w której codziennie składane są tysiące reklamacji, możliwość szybkiej weryfikacji jest dla operatora ogromną zaletą.

Internet Rzeczy w najdłuższym tunelu kolejowym świata

Otwarty w grudniu ub.r. Gotthard Base – najdłuższy tunel kolejowy na świecie – nie jest jedynie perłą myśli inżynierskiej. To również jeden z pierwszych poważnych projektów inżynieryjnych obejmujących wdrożenie zaawansowanej technologii Internetu Rzeczy (IoT).
Do całodobowego zarządzania bezpieczeństwem pasażerów i pociągów w jednym z najtrudniejszych środowisk operacyjnych wykorzystano sieć urządzeń IoT: czujniki, kamery telewizji dozorowej, system wentylacji, infrastrukturę odprowadzania wody, system łączności, sterowania i monitoringu.

Przez alpejski tunel Gotthard Base codziennie z prędkością 250 km/h przejeżdżają pociągi pasażerskie przewożące 9 tys. podróżnych oraz maks. 260 pociągów towarowych, których składy są znacznie dłuższe i cięższe niż przed laty.
Obszar tunelu powinien być obsługiwany przez wyjątkowo niezawodną sieć IP. Nawet minimalne zakłócenia łączności sieciowej spowodowane zbyt mało wydajnym transferem danych lub powstawaniem wąskich gardeł mogą potencjalnie spowodować opóźnienia, a nawet zagrozić bezpieczeństwu obsługi i pasażerów. Większość rozwiązań technicznych została zautomatyzowana. Pozwoliło to uzyskać wyjątkowo stabilną i niezawodną sieć niezbędną do przesyłania ważnych danych operacyjnych z i do tunelu. Środowisko IoT jest oparte na komunikacji w czasie rzeczywistym między urządzeniami IP – „rzeczami" – w celu natychmiastowego gromadzenia danych operacyjnych i zapewnienia personelowi obsługi informacji potrzebnych do bezproblemowego i bezpiecznego działania wszystkich systemów w obrębie tunelu.
Jednym z przykładów mogą być drzwi. Jeśli jakiekolwiek prowadzące do obszarów serwisowych lub tuneli dostępu pozostałyby otwarte, ciśnienie spowodowane przemieszczaniem się ultraszybkiego pociągu pasażerskiego wywołałoby znaczne uszkodzenia mechaniczne systemów w obrębie tunelu, dlatego wszystkie drzwi w tunelu działające w ramach IoT są monitorowane przez całą dobę. W przypadku nieodpowiednio zabezpieczonych do sterowni są wysyłane automatyczne powiadomienia.

Tunel Gotthard wymaga zastosowania wzmocnionej sieci złożonej z odpornych elementów, zapewniającej niezawodną i bezpieczną komunikację.

Jeśli weźmiemy pod uwagę wysyłanie i odbieranie danych w czasie rzeczywistym przez czujniki, kamery systemu wizyjnego, system wentylacji, infrastrukturę odprowadzania wody, system łączności, sterowania i monitoringu w całym obiekcie, wiadomo już, dlaczego systemy niezawodnej łączności są tak ważne.
W dwóch równoległych tunelach funkcjonują dwie osobne, niezależne sieci łączące wszystkie punkty końcowe IoT i wykorzystane do przesyłania informacji do operatorów centrów sterowania tuneli. Sieci te muszą być niezawodne i przystosowane do pracy przez całą dobę w dużym zakresie temperatury i we wszystkich rodzajach środowisk operacyjnych. Oznacza to konieczność wykorzystania przełączników różniących się od powszechnie stosowanych – przeznaczonych do pracy w najbardziej wymagających środowiskach o nieprzerwanym ruchu i gwarantujących bezbłędną komunikację.

Specjalna wzmocniona sieć i urządzenia klasy przemysłowej umożliwiają wdrożenie w tunelu Gotthard urządzeń IoT.

Wiele komponentów sieci musi pracować w tunelu przez dłuższy czas, z dala od bezpiecznych centrów przetwarzania danych, gdzie warunki pracy znajdują się pod stałą kontrolą. W niektórych obszarach w tunelu temperatura może sięgać 40°C przy wilgotności względnej dochodzącej do 70 proc., co oznacza duże przekroczenie norm w porównaniu ze zwykłymi, domowymi środowiskami pracy przełączników.
Sporym problemem jest też pył metalowy. Nawet w biurowych warunkach pracy urządzeń zapylenie jest problemem, ale wewnątrz tunelu kolejowego może ono powodować poważne awarie elementów sieci, hamulce pociągów bowiem nieustannie wyrzucają w powietrze pył metalowy. Ponadto zakłócenia elektromagnetyczne i wibracje spowodowane codziennymi czynnościami poważnie ograniczają okres sprawności standardowych przełączników i powodują ich uszkodzenia mechaniczne.
Tunel Gotthard został wyposażony w sieć wzmocnioną. Po pierwsze użyto przełączników, punktów dostępowych i routerów, które standardowo obsługują zintegrowane systemy zabezpieczeń, dynamiczne dostosowywanie wydajności sieci w celu wdrażania aplikacji w czasie rzeczywistym oraz niezawodną komunikację szerokopasmową IP.
Po drugie wykorzystano sprzęt sieciowy w obudowach klasy przemysłowej.
Zadanie opracowania i wdrożenia sieci do przesyłania danych zostało powierzone inżynierom z firmy Alpiq InTec, który użyli ponad 450 wzmocnionych przełączników LAN OmniSwitch® 6855 firmy Alcatel-Lucent do budowy szkieletu sieci do przesyłania danych pracującej w obrębie tunelu.
Minimum obsługi prewencyjnej i napraw jest niezwykle istotną kwestią podczas instalowania sieci nawet 2,3 km w głąb skały. Przełączniki te wykorzystują system chłodzenia konwekcyjnego opartego na radiatorach, a nie na wentylatorach, redukując zagrożenie związane z zanieczyszczeniem cząsteczkami metalu i uszkodzeniem wewnętrznych elementów elektronicznych.

Głos branży

Zabezpieczenia techniczne stosowane w sektorze transportu i logistyki to dla rynku security duże wyzwanie. Wymagają rozwiązań specjalizowanych, które z jednej strony muszą zapewnić bezpieczeństwo pasażerów i pracowników, z drugiej – nie mogą obniżać komfortu ich podróżowania i pracy. Dodatkowym utrudnieniem jest wzrost zagrożenia terrorystycznego, które dało już o sobie znać w krajach Europy Zachodniej.

Piotr Świder,
Key Account Manager, Hikvision Poland

Hikvision: rozwiązania sprawdzone, kompleksowe i łatwe w integracji

Infrastruktura transportowa jest klasyfikowana jako część tzw. infrastruktury krytycznej, czyli mającej podstawowe znaczenie dla funkcjonowania państwa i społeczeństwa. Dlatego rozwiązania zapewniające bezpieczeństwo pasażerów muszą być sprawdzone, kompleksowe i łatwe w integracji.

Tego typu projektom stawia się wiele wymagań, przy czym każdy z nich ma specyficzne uwarunkowania i normy określone w oficjalnych dokumentach. Dla przykładu norma EN50155 jest wymagana właściwie tylko w kolejnictwie. Niezbędna jest integracja, by system, składający się z mniejszych podsystemów, mógł spełniać swoje podstawowe zadanie, czyli zagwarantowanie bezpieczeństwa podróżnym.

Kluczowym elementem jest koordynacja pracy systemów zabezpieczeń z działaniami operatorów w centrach monitoringu. Detekcja zdarzenia i alarm są ważne, lecz najważniejsza jest umiejętna i właściwa reakcja operatora. Coraz częściej systemy zabezpieczeń pełnią funkcję prewencyjną, a więc ostrzegają przed zagrożeniem, np. nasze kamery mają algorytmy automatycznej detekcji pozostawionego obiektu na lotnisku, wkroczenia w zakazaną strefę czy przekroczenia linii na peronie kolejowym.

Tego typu infrastruktura wymaga systemów dedykowanych. Obserwując sytuację na świecie, inwestorzy powinni kierować się kryterium niezawodności, jakości i dostępności opcji (zaawansowana analityka *Hikvision Smart Solutions* czy system rozpoznawania tablic rejestracyjnych, który można powiązać z uprawnieniami do wjazdu w określone strefy). Rynek dozoru wizyjnego dla transportu będzie się rozwijał w kierunku zastosowania kamer o coraz wyższych rozdzielczościach, a zarejestrowany materiał będzie poddawany zaawansowanej analizie wideo. Przewidujemy również coraz szersze zastosowanie kamer termowizyjnych w obiektach infrastruktury transportowej, np. w portach lotniczych, gdzie tradycyjne kamery dozorowe mogą okazać się niewystarczające.

Sądzimy, że w Polsce rozpoczną się spore inwestycje w tzw. inteligentne systemy transportowe w średnich i małych miastach. Autobusy, wagony kolejowe, tramwaje będą wyposażane w wysokiej klasy systemy monitoringu wizyjnego. Bezpieczeństwo pasażerów to dla branży duże wyzwanie, dlatego Hikvision priorytetowo traktuje ten segment rynku.

Andrzej Oliński,
dyrektor Pionu Klientów Kluczowych, T4B

T4B poprawia bezpieczeństwo na dworcach kolejowych

Obecnie użytkowane systemy zabezpieczeń w środkach transportu publicznego składają się z wielu kamer, czujników i elementów peryferyjnych, stąd też ilość informacji docierających do operatorów jest bardzo duża. W związku z tym ważna jest możliwie szeroka integracja różnych systemów w jeden spójny nadrzędny system zarządzający. Jego rolą ma być nie tylko wizualizacja stanu poszczególnych elementów i zarządzanie nimi z jednego poziomu, ale także wspomaganie pracowników ochrony. Szczególnie istotne, aby alarmy docierające do osób odpowiedzialnych za bezpieczeństwo były wstępnie filtrowane, automatycznie potwierdzane i weryfikowane przez system. W przypadku kilku tysięcy kamer, a tyle docelowo może być zainstalowanych w całym systemie, odpowiednio zaprogramowana analityka wideo stanowi podstawę prawidłowo działającego systemu bezpieczeństwa. W pewnym stopniu zastępuje ona operatorów, stanowiąc jednocześnie nieocenioną pomoc w dostrzeganiu zagrożeń.

Rozległe systemy bezpieczeństwa będą się rozwijać w kierunku jednolitych systemów zarządzania, zasilanych ogromną ilością informacji z systemów podległych, szczególnie obrazami wideo z analizą ich treści. Informacje te w połączeniu z wprowadzonymi do systemu automatycznymi procedurami zarządzania kryzysowego migrują w stronę sztucznej inteligencji. Może ona zautomatyzować pracę pracowników ochrony, ale trzeba pamiętać, że zarządzanie i podejmowanie ostatecznych decyzji należy do odpowiednich służb.

W 2015 r. PKP SA zleciła firmie T4B zaprojektowanie i zbudowanie jednego z najnowocześniejszych systemów bezpieczeństwa publicznego w Europie.

PSIM *(Physical Security Information Management)* został wykonany i wdrożony na najważniejszych dworcach kolejowych zarządzanych przez PKP SA. Celem była poprawa bezpieczeństwa podróżnych i użytkowników dworców.

System jest narzędziem innowacyjnym, umożliwiającym przetwarzanie i gromadzenie zebranych informacji według ściśle określonych procedur. Zainstalowano wysokiej klasy kamery dozorowe oraz wiele nowoczesnych urządzeń, które zintegrowano z tymi już istniejącymi.

Mikołaj Tukalski, zastępca dyrektora Biura Inwestycji PKP SA, zapewnił, że spółka stawia na ciągłą modernizację systemów, aby zapewnić bezpieczne korzystanie z dworców.

Maciej Pietrzak,
Sales Support Engineer, Dahua Technology Poland

Dahua podkreśla specyficzne wymagania

Rośnie zainteresowanie systemami zabezpieczeń przeznaczonymi do środków komunikacji publicznej. W prywatnych przedsiębiorstwach natomiast dominuje zainteresowanie systemami umożliwiającymi nadzorowanie floty pojazdów służbowych.

Każdy ze środków transportu publicznego, takich jak linie autobusowe czy kolej, stawia przed projektantem specyficzne wymagania, różne są też kryteria doboru urządzeń security w nich instalowanych. Kamery wewnętrzne, których zadaniem jest umożliwienie obserwacji tego, co dzieje się w pojazdach i ich najbliższym otoczeniu, muszą spełniać wymogi zawarte w normach. EN 50155:2007 wymaga m.in., by ich obudowy były bezpieczne dla pasażerów (nie miały ostrych krawędzi) oraz odporne na uszkodzenia. Wymogi dotyczące odporności na zakłócenia elektromagnetyczne i wstrząsy oraz sposobu połączeń urządzeń w systemie (zwykle złącze M12) są określone w normie EN 50121-4:2015.

Wysokie wymagania dotyczą również zastosowanych urządzeń rejestrujących. Powinny one mieć zwartą budowę odporną na uszkodzenia mechaniczne czy wstrząsy, i nie posiadać żadnych elementów ruchomych. Nie stosuje się w nich wentylatorów, ale chłodzenie pasywne, a dane zapisuje na dyskach SSD. Ponadto wyposaża się je w elementy antywibracyjne amortyzujące ciągłe drgania.

Rejestratory powinny zapewniać szybką wymianę nośnika danych, ale tylko osobie upoważnionej. Oprócz rejestracji obrazu i dźwięku rejestrator powinien umożliwiać transmisję danych, by móc zdalnie komunikować się z urządzeniem.

Jestem przekonany że w świetle ostatnich wydarzeń coraz więcej firm z branży transportowej zacznie stosować systemy do nadzoru pojazdów. Nie tylko, aby kontrolować kierowców, ale również zapewniać im bezpieczeństwo.

W środkach transportu systemy dozoru wizyjnego są już standardem. Właściciele prywatnych pojazdów również coraz częściej decydują się na montaż kamer wideo. Nie mam wątpliwości, że jednym z głównych kierunków rozwoju branży zabezpieczeń w najbliższym czasie będzie transport i komunikacja.

Axis o zabezpieczeniach kolei

Jan T. Grusznic
Sales Engineer,
Axis Communications

Obiekty obsługujące ruch pasażerski muszą spełniać surowe kryteria dotyczące ochrony i bezpieczeństwa. System monitoringu na dworcach, stacjach i przystankach kolejowych wspiera działania Straży Ochrony Kolei w zapewnieniu bezpieczeństwa pasażerów, pracowników, towarów, infrastruktury i majątku trwałego przed możliwymi zagrożeniami, tj. wandalizmem, kradzieżami, handlem substancjami zakazanymi, pożarami czy terroryzmem. Stawienie im czoła to poważne wyzwanie ze względu na różnorodność obszarów podlegających dozorowi: linie kolejowe, perony, przejścia podziemne, parkingi, budynki, przechowalnie bagażu czy pociągi w czasie postoju.

Współpraca z UITP (Międzynarodowe Stowarzyszenie Transportu Publicznego) pozwoliła nam lepiej zrozumieć potrzeby rynku transportu zbiorowego. Zaowocowała opracowaniem wysokorozdzielczych kamer wieloprzetwornikowych spełniających wymagania emisji i odporności na zakłócenia urządzeń sygnalizacji i telekomunikacji w środowisku kolejowym. Duże ograniczenia przepustowości w paśmie transmisyjnym rozwiązaliśmy, wprowadzając do istniejącego zaawansowanego multistrumieniowania (tzw. Zipstream), smart koder zgodny ze standardem H.264, który pozwala na zmniejszenie zajętości pasma w okresie niewielkiego ruchu.

W perspektywie nadchodzących inwestycji i budowy rozległego geograficznie systemu zabezpieczeń (w tym dozoru wizyjnego) w obiektach infrastruktury transportu zbiorowego najistotniejsze pozostają trzy wymagania: otwartość oparta na standardach rynkowych, bezpieczeństwo wymiany informacji i bezawaryjność stosowanych urządzeń. Stanowią one gwarancję dalszej rozbudowy systemu i utrzymania ciągłości działania całego systemu.

Istotne staną się również możliwości wymiany informacji między samymi urządzeniami w obrębie ustandaryzowanych protokołów komunikacyjnych i skuteczniejsze przetwarzanie w urządzeniach końcowych.

Wiele dotychczasowych wdrożeń z wykorzystaniem technologii Axis znacząco przyczyniło się do zwiększenia poczucia komfortu oraz bezpieczeństwa użytkowników i pracowników w publicznym transporcie zbiorowym. Kamery, jako element prewencyjny, skutecznie zapobiegły wielu wypadkom, aktom agresji i próbom kradzieży.

Wysoka jakość i użyteczny obraz wpłynęły też na zwiększenie wykrywalności zdarzeń oraz identyfikację sprawców dewastacji i wybryków chuligańskich. Wykorzystywana w kamerach analiza obrazu i dźwięku powiadamia np. o tłumie, agresywnych okrzykach czy obecności na torach lub krawędzi peronu, przyspieszając moment interwencji. Rewelacyjnie sprawdza się Axis Corridor Format ze względu na obserwację przestrzeni wąskich i zarazem długich. Ta technologia dostarcza obraz w układzie pionowym bez strat w poklatkowości i rozdzielczości, co przekłada się również na mniejszą liczbę kamer przypadającą na obszar.

Nodex: integracja i bezpieczeństwo pożarowe

Janusz Sawicki
Instytut Bezpieczeństwa Pożarowego NODEX

Przy obecnym rozwoju technicznych zabezpieczeń przeciwpożarowych – począwszy od systemów wczesnej detekcji pożaru i związanych z nimi urządzeń pozwalających ograniczyć oddziaływanie pożaru, jego tłumienie i zapewniających bezpieczne warunki ewakuacji i działanie jednostek ratowniczo-gaśniczych – nie ma większych problemów z doborem odpowiednich systemów do obiektów budowlanych infrastruktury związanej z transportem. Dotyczy to obiektów użyteczności publicznej (dworce, terminale lotnicze) oraz budynków kategorii przemysłowo-magazynowej, tzw. PM. Stosowanie odpowiednich technicznych środków zabezpieczeń zależy od gęstości obciążenia ogniowego, liczby osób w nich przebywających i parametrów architektonicznych. Wymagania dla tego typu obiektów są zawarte w przepisach techniczno-budowlanych, wytycznych projektowania, specyfikacjach technicznych i szczególnych wymaganiach resortu transportu. Osobnym zagadnieniem jest zabezpieczenie przeciwpożarowe ruchomych jednostek transportowych, szynowych, drogowych i powietrznych.

Rozwiązania zapewniające bezpieczeństwo użytkowników tych obiektów powinny charakteryzować się przede wszystkim wysoką niezawodnością działania w całym okresie ich eksploatacji, powinny one także mieć możliwość współpracy, czyli odpowiedni poziom kompatybilności, co pozwoli spełnić wymagania scenariusza pożarowego.

Systemy i rozwiązania techniczne instalowane w obiektach budowlanych i instalacjach technologicznych stanowią 50 proc. całego systemu odpowiedzialnego za ich bezpieczeństwo pożarowe. Drugie 50 proc. stanowi odpowiednio przeszkolony personel, tzn. taki, który potrafi podejmować właściwe decyzje w czasie rzeczywistym w sytuacji kryzysowej w obiekcie.

Personel i jednostki ratowniczo-gaśnicze podejmują decyzje na podstawie informacji przekazywanych przez techniczne instalacje ppoż. i inne za pośrednictwem tzw. urządzeń integrujących. Urządzenia integrujące pozwalają na ciągły nadzór instalacji przeciwpożarowych, poprawny odczyt komunikatów wspierany przez zaprogramowane w integratorach procedury, a także na ręczne sterowanie urządzeniami przeciwpożarowymi. Aby uzyskać wymagany poziom integracji, a tym samym – naszym zdaniem – wysoki poziom bezpieczeństwa pożarowego, należy szczególnie starannie w procesie planowania inwestycji dokonywać wyboru odpowiednich urządzeń pod kątem ich możliwości zintegrowania i uzyskiwania od nich odpowiedniej jakości komunikatów.

Ważnym ogniwem systemu bezpieczeństwa są również operatorzy, którzy powinni mieć wiedzę, a także predyspozycje do podejmowania decyzji. Instytut Bezpieczeństwa Pożarowego Nodex prowadzi działania szkoleniowe w zakresie bezpieczeństwa pożarowego w obszarach rozwiązań technicznych i szkolenia personelu odpowiedzialnego za bezpieczeństwo pożarowe powierzonych im obiektów budowlanych.

W procesie planowania inwestycji i modernizacji obiektów ważny jest dobór urządzeń i systemów przeciwpożarowych pozwalających na ich integrację i współdziałanie, by nie wpływały negatywnie na funkcjonowanie innych urządzeń w całym systemie. Należy też wziąć pod uwagę specyfikę obiektu, zidentyfikować zagrożenia i dobrać odpowiednie systemy przeciwpożarowe.

Linc Polska: nowoczesna ochrona strefy perymetrycznej

Jakub Sobek
certyfikowany trener,
Linc Polska

W marcu ub.r. dwóch zamachowców-samobójców zdetonowało ładunki wybuchowe na lotnisku Zaventem w Brukseli. Trzeci wysadził się w wagonie metra. W wyniku tych działań zginęły 32 osoby, a 340 zostało rannych. Trzy miesiące później w porcie lotniczym w Stambule doszło do kolejnego zamachu z udziałem trzech samobójców, którzy wysadzili się w trzech różnych miejscach lotniska. Tym razem bilans ofiar był jeszcze większy – 48 osób zginęło, a co najmniej 239 zostało rannych. Wydarzenia te pokazują, jak dużym wyzwaniem jest i będzie w przyszłości ochrona lotnisk i obiektów logistycznych. Nic nie wskazuje na to, że zagrożenia związane z atakami terrorystycznymi będą z czasem maleć. Pojawiają się także nowe zagrożenia, które będą zyskiwać na sile, takie jak loty dronów w pobliżu lotnisk lub w ich obrębie.

Wszystko to wymusza ciągłe inwestycje związane z podnoszeniem poziomu bezpieczeństwa takich obiektów. Rosnąca z roku na rok liczba pasażerów na lotniskach stanowi kolejne wyzwanie. Ochrona musi zawsze balansować pomiędzy komfortem osób podróżujących a ich bezpieczeństwem. Chodzi przecież o stosowanie takich technologii i rozwiązań technicznych, które nie będą miały dla pasażerów charakteru opresyjnego, stresującego lub w pewnym sensie zastraszającego. Wpływałoby to negatywnie na wizerunek lotnisk, a tym samym powodowałoby straty w ich działalności.

Planowanie każdego elementu systemu bezpieczeństwa w obiektach transportowych i logistycznych powinno być poprzedzone analizą ryzyka dla danego kraju i konkretnego lotniska oraz weryfikacją obecnej infrastruktury technicznej.

Od strony zabezpieczeń technicznych w obiektach logistycznych duży nacisk kładzie się obecnie na prawidłową ochronę strefy perymetrycznej. Standardem już jest wykorzystywanie do tego celu kamer termowizyjnych. Ten trend w kolejnych latach na pewno się utrzyma i będą one stosowane coraz częściej. Mają na to wpływ duża ich skuteczność, ciągły spadek cen oraz coraz lepsza jakość obrazu. Ponadto coraz doskonalsze algorytmy analizy wideo współpracują znacznie skuteczniej z kamerami termowizyjnymi niż z tradycyjnymi.

Zastosowanie kamer termowizyjnych pozwala także zmniejszyć liczbę urządzeń potrzebnych w strefie perymetrycznej, ponieważ ich zasięg jest znacznie większy niż kamer światła widzialnego. Wpływa to na obniżenie kosztów instalacji całego systemu, a co najważniejsze – do systemu trafia mniej sygnałów wizyjnych. Trzeba pamiętać, że zasoby ludzkie przeznaczane do obsługi centrów monitoringu są ograniczone. Ma to związek ze wzrostem kosztów zatrudnienia. Dlatego istotne jest ograniczanie liczby sygnałów wizyjnych i wspieranie operatorów przez coraz lepsze algorytmy do analizy wideo.

Ze względu na zagrożenia spowodowane dronami na lotniskach coraz częściej w systemach ochrony będą pojawiać się rozwiązania bazujące na radarach. Wykrywają one nawet niewielkie pojazdy z odległości kilku kilometrów, co pozwala na podjęcie właściwych działań z odpowiednim wyprzedzeniem.

Oprócz rozwiązań technicznych jednym z najistotniejszych czynników podnoszących bezpieczeństwo np. na lotniskach jest przeszkolony personel, który zwraca uwagę na nietypowe zachowania pasażerów lub pozostawione przedmioty.

Dla inwestorów i menedżerów odpowiedzialnych za bezpieczeństwo obiektów logistycznych i transportowych istotne są też specjalistyczne szkolenia. Nie chodzi o komercyjne prezentacje produktów, ale o szkolenia techniczne pozwalające lepiej zrozumieć, jak działają współcześnie wykorzystywane technologie i na co zwracać uwagę, decydując się na konkretne rozwiązanie. Na rynku polskim takie szkolenia świadczy m.in. Polska Izba Systemów Alarmowych, w której za program zajęć odpowiadają merytorycznie przygotowani wykładowcy. Ponieważ współczesne technologie rozwijają się szybko, uczestnictwo w tego typu szkoleniach jest szczególnie ważne.

Wszystkie autobusy i tramwaje zostaną wyposażone w kamery

– mówi **Michał Domaradzki, pełnomocnik prezydent Warszawy ds. bezpieczeństwa w publicznym transporcie zbiorowym**

Czym zajmuje się pełnomocnik Warszawy do spraw bezpieczeństwa w publicznym transporcie zbiorowym? To nowe stanowisko w stołecznym ratuszu...
Pełnomocnikiem pani prezydent jestem od 11 maja 2016 r. Moim zadaniem jest planowanie oraz koordynowanie działań związanych z bezpieczeństwem w komunikacji, współpraca z biurami i jednostkami urzędu miasta w zakresie bieżących potrzeb oraz planowanych rozwiązań w obszarze bezpieczeństwa w publicznym transporcie zbiorowym. Ponadto planuję i koordynuję działania w zakresie bezpieczeństwa spółek: Metro Warszawskie, Miejskie Zakłady Autobusowe, Tramwaje Warszawskie, Szybka Kolej Miejska, a także pozostałych operatorów publicznego transportu zbiorowego.

Michał Domaradzki
pełnomocnik prezydent Warszawy do spraw bezpieczeństwa w publicznym transporcie zbiorowym

Czy pół roku wystarczyło na zapoznanie się z bezpieczeństwem transportu miejskiego w Warszawie? Jakie działania planuje Pan w najbliższym czasie?
Rozpocząłem od przeglądu procedur bezpieczeństwa we wszystkich spółkach transportowych aglomeracji warszawskiej. W wielu obszarach próbujemy je ujednolicać, tak aby odpowiednim poziomem bezpieczeństwa otoczyć pasażerów zarówno autobusów, tramwajów, jak i metra. Pomocnym do tego narzędziem jest monitoring wizyjny, który jest ciągle uzupełniany. Chcemy, by docelowo w te rozwiązania został wyposażony każdy pojazd. A mówimy tu o ogromnej skali, bo w jednym momencie po warszawskich ulicach jeździ około 1,5 tys. autobusów i ponad 400 tramwajów. Czeka nas więc olbrzymie przedsięwzięcie. Obecnie monitoringiem jest objętych około 70% liczby autobusów i 40% tramwajów. Zarekomendowałem Tramwajom Warszawskim, aby każdy pojazd został wyposażony w kamery, i te prace w tym momencie trwają. Trudno jednak inwestować w pojazdy, które niedługo będą wycofywane z ruchu. Inwestycje w system monitoringu będą więc prowadzone równolegle z inwestycjami w nowy tabor. Na pewno jednak wszystkie nowe tramwaje oraz te, przed którymi jeszcze długi czas eksploatacji, zostaną wyposażone w systemy dozoru wizyjnego. Ten projekt jest rozpisany na dłuższy okres. Inwestycję szacujemy na kilkanaście milionów złotych.

> W specyfikacji do nowych umów z przewoźnikami wprowadzono wymóg prowadzenia monitoringu wizyjnego online.

> Inwestycje w monitoring będą prowadzone równolegle z inwestycjami w nowy tabor tramwajowy. Ten projekt rozpisano na długo, a jego budżet to kilkanaście milionów złotych.

Jak przedstawia się kwestia monitoringu wizyjnego w warszawskich autobusach, których jeździ po ulicach znacznie więcej niż tramwajów?
Specyfiką warszawskiego taboru autobusowego jest to, że około 30% z nich to pojazdy przewoźników prywatnych, z którymi miasto podpisało umowę. Wszystkie nowe autobusy, które są wprowadzane do ruchu, muszą być wyposażone w systemy monitoringu – to jedno z naszych wymagań. Chcemy, aby w nowych pojazdach zostały zainstalowane również alcolocki, czyli techniczne urządzenia do badania stanu trzeźwości kierowcy, odcinające zapłon w razie konieczności.
Niedawno podjęliśmy decyzję, by w specyfikacji do nowych umów znalazło się wymaganie o prowadzeniu monitoringu wizyjnego online – obraz ma być przesyłany w czasie rzeczywistym do dyżurnego ruchu. Od 1 grudnia 2016 r. na ulice wyjechało 50 nowych autobusów jednej z prywatnych spółek, firmy Arriva, które zostały już wyposażone w taki system dozoru wizyjnego z podglądem online. Jeżeli to rozwiązanie się sprawdzi, będziemy zawierać te wymagania w każdej kolejnej umowie z operatorem.

Gdzie znajduje się centrum monitoringu wizyjnego warszawskiej komunikacji miejskiej?
Podgląd online ma dyżurny ruchu w Zarządzie Transportu Miejskiego, który koordynuje funkcjonowanie całej komunikacji w stolicy. W razie wystąpienia incydentu to on pierwszy reaguje, decyduje o uruchomieniu pojazdu zastępczego czy zorganizowaniu objazdu lub skierowaniu sprawy do Miejskiego Centrum Zarządzania Kryzysowego, gdzie współpracują ze sobą przedstawiciele policji, straży pożarnej czy właśnie ZTM.

Jak wygląda stan zabezpieczeń w metrze, które zapewne jest szczególnie narażone na różne zagrożenia?
Tu sytuacja rzeczywiście wygląda inaczej. To stosunkowo nowy przewoźnik, ma więc tę przewagę, że już korzysta z najnowocześniejszych rozwiązań. W metrze działa obecnie prawie 1100 kamer i jest to obszar bardzo dobrze zabezpieczony. Na każdej stacji pracuje dyżurny, który ogląda obrazy z tych kamer. Ponadto druga linia metra została wyposażona w system wykrywający zbliżanie się pasażera do krawędzi peronu. Dyżurny stacji natychmiast zostaje poinformowany o takim wydarzeniu, a z głośników jest nadawany komunikat głosowy z ostrzeżeniem o niebezpieczeństwie.
Mogę bez wahania powiedzieć, że metro należy do najbezpieczniejszych miejsc w Warszawie. Statystyki wykazują tu niewiele zdarzeń o charakterze przestępczym, co jest zapewne efektem działania z jednej strony kompleksowego systemu monitoringu wizyjnego, z drugiej – dobrze zorganizowanej pracy Służby Ochrony Metra.

Czy w warszawskim metrze, podobnie jak w Paryżu czy Moskwie, podejmuje się temat instalowania bramek znanych np. z portów lotniczych?
Na razie nie mam informacji o takich planach, natomiast metro ściśle współpracuje ze służbami, które na bieżąco prowadzą analizę i określają poziom ryzyka. Nie wykluczam, że jeśli te służby przekażą nam informację, że ryzyko realnie wzrasta, weźmiemy pod uwagę skorzystanie z takich zabezpieczeń technicznych.

Jak układa się współpraca miasta z policją?
Podpisaliśmyporozumienie z Komendą Stołeczną Policji, na którego mocy m.in. udostępniamy nagrania z naszych kamer czy dane pozwalające na wypracowanie najlepszych procedur reagowania na zagrożenia terrorystyczne. Często też przekazujemy wycofywane z ruchu autobusy czy tramwaje, by policyjni antyterroryści mogli je wykorzystywać podczas ćwiczeń.

Dziękuję za rozmowę.
Rozmawiał **Mariusz Kucharski**

O wymaganiach w zakresie zabezpieczenia pojazdów szynowych

– opowiada **Marcin Pikul z firmy PESA Bydgoszcz**

Marcin Pikul
PESA Bydgoszcz

szef Zespołu ds. Zarządzania Projektami LRV, Dział Badań i Rozwoju, PESA Bydgoszcz

Jakie zabezpieczenia techniczne stosuje się obecnie w pojazdach szynowych?
Poziom zabezpieczenia pojazdów szynowych różni się w zależności od typu danego pojazdu. Dzisiaj najlepiej zabezpieczone jest metro – i jest to trend ogólnoświatowy. W tym przypadku systemy elektroniczne wykorzystuje się do monitorowania zagrożeń we wszystkich obszarach eksploatacji. Priorytetem jest zagwarantowanie bezpieczeństwa pasażerom w automatycznym ruchu pojazdów w systemie UTO (*Unattended Train Operation*). Kolejnymi typami pojazdów pod względem zaawansowania systemów zabezpieczeń są pociągi elektryczne (EMU), pociągi spalinowe (DMU), tramwaje, wagony pasażerskie i lokomotywy.

Jakie różnice w wymaganiach dotyczących zabezpieczeń pojazdów szynowych dostrzega Pan na rynkach zagranicznych?
Każdy kraj ma specyficzne wymagania. W sektorze kolejowym w Europie są one częściowo regulowane przepisami interoperacyjności TSI dotyczącymi zdolności systemu kolei do zapewnienia bezpiecznego i nieprzerwanego przejazdu pociągów. Poziom zaawansowania systemów jest jednak różny i w dużej mierze zależy od infrastruktury, w której pojazdy są eksploatowane.
W sektorze lekkich pojazdów szynowych natomiast występują znacznie większe różnice w zakresie zaawansowania instalowanych systemów zabezpieczeń. Wynika to w głównej mierze z tego, że poszczególne państwa zazwyczaj nie normalizują wymagań dotyczących tramwajów poruszających się w wydzielonej infrastrukturze danego miasta.

Czy wymagania obowiązujące na polskim rynku znacząco odbiegają od zagranicznych?
Wymagania obowiązujące w Polsce w zakresie pojazdów kolejowych są zgodne z wymaganiami europejskimi TSI. Natomiast przepisy dotyczące tramwajów definiują systemy bezpieczeństwa jedynie w bardzo wąskim zakresie – w zasadzie tylko podstawowe bezpieczeństwo ruchu pojazdów w warunkach miejskich. W Polsce nie ma określonych wymagań dla systemów przeciwpożarowych, antykolizyjnych czy monitoringu wizyjnego. Każdy klient dostosowuje je do swoich potrzeb.

Czy wszystkie pojazdy są wyposażane w kamery dozorowe?
Rzeczywiście, obecnie wszyscy zamawiający zgłaszają zapotrzebowanie na systemy monitoringu wizyjnego wraz z zapisem danych. Jeśli zaś chodzi o szczegółowe specyfikacje, to poszczególni klienci przedstawiają nam swoje konkretne wymagania.

Jak przedstawia się sytuacja w odniesieniu do czujek dymu?
Jeśli chodzi o tę kwestię, to nie wszystkie pojazdy są wyposażane w czujki dymu. W tym przypadku zależy to od wymagań klienta. W niektórych pojazdach natomiast są instalowane systemy gaszenia pożarów, szczególnie w sektorze DMU (*Diesel Multiple Units*).

Czy urządzenia i systemy zabezpieczeń technicznych są dobierane przez producenta pojazdów, czy jednak są to elementy instalowane według specyfikacji zamawiającego?
Specyfikacja zamawiającego dotyczy konkretnej serii pojazdów. Jeżeli zamawiający zgłasza dodatkowe wymagania w tym zakresie, to wtedy wszystkie pojazdy wymienione w danym zamówieniu, czyli serii, zostają wyposażone w odpowiednie systemy. Jeśli natomiast chodzi o branżę kolejową, to tutaj pojęcie produkcji seryjnej w rozumieniu *automotive* praktycznie nie istnieje. W tym przypadku serie liczą od jednego do maksymalnie kilkuset pojazdów.

Czy zdarza się, że klient zamawia pojazdy bez urządzeń i systemów zabezpieczeń technicznych, a wyposaża je we własnym zakresie?
Samodzielne doposażenie pojazdów przez zamawiającego w okresie gwarancji jest niedozwolone. I zawsze to podkreślamy. W przypadku zakupu nowych pojazdów klient definiuje swoje wymagania przed etapem projektowania i produkcji. Doposażeniu podlegają jedynie „stare" pojazdy eksploatowane już przez klienta. Ewentualne doposażenie pojazdów w systemy zabezpieczeń w pierwszych latach eksploatacji może wynikać ze zmiany infrastruktury, w której pojazd jest eksploatowany. Dzieje się tak na przykład, gdy pojawiają się plany wykorzystania pojazdu do obsługi krajowych i zagranicznych połączeń kolejowych.

Dziękuję za rozmowę.
Rozmawiał **Mariusz Kucharski**

PESA Bydgoszcz otrzymała jedno z najważniejszych na świecie wyróżnień w dziedzinie wzornictwa przemysłowego **iF DESIGN AWARD 2016**. Nagrodzonym produktem został PesaDART – pojazd wyprodukowany dla PKP Intercity.

PESA Bydgoszcz SA to największy polski producent pojazdów szynowych na potrzeby transportu kolejowego (lokomotywy, zespoły trakcyjne, wagony) i miejskiego (tramwaje). Firma świadczy także usługi w zakresie modernizacji, napraw i przeglądów taboru.

Bezpieczeństwo na lotniskach

Tam nie polecę, tam nie jest bezpiecznie **– takie stwierdzenie w ustach pasażera to dla każdego lotniska sygnał poważnych kłopotów.** Paryż, Bruksela, a ostatnio Stambuł są ofiarami niewidzialnej trucizny, jaką jest strach przed kolejnym zamachem terrorystycznym.

Już samo zagrożenie terrorystyczne, a tym bardziej krwawe zamachy, oprócz tragicznych skutków dla ludzi, niosą także natychmiastowe konsekwencje biznesowe znacznie wykraczające poza funkcjonowanie lotniska. Operujące tam linie lotnicze notują ogromne straty i są zmuszone do redukowania siatki połączeń, co zmniejsza atrakcyjność lotniska i – niczym kula śnieżna – powoduje dalsze straty. Spirala w kilka miesięcy ciągnie wszystko w dół. Jako przykład mogą posłużyć ostatnie decyzje Turkish Airlines, linii będącej dotychczas symbolem sukcesu i niebywałego rozwoju. Utrata 10 mln pasażerów rocznie spowodowała pierwsze od lat spadki dochodów, co wymusiło uziemienie trzydziestu samolotów. Pojawienie się takiego negatywnego trendu trwa zaledwie kilka miesięcy, jego odwrócenie natomiast zajmuje co najmniej kilka lat.

Czasy się zmieniły. Do przeszłości należą problemy z rozchwianą i nieprzewidywalną ceną paliwa. Dziś największym zagrożeniem dla branży lotniczej jest zapewnienie poczucia bezpieczeństwa.

Dotychczas prostą odpowiedzią lotnisk na nowe zagrożenie było wprowadzenie kolejnych kontroli. Schemat jest prosty: akcja – reakcja. Bomba została umieszczona w butach, więc wszystkim sprawdzamy buty, zagrożenie stanowią płyny, więc zabieramy płyny. To się jednak zmieniło. Przed nami zupełnie nowe wyzwanie: stale rosnący ruch pasażerski, określany w języku branży lotniczej „nieustającymi wyzwaniami operacyjnymi". Linie lotnicze dysponujące coraz większymi samolotami oczekują, że większa liczba pasażerów w tym samym czasie do samolotu wsiądzie i z niego wysiądzie, że szybko i sprawnie przesiądą się na kolejny rejs, a wraz z nimi tę samą drogę odbędzie ich bagaż. Prawdziwą plagą zagęszczonego nieba są bowiem opóźnienia. Jedynym zaś sposobem na ich wyraźne zmniejszenie jest sprawność operacji w porcie lotniczym. I tu tkwi **największe wyzwanie: zapewnić bezpieczeństwo, ale nie kosztem czasu podróży, a przede wszystkim nie kosztem dodatkowych utrudnień.**

Wiele ankiet przeprowadzonych wśród podróżnych potwierdza, że poziom akceptacji wymogów bezpieczeństwa się zwiększa, ale jednocześnie spada tolerancja dla ich uciążliwości. Nikt nie rozumie, że w dobie iPhone'a i postępujących innowacji kontrola osobista oznacza rozebranie się prawie „do rosołu" i dokonanie fizycznego przeszukania. Kontrola bagażu to nadal krępujące publiczne wyjmowanie rzeczy osobistych na oczach dziesiątków obcych ludzi. Do rangi symbolu urosła, nadal praktykowana w wielu portach lotniczych, konieczność skosztowania przez matkę jedzenia, które wnosi dla podróżującego z nią niemowlęcia, w celu wykluczenia w składzie materiałów wybuchowych… Te krępujące, ale i nieskuteczne metody otwierają ogromne zapotrzebowanie na kontrolę bezpieczeństwa opartą w coraz większym stopniu na technice i technologii.

Przyszłością zabezpieczeń na lotniskach są z pewnością urządzenia do bezdotykowej kontroli osobistej stosowane już w USA. Nie dość, że kontrola zajmuje kilka sekund, to jest skuteczniejsza i dla wielu osób mniej krępująca. Na podobnej zasadzie odbywa się już kontrola bagażu rejestrowanego i ładunków cargo. Trzeba podkreślić, że bagażu podróżującego po świecie jest statystycznie dwa razy więcej niż pasażerów, a do jego kontroli od dawna wykorzystuje się znacznie więcej techniki niż do kontroli osobistej pasażerów. Inaczej lotniska musiałyby zatrudniać nie kilka, ale kilkanaście tysięcy osób, a i tak nie każdy bagaż dotarłby na czas.

W zakresie bezpieczeństwa w branży lotniczej można zaobserwować pewien paradoks: rozważa się, czy pilota może zastąpić automat lub kontrolerzy lotniczy pilotujący samolot z ziemi. Nadal jednak są wątpliwości w kwestii zagwarantowania bezpieczeństwa na lotniskach przy użyciu technologii, które miałyby zastąpić człowieka. A to chyba jedyna słuszna droga.

Bezpieczeństwo na lotniskach nie będzie zapewnione bez masowego stosowania nowoczesnych technologii security.

BIO

Sebastian Mikosz
prezes eSKY.pl, dwukrotnie prezes PLL LOT,
autor książki *Leci z nami pilot. Kilka prawd o liniach lotniczych.*

Dworzec Łódź Fabryczna

Problemy z planowaniem tras kablowych przeznaczonych do technicznych urządzeń ppoż. w obiektach budowlanych.

Janusz Sawicki
Instytut Bezpieczeństwa Pożarowego Nodex

Bezpieczeństwo pożarowe obiektów jest wymaganiem podstawowym nr 2 dla obiektów budowlanych i ujęte tam tezy dotyczące obszarów bezpieczeństwa pożarowego powinny być bezwzględnie w tych obiektach spełnione.
Duży udział w zapewnieniu akceptowalnego poziomu bezpieczeństwa pożarowego mają techniczne urządzenia, systemy i instalacje przeciwpożarowe. Integralną częścią tych systemów i instalacji są trasy kablowe, za pomocą których są one zasilane, kontrolowane i sterowane.
Trasy kablowe wraz z urządzeniami nośnymi i zamocowaniami wg § 187, pkt 3 Warunków Technicznych[1] są określane zespołami kablowymi. Warunki techniczne definiują je następująco: „przewody i kable elektryczne oraz światłowodowe, zwane dalej **zespołami kablowymi**, stosowane w systemach zasilania i sterowania urządzeniami służącymi ochronie przeciwpożarowej, powinny zapewniać ciągłość dostawy energii elektrycznej lub przekazu sygnału przez czas wymagany do uruchomienia i działania urządzenia, z zastrzeżeniem ust. 7. Ocena zespołów kablowych w zakresie ciągłości dostawy energii elektrycznej lub przekazu sygnału, z uwzględnieniem podłoża i przewidywanego sposobu mocowania do niego, powinna być wykonana zgodnie z warunkami określonymi w Polskiej Normie[2] dotyczącej badania odporności ogniowej".

> Integralną częścią systemów i instalacji ppoż. są trasy kablowe, za pomocą których są one zasilane, kontrolowane i sterowane.

Z tego zapisu wynikają następujące wnioski:

1. Zespół kablowy składa się z kabli i przewodów oraz urządzeń nośnych, takich jak drabinki, koryt kablowych różnego rodzaju, uchwytów i innego rodzaju osprzętu mocującego o odpowiednich parametrach odporności ogniowej. Wszystkie te składowe są określone przez klasyfikację definiującą ich odporność na temperaturę pożaru. I tak przewody są klasyfikowane za pomocą właściwości dostarczania energii elektrycznej i sygnału w warunkach pożaru jako PH 15, 30, 60, 90, 120 dla kabli cienkich oraz P 15, 30, 60, 90 dla kabli grubych. Cały zespół kablowy i elementy nośne przyjęto oceniać zgodnie z normą DIN 4102-12 Zachowanie się materiałów i elementów budowlanych pod wpływem ognia. Część 12: *podtrzymanie funkcji elektrycznych linii kablowych. Wymagania i badania.* Są one klasyfikowane jako E 30, 60, 90.
2. Zespół kablowy należy zawsze oceniać, biorąc pod uwagę rodzaj podłoża, do którego będą mocowane w obiekcie.

O ile przesłanie pierwszego wniosku jest zrozumiałe, o tyle zapis wniosku drugiego może stanowić problem dla projektantów i wykonawców instalacji ppoż. Występuje on np. wtedy gdy obiekt budowlany ma klasę odporności ogniowej E, a ściany i elementy, do których mają być mocowane zespoły kablowe, są klasyfikowane jako EI 0.
Z praktyki Instytutu Bezpieczeństwa Pożarowego Nodex wynika, że urządzenia przeciwpożarowe, a więc również zespoły kablowe służące do zasilania tych urządzeń i sterowania nimi, są montowane w ostatnich etapach realizacji budowy obiektu, co jest zrozumiałe. Wydaje się natomiast błędem brak planowania tras kablowych w odniesieniu do urządzeń przeciwpożarowych w czasie tworzenia projektu architektonicznego. Ten błąd powoduje niewątpliwie zwiększenie kosztów i wydłużenie czasu inwestycji, a niekiedy uniemożliwia spełnienie wymagania podstawowego nr 2 zgodnie z obowiązującymi przepisami. W takich przypadkach są stosowane różne rozwiązania zamienne zwiększające zazwyczaj koszty instalacji przeciwpożarowych. To bardzo dziwna sytuacja chociażby dlatego, że planowanie tras kablowych bytowych instalacji elektrycznych i sanitarnych jest dokonywane już w procesie realizacji projektu budowlanego. Operaty budowlane i projekty architektoniczne przewidują co prawda instalowanie technicznych urządzeń ppoż., takich jak wentylatory oddymiające, klapy odcinające, centrale sterujące i inne, niestety nie ma w nich wymagań dotyczących zespołów kablowych, czyli zapewnienia odpowiedniego podłoża lub konstrukcji nośnych do mocowania tras kablowych, a także przebiegu zespołów kablowych w rzeczywistym obiekcie budowlanym.

> W procesie projektowym powinni uczestniczyć eksperci, którzy zaproponują rozwiązanie problemów w sposób właściwy i zgodny z przepisami.

Tego rodzaju problemy wystąpiły m.in. w trakcie realizacji tras kablowych w obiekcie Dworca Łódź Fabryczna. Spełnienie postulatów dotyczących wykonania przeciwpożarowych zespołów kablowych zgodnie z przepisami wymagało od wykonawców tych zespołów olbrzymiej inwencji i niemałych nakładów finansowych. Z pomocą IBP Nodex zadanie to zostało wykonane pomyślnie i obiekt został odebrany.
Znamienne są tutaj dwa przypadki wymagające rozwiązania problemów z przeciwpożarowymi trasami kablowymi: pierwszy to zespoły nośne w hali głównej służące do sterowania i zasilania instalacji oddymiania grawitacyjnego, drugi to sterowanie i zasilanie przeciwpożarowych klap odcinających otwierających otwory oddymiania mechanicznego. Przypadki te zaprezentowano na *fot. 1* i *2*.
W obu przypadkach należało zastosować specjalne rozwiązania i zabiegi techniczne, które pozwoliły na zrealizowanie zasilania urządzeń przeciwpożarowych i sterowania nimi.

Fot. 1. Widok systemu nośnego siatkowych korytek kablowych do zasilania instalacji oddymiania grawitacyjnego.

Fot. 2. Widok zespołu klap odcinających zamykających wlot do oddymiających wentylatorów wyciągowych.

Podsumowanie

W artykule nie opisano szczegółowych rozwiązań technicznych zastosowanych w obiekcie Dworca Łódź Fabryczna. Przytoczone przykłady obrazują problem, jaki napotykają wykonawcy instalacji przeciwpożarowych. Ważne, by architekci i specjaliści, którzy opracowują operaty i scenariusze pożarowe w początkowej fazie tworzenia projektu budowlanego, zwrócili uwagę na to, aby problemy związane z rzeczywistym sposobem prowadzenia i mocowania przeciwpożarowych zespołów kablowych były rozwiązywane w początkowej fazie realizacji budowy.
Takie działania powinny być związane z uczestnictwem w procesie projektowym ekspertów, którzy potrafią w sposób właściwy i zgodny z przepisami ocenić i zaproponować rozwiązanie tych problemów. Wszystkich zainteresowanych zapraszam do dyskusji na ten temat na stronach IBP Nodex.

[1] Rozporządzenie Ministra Infrastruktury z 12 kwietnia 2002 r. z późniejszymi zmianami w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (tekst jedn. Dz.U. z 2009 r. nr 56, poz. 461).
[2] PN-EN 1363-1:2001 Badania odporności ogniowej – Część 1: Wymagania ogólne.

Scenariusze pożarowe

podstawy prawne i zasady tworzenia

Rafał Porowski, Waldemar Wnęk
Wydział Inżynierii Bezpieczeństwa Pożarowego,
Szkoła Główna Służby Pożarniczej

Formalne określenie „scenariusza pożarowego" zostało wprowadzone do rozporządzenia MSWiA z 2 grudnia 2015 r. w sprawie uzgadniania projektu budowlanego pod względem ochrony przeciwpożarowej (Dz.U. z 2015 r., poz. 2117). Jego definicję podano jako opis sekwencji możliwych zdarzeń w czasie pożaru reprezentatywnego dla danego miejsca wystąpienia lub obszaru oddziaływania, w szczególności dla strefy pożarowej lub strefy dymowej, z uwzględnieniem przede wszystkim:

- sposobu funkcjonowania urządzeń przeciwpożarowych, innych technicznych środków zabezpieczenia przeciwpożarowego, urządzeń użytkowych lub technologicznych oraz ich współdziałania i oddziaływania na siebie,
- rozwiązań organizacyjnych niezbędnych do właściwego funkcjonowania projektowanych zabezpieczeń.

Ponadto w jednym z 14 wymienionych danych wymaganych w projekcie budowlanym, określonych oraz przedstawionych przez projektanta zapisano:

11) informacje o doborze urządzeń przeciwpożarowych i innych urządzeń służących bezpieczeństwu pożarowemu, dostosowanym do wymagań wynikających z przepisów dotyczących ochrony przeciwpożarowej i przejętych scenariuszy pożarowych, z podstawową charakterystyką tych urządzeń.

Niestety nie określono ani zakresu i treści, ani definicji tego scenariusza. Biorąc pod uwagę powyższe, proponujemy następującą rolę scenariusza rozwoju zdarzeń na wypadek pożaru:

- zapewnienie właściwego doboru urządzeń ppoż.,
- możliwość bezpiecznej ewakuacji ludzi, m.in. przez sterowanie urządzeniami ppoż.,
- dobór odpowiednich materiałów i wyrobów budowlanych,
- zapewnienie właściwego szkolenia personelu,
- planowanie operacyjne na potrzeby działań ratowniczo-gaśniczych,
- przeprowadzenie analizy potencjalnych skutków pożaru dla ludzi i konstrukcji budynku.

Podstawowym parametrem, na którego podstawie można odpowiedzieć na pytanie: „Jak duży jest pożar", jest HRR *(Heat Release Rate)*. Oznacza on szybkość wydzielania ciepła podczas reakcji spalania.

Planowany do przeanalizowania scenariusz uwzględniający rozwój pożaru w pomieszczeniu i/lub obiekcie budowlanym powinny charakteryzować następujące parametry:

- moc pożaru,
- szybkość wydzielania się z pożaru toksycznych produktów spalania,
- szybkość wydzielania się dymu pożarowego,
- rozmiar pożaru,
- czas trwania pożaru,
- czas niezbędny do osiągnięcia kluczowych zdarzeń podczas scenariusza pożarowego (np. zjawiska *flashover* czy *backdraft*).

Podstawowym parametrem, na którego podstawie można odpowiedzieć na pytanie: „Jak duży jest pożar", jest HRR *(Heat Release Rate)*. Oznacza on szybkość wydzielania ciepła podczas reakcji spalania. Parametr HRR (moc pożaru) dla każdego palącego się przedmiotu jest mierzony eksperymentalnie w kilowatach [kW]. HRR określa się dla szybkości, przy której reakcje spalania wydzielają maksimum ciepła. Bardzo często HRR mylnie definiuje się jako szybkość ubytku masy mierzoną w [kg/s]. Nie jest to jednak to samo. Wielkość parametru HRR można określić następującym wzorem [1]:

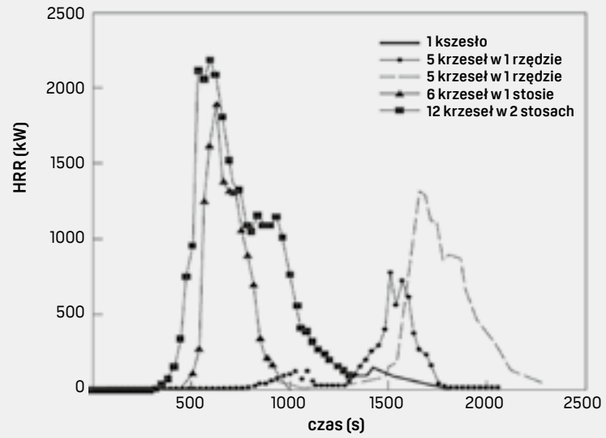
PARAMETR HRR

$$HRR = \Delta h_c \times m^*$$

Δh_c – ciepło spalania [MJ/kg]
m^* – szybkość ubytku masy [kg/s]

Parametr HRR jest bardzo istotny podczas rozwoju pożarów, gdy dopływ powietrza wymaganego do podtrzymania procesów spalania jest dość duży, a charakterystyka pożarowa materiału palnego wpływa na szybkość spalania. Podczas tej fazy rozwoju pożaru wartość HRR rośnie w czasie. Dla wielu materiałów i wyrobów budowlanych wartość HRR jest mierzona w laboratoriach badawczych i ogólnie dostępna [2].

Rys. 1. Wyniki badań doświadczalnych mocy pożaru podczas spalania różnych grup krzeseł [1]



Jednym z kluczowych elementów w każdym scenariuszu pożarowym w obiektach budowlanych jest możliwość wystąpienia zjawiska *flashover,* czyli rozgorzenia. Jest to jednoczesne zapalenie się wszystkich materiałów palnych w analizowanym pomieszczeniu. Parametry krytyczne stanowiące o początku rozgorzenia to [2]:

- średnia temperatura górnej warstwy gazów – 600°C,
- strumień ciepła na poziomie podłogi – 20 kW/m^2.

Projektowany scenariusz może zakładać pożar o tzw. stanie ustalonym, podczas którego jest wydzielana stała ilość ciepła, albo pożar, którego rozwój zależy od czasu. Scenariusze pożarowe w funkcji czasu są powszechnie stosowane do szacowania pewnych kluczowych zdarzeń w teorii rozwoju pożarów, takich jak zjawisko *flashover,* czas zadziałania systemu sygnalizacji pożarowej, utrata odporności ogniowej danego elementu konstrukcji itp.

Z kolei założenie w scenariuszu ustalonego stanu pożaru pozwala na pozostawienie pewnego marginesu bezpieczeństwa w doborze urządzeń przeciwpożarowych, ze szczególnym uwzględnieniem systemów wentylacji pożarowej.

Charakterystyka scenariusza pożarowego ma ogromny wpływ na projektowanie urządzeń przeciwpożarowych w budynku, a tym samym na odpowiedni poziom bezpieczeństwa pożarowego. Należy zwrócić uwagę, że dla danego obiektu może okazać się konieczne poddanie analizie kilku scenariuszy pożarowych.

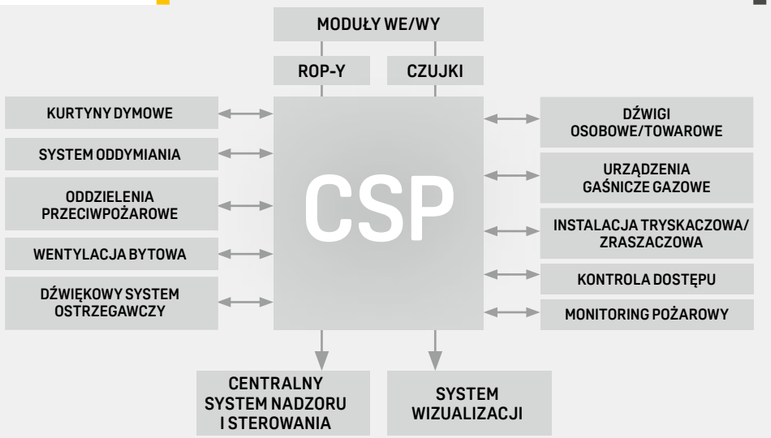
Charakterystyka scenariusza pożarowego ma ogromny wpływ na dobór urządzeń ppoż. w budynku, a tym samym na odpowiedni poziom bezpieczeństwa pożarowego.

Trzeba również zadbać o to, aby wspomniane scenariusze odnosiły się do warunków najbardziej niekorzystnych, jakie mogą wystąpić w danym obiekcie.

Projektowany scenariusz pożarowy powinien dążyć do zapewnienia warunków bezpiecznej ewakuacji ludzi oraz wydzielenia strefy objętej pożarem. Osiągnięcie bezpiecznej ewakuacji będzie możliwe przede wszystkim poprzez zapewnienie odpowiedniego sterowania urządzeniami przeciwpożarowymi, jak również właściwego przeszkolenia personelu. Kryterium bez-

Bezpieczeństwo pożarowe

Przystępując do tworzenia scenariuszy pożarowych, należy gruntownie przeanalizować funkcje, sposób działania i możliwe skutki uboczne zadziałania urządzeń ppoż.



Rys. 2. Urządzenia ppoż. i inne możliwe do sterowania poprzez system sygnalizacji pożarowej [5]

piecznej ewakuacji uznaje się za spełnione, jeżeli [2]:

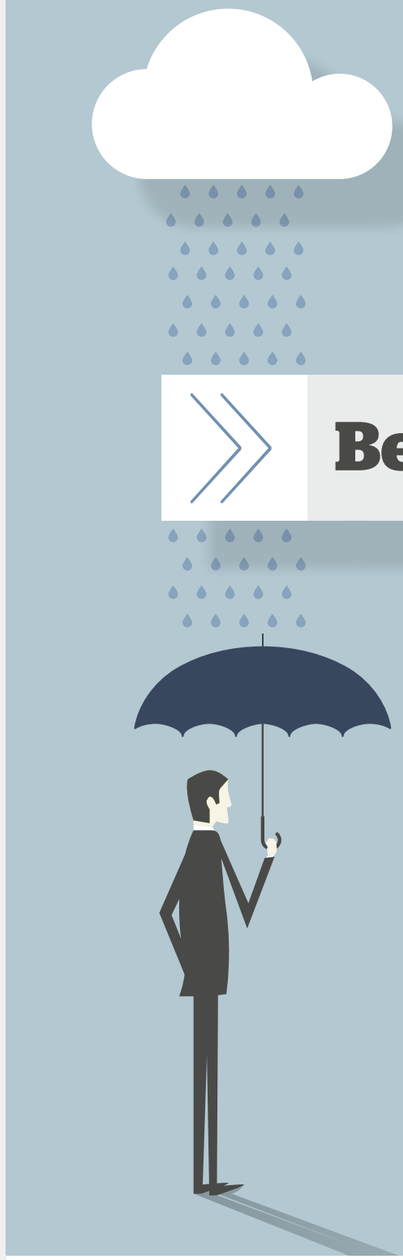
$$DCBE > WCBE + \text{margines bezpieczeństwa}$$

DCBE – dostępny czas bezpiecznej ewakuacji
WCBE – wymagany czas bezpiecznej ewakuacji

Margines bezpieczeństwa powinien być oceniany indywidualnie dla danego obiektu, z uwzględnieniem liczby użytkowników budynku, jego funkcji, uwarunkowań konstrukcyjnych, wyposażenia (np. nagromadzenia materiałów palnych) oraz szacowanego zagrożenia życia. Aby jednak projektowany scenariusz pożarowy zagwarantował bezpieczną ewakuację ludzi, muszą być spełnione określone warunki brzegowe odnoszące się do parametrów pożaru oraz rozprzestrzenienia dymu w obiekcie budowlanym, w tym m.in. [3, 7]:
• temperatura gazów pożarowych (warstwy dymu) na wysokości przekraczającej 2 m od poziomu drogi ewakuacyjnej powinna być mniejsza niż 200°C, jeżeli obliczenia pożaru projektowego są oparte na obniżającej się warstwie górnej gorącego dymu w pomieszczeniu lub na drogach ewakuacyjnych przy minimalnie czystej przestrzeni do 2 m (modele strefowe i korelacje inżynierskie);
• temperatura powietrza w przestrzeni drogi ewakuacyjnej do wysokości 1,8 m poniżej 60°C;
• zasięg widzialności znaków ewakuacyjnych i elementów konstrukcyjnych budynku na wysokości 1,8 m od poziomu podłogi drogi ewakuacyjnej nie mniejszy niż 10 m;
• gęstość strumienia promieniowania cieplnego na wysokości 1,8 m od poziomu posadzki nie większa niż 2,5 kW/m^2 w czasie niezbędnym na ewakuację;
• przyjmuje się, że podczas spalania standardowych materiałów palnych toksyczność dymu nie jest parametrem krytycznym, jeżeli jest zachowana widzialność przekraczająca 5 m.

Przystępując do tworzenia poszczególnych scenariuszy pożarowych, należy gruntownie przeanalizować funkcje, sposób działania i możliwe skutki uboczne zadziałania urządzeń przeciwpożarowych. Nie bez znaczenia jest też możliwość zastosowania systemu integrującego do sterowania urządzeniami bezpieczeństwa. Konieczne jest również przewidzenie możliwych reakcji użytkowników obiektu, które mogą mieć wpływ na uruchomienie alarmowania i proces ewakuacji.
W systemach sygnalizacji pożarowej możliwe jest automatyczne, zależne od miejsca detekcji pożaru i zaprogramowanych zależności czasowo-zdarzeniowych, wysterowanie wind, zamknięcie drzwi i bram pożarowych, zamknięcie klap pożarowych w wentylacji bytowej, otwarcie klap nawiewnych oraz wyciągowych wentylacji oddymiającej, otwarcie klap wentylacji grawitacyjnej, otwarcie drzwi na drogach ewakuacyjnych, wysterowanie instalacji gaszenia, odcięcie dopływu gazu, zatrzymanie wentylacji i procesów przemysłowych. Możliwe są także inne reakcje i sterowania wykonywane zgodnie ze scenariuszem pożarowym dla obiektu [5].
Należy pamiętać również o bardzo istotnym aspekcie znaczenia scenariusza pożarowego dla bezpieczeństwa ekip ratowniczych. W tym zakresie projektowany scenariusz musi zapewniać w obiekcie spełnienie następujących parametrów krytycznych, które mogą wystąpić w czasie pożaru [6]:
• temperatura powietrza w przewidywanym czasie podjęcia działań ratowniczo-gaśniczych na wysokości 1,75 m od poziomu posadzki w odległości do 15 m od źródła pożaru nie powinna przekraczać 120°C,
• widzialność wyjścia ewakuacyjnego – drogi ucieczki.

Literatura
[1] SFPE Handbook of Fire Protection Engineering, Society of Fire Protection Engineers, 2008.
[2] PD 7974-1:2003, Application of fire safety engineering principles to the design of buildings – Part 1: Initiation and development of fire within the enclosure of origin, British Standards.
[3] PD 7974-2:2003, Application of fire safety engineering principles to the design of buildings – Part 2: Spread of smoke and toxic gases within and beyond the enclosure of origin, British Standards.
[4] PD 7974-3:2003, Application of fire safety engineering principles to the design of buildings – Part 3: Structural response and fire spread beyond the enclosure of origin, British Standards.
[5] PD 7974-4:2003, Application of fire safety engineering principles to the design of buildings – Part 4: Detection of fire and activation of fire protection systems, British Standards.
[6] PD 7974-5:2003, Application of fire safety engineering principles to the design of buildings – Part 5: Fire service intervention, British Standards.
[7] PD 7974-6:2003, Application of fire safety engineering principles to the design of buildings – Part 6: Human factors: Life safety strategies – Occupant evacuation, behavior and condition, British Standards.



W dobie dynamicznie zmieniających się zagrożeń zmienia się także zakres działań, którymi zajmują się specjaliści od bezpieczeństwa biznesu. Jest to jednak niewątpliwie coraz ważniejsza dziedzina, która w niepewnych czasach dotyczy w zasadzie wszystkich aspektów funkcjonowania firm i instytucji.

Bezpieczeństwo biznesu

Bezpieczeństwo biznesu to m.in.:
• ochrona fizyczna,
• systemy zabezpieczeń technicznych,
• bezpieczeństwo logistyczne,
• bezpieczeństwo imprez masowych,
• bezpieczeństwo informacji,
• bezpieczeństwo podróży,
• weryfikacja kontrahentów i osób,
• brand protection,
• loss prevention,
• bezpieczeństwo hoteli,
• bezpieczeństwo obiektów handlowych,
• ochrona VIP-ów,
• zagrożenia terrorystyczne.

Partnerem merytorycznym działu *Bezpieczeństwo biznesu* jest firma SASMA, która zapewnia najwyższy poziom merytoryczny publikowanych treści i poruszanych tematów. Do współpracy włączyli się również doświadczeni praktycy – wysokiej klasy specjaliści od bezpieczeństwa biznesu z kraju i zagranicy.

ROZWÓJ PRZESTĘPCZOŚCI W OBSZARZE DANYCH OSOBOWYCH – KRADZIEŻ TOŻSAMOŚCI

Autor odnosi się do groźnych skutków kradzieży oraz fałszowania tożsamości osób fizycznych i prawnych w działalności przedsiębiorcy zajmującego się ochroną osób i mienia oraz systemami alarmowymi. Wskazuje na różne zdarzenia, a także omawia ich potencjalne negatywne skutki dla firmy i jej pozycji na rynku.
Artykuł stanowi rozwinięcie problematyki zasygnalizowanej w pierwszej części cyklu opublikowanej w ostatnim numerze „Systemów Alarmowych" (6/2016).

Marek Blim

Prawna ochrona danych osobowych ma na celu uporządkowanie wszelkich czynności zmierzających do ochrony osób fizycznych przed pochopnym ujawnieniem czy utratą ich danych stanowiących tożsamość w świecie e-biznesu. Ale jak przedsiębiorca, zajmujący się systemami alarmowymi w fizycznej i technicznej ochronie osób i mienia, może to wykorzystać w swojej praktyce zawodowej? Odpowiedź brzmi: skutecznie, zwłaszcza że świadczy usługi dla mikroprzedsiębiorstw sygnowanych nazwiskiem właściciela (np. firma „Cerber – Jan Nowak", adres firmowy jest adresem domowym właściciela), a użytkownicy systemów nagminnie używają swoich danych osobowych do tworzenia haseł dostępowych. Odrębną kwestią jest ochrona dostępu do wybranych urządzeń (np. depozytory kluczy) z zasady realizowana w dużych firmach za pośrednictwem imiennych kart dostępowych (dane osobowe, a także elementy biometrii danej osoby fizycznej).
Pożądane jest więc wdrażanie mechanizmów zwiększających ochronę prywatności, przede wszystkim zalecanych w nowym rozporządzeniu Parlamentu i Rady Europejskiej (tzn. *privacy by design* – na etapie projektowania; *privacy by default* – jako ustawienia domyślne), w odniesieniu do danych osób fizycznych będących użytkownikami tychże systemów ochronnych.

Przedsiębiorca w systemach ochronnych a kwestia fałszywej tożsamości

Przedsiębiorca prowadzący firmę usługową z zakresu ochrony obiektu (systemy alarmowe, ochrona fizyczna i techniczna) jest swego rodzaju powiernikiem wiedzy w zakresie działalności zawodowej (projektowanie, montaż, eksploatacja, obsługa bieżąca czy konserwacja) w odniesieniu do chronionych zasobów (mienie, wartości, informacje, zasoby ludzkie). Sytuacja ta nakłada na niego obowiązek szczególnej wnikliwości wobec wszelkich oddziaływań zewnętrznych i wewnętrznych związanych z wykonywanymi zleceniami i kontraktami, w ocenie prawdziwości tożsamości osób nawiązujących kontakty zawodowe (wywiad gospodarczy, konkurencja) lub informacyjno-handlowe (pseudodziennikarze, środowiska przestępcze) przy okazji licznych wystaw i targów zawodowych.
Odrębną kwestią dla wizerunku firmy i jej pozycji na rynku staje się nadzór nad pracownikami własnymi i wynajętymi (zachowanie tajemnic firmy), potwierdzenie ich wiarygodności i poprawności działania (casus: napad dokonany przez ochroniarzy banku 3 marca 2001 r. na placówkę Kredyt Banku w Warszawie)[1].
Wymagania ochrony wynikają z ogólnie znanych faktów związanych z działaniami o charakterze szpiegostwa gospodarczego i przestępczego typu:
– pośrednik (zwykle z fałszywą tożsamością) z podstawionymi zleceniami, rozpoznający potencjał osobowy firmy (działanie bardzo często związane z *headhuntingiem*);
– pseudozamówienie i oferta z SIWZ mająca na celu rozpoznanie potencjału czy możliwości organizacyjno-technicznych oraz osobowych (uprawnienia zawodowe pracowników);
– wyłudzenie istotnych informacji zawodowych od pracownika przez „fałszywego dziennikarza" pod pozorem wywiadu dla czasopisma branżowego (działanie prowadzone na ogół przy okazji targów i wystaw specjalistycznych).

> Zasada postępowania jest prosta. Zawsze licz na siebie, czyli wierz i sprawdzaj! Każdy sam musi bowiem zadbać o powodzenie prowadzonej przez siebie działalności.

Wszystkie te działania mają charakter oszustwa (fraud) i są realizowane „pod przykryciem" fałszywej tożsamości osób fizycznych (zamawiający, dziennikarz, dociekliwy interesant) lub prawnych (oferty i zapytania e-mailowe z witryn publicznych itp.), często są poparte dodatkowymi czynnościami socjotechnicznymi (tzw. oswajanie ofiary) przez oszukującego.
Zabezpieczenie podstawowe polega na ustanowieniu w firmie/przedsiębiorstwie stanowiska uprawnionego do kontaktów zewnętrznych (osoba przeszkolona i w pełni świadoma potencjalnych szkodliwych skutków w przypadku ujawnienia istotnej wiedzy), będącego filtrem informacyjnym dla otoczenia zewnętrznego, przy jednoczesnym przeszkoleniu i uświadomieniu całego personelu o potencjalnych szkodliwych dla firmy działaniach w jej otoczeniu. Identyfikacja potencjalnych ataków umożliwia na ogół skuteczną ochronę przed nimi oraz ew. podjęcie przez zagrożonego nimi przedsiębiorcę działań administracyjno-prawnych przeciwko sprawcom.

Kradzież lub przejęcie tożsamości osoby fizycznej i jej potencjalne skutki dla firmy

Współcześnie pojęcie kradzieży tożsamości osoby fizycznej wiąże się nie tyle z utratą dokumentów papierowych (portfel z dowodem osobistym, paszportem, kartami kredytowymi, przepustkami itp.), ile z przechwyceniem danych z tych dokumentów (dane osobowe, PESEL, PIN itp.) identyfikujących i uwierzytelniających, którymi dana osoba posługuje się w kontaktach elektronicznych (e-business, e-payment, e-health itd.). Dane osoby uzyskane w nielegalny sposób mogą stać się elementem oszustwa finansowego, szantażu zawodowego lub prywatnego bądź kompromitacji w środowisku czy życiu prywatnym. Zagrożenie ujawnieniem danych osobowych na dużą skalę[2] powoduje komplikacje i wymuszone działania sprawdzające osób oraz instytucji (m.in. szturm na międzybankową bazę dokumentów zastrzeżonych)[3].

Poszkodowany przedsiębiorca

Mówiąc o przedsiębiorcy poszkodowanym z racji nieuprawnionego ujawnienia (w postaci przejęcia lub kradzieży danych osobowych), nie odnosimy się do niego jako osoby fizycznej, której dane osobiste zostały przechwycone i z tego tytułu poniosła ona indywidualne straty. W rozumieniu treści artykułu przedsiębiorca, właściciel firmy, jej kierownik to osoby, które z mocy prawa (uodo)[4] są odpowiedzialne za ochronę wszystkich danych osobowych przetwarzanych w przedsiębiorstwie, firmie, organizacji jako ustawowy administrator danych osobowych (ADO), w tym także za ich upoważnione przetwarzanie. Jeżeli dojdzie do ich ujawnienia, to właśnie administrator musi mieć świadomość odpowiedzialności:
– **karnej – na podstawie rozdz. 8 art. 47–54 ustawy o ochronie danych osobowych** (tekst jednolity: Dz.U. z 2016 r., poz. 922 z późn. zm.),
– **cywilnej – w postępowaniu odszkodowawczym na podstawie art. 415** i/lub **art. 429** kodeksu cywilnego z 23 kwietnia 1964 r. tekst jednolity: Dz.U. z 2016 r., poz. 380 z późn. zm.)
wszczętym przez osobę, której dane ujawniono, i jest ona z tego tytułu poszkodowaną, ponieważ **wg rozdz. 5 uodo, art. 36, ust. 1** to właśnie ADO jest obowiązany zastosować środki zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udo-

1) P. Machajski, *Kryminalna Warszawa*, „Gazeta Wyborcza", 22.08.2015 r.
2) J. Kosmatka, „Dziennik Łódzki", 26 sierpnia 2016 r.; *www.dzienniklodzki.pl/na-sygnale/a/abw-w-lodzkich-kancelariach-komorniczych-sledztwo-w-sprawie-wycieku-numerow-pesel,10557384/.*
3) Kampania Informacyjna Systemu DZ, *www.dokumentyzastrzezone.pl* – jest już ponad półtora miliona dokumentów zastrzeżonych (15.09.2016).
4) Uodo – ustawa z 27 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2016 r., poz. 922).

stępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy i zmianą, utratą, uszkodzeniem lub zniszczeniem zarówno u siebie, jak i w przypadku ich powierzenia usługodawcy (outsoucerowi, procesorowi) w ramach zleconej usługi. Zatem wszelkie nieuprawnione działania skierowane przeciw zbiorom danych osobowych posiadanym przez przedsiębiorcę mogą się stać podstawą do strat i szkód w majątku firmy oraz penalizacji działań wobec jej osób funkcyjnych. Przedsiębiorstwo, firma, organizacja może także stać się ofiarą oszustwa z wykorzystaniem fałszywej tożsamości kontrahenta. Bezpieczeństwo osób poszkodowanych oraz obrotu gospodarczego zależy od powszechnego przeciwdziałania wyłudzeniom z użyciem cudzej tożsamości.

Pojęcie kradzieży tożsamości osoby fizycznej wiąże się nie tyle z utratą dokumentów papierowych (dowód osobisty, paszport, karty kredytowe, przepustki itp.), ile z przechwyceniem danych z tych dokumentów (dane osobowe, PESEL, PIN itp.) identyfikujących i uwierzytelniających, którymi posługujemy się w kontaktach elektronicznych (e-business, e-payment, e-health itd.).

Poszkodowany pracownik

Pracownik, podejmując pracę, ma obowiązek podania pracodawcy swoich danych osobowych zgodnie z ustawą z 5 maja 1974 r. – Kodeks pracy (tekst jednolity: Dz.U. z 2014 r., poz. 1502 z późn. zm.). Zmiany dotyczące zakresu danych osobowych pracownika wprowadzono w 2003 r., dodając poniższy artykuł:

art. 22 *§ 1. Pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących: 1) imię (imiona) i nazwisko; 2) imiona rodziców; 3) datę urodzenia; 4) miejsce zamieszkania (adres do korespondencji); 5) wykształcenie; 6) przebieg dotychczasowego zatrudnienia.*

§ 2. Pracodawca ma prawo żądać od pracownika podania, niezależnie od danych osobowych, o których mowa w § 1, także: 1) innych danych osobowych pracownika, a także imion i nazwisk oraz dat urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy; 2) numeru PESEL pracownika nadanego przez Rządowe Centrum Informatyczne Powszechnego Elektronicznego Systemu Ewidencji Ludności (RCI PESEL).

§ 3. Udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą. Pracodawca ma prawo żądać udokumentowania danych osobowych osób, o których mowa w § 1 i § 2.

§ 4. Pracodawca może żądać podania innych danych osobowych niż określone w § 1 i § 2, jeżeli obowiązek ich podania wynika z odrębnych przepisów.

§ 5. W zakresie nieuregulowanym w § 1–4 do danych osobowych, o których mowa w tych przepisach, stosuje się przepisy o ochronie danych osobowych.

Należy jednak pamiętać, że to od przyszłego pracownika zależy, w jaki sposób, gdzie, kiedy i komu te dane zostaną przez niego przekazane. Nieprzemyślane udostępnianie własnych danych w trakcie aplikacji o zatrudnienie stwarza okazję do oszustw. Powołana 15 września 2016 r. Komisja Kodyfikacyjna Prawa Pracy być może będzie w stanie opracować podczas zaplanowanych osiemnastu miesięcy tekst kodeksu nowej, odpowiadającej rzeczywistym stosunkom prawnym, konstytucji zatrudnienia[5].

Odrębnym problemem są działania socjotechniczne różnego rodzaju akwizytorów, oferentów czy konsultantów podejmowane wobec konkretnych osób w firmie i obliczone na pozyskanie danych osobowych i zawodowych pracowników planowanych do ew. przejęcia przez konkurencję („łowcy głów" – *headhunting*).

Jedynym sposobem przeciwdziałania są szkolenia uczące, czego można się po takich „gościach" spodziewać i jak temu zjawisku zapobiegać, aby nie dać się sprowokować do mimowolnego ujawnienia chronionych danych (często nie tylko osobowych)[6].

Poszkodowany klient

Działalność przedsiębiorcy zajmującego się projektowaniem, montowaniem, eksploatacją oraz konserwacją systemów ochronnych (alarmowych, ochrony fizycznej i technicznej) jest reakcją na potrzeby rynku, na którym klienci oczekują tego typu usług w trosce o swoje dobra (mienie, wartości, informacje). Sytuacja, w której „posiadacz dóbr" czasem o znacznej wartości szuka oszczędności przy instalowaniu alarmów do ich ochrony, nie należy do rzadkości, a to w ostatecznym rachunku skutkuje często stratami, nie tylko materialnymi.

Kradzież i przejęcie tożsamości osoby prawnej i jej potencjalne skutki dla firmy

Przedsiębiorca w XXI wieku, w epoce e-społeczności i e-biznesu, realizując płatności za pośrednictwem metod typu e-payment i e-banking, powinien pamiętać, że przestępcy dokonujący kradzieży tożsamości stosują coraz bardziej urozmaicone sposoby pozyskiwania informacji poufnych, takie jak wirusy komputerowe, robaki, konie trojańskie oraz tzw. techniki inżynierii społecznej (techniki wykorzystujące naiwność i niewiedzę innych użytkowników internetu) w odniesieniu zarówno do osoby prywatnej, jak i do uprawnionego przedstawiciela firmy.

Ponadto przedsiębiorca funkcjonujący w ramach transakcji *homebankingu* w swojej firmie powinien mieć świadomość, że od 2007 r. rozwijają się techniki oparte na złośliwym oprogramowaniu, takim jak Mebroot czy ZEUS, które wykradają dane wpisywane do poprawnego serwisu transakcyjnego czy strony banku. Programy tego typu ewoluują, obecnie umożliwiają nawet zmianę numeru konta docelowego w momencie dokonywania transakcji, w wyniku czego środki trafiają bezpośrednio na konto przestępcy.

Obecnie – mimo stosowania różnych metod zabezpieczeń chroniących przed przestępcami, takich jak loginy, hasła, kody jednorazowe, tokeny, hasła SMS-owe, podpisy elektroniczne – nie można czuć się w pełni bezpiecznie. Żadna ze wskazanych metod nie gwarantuje stuprocentowego bezpieczeństwa i zidentyfikowania osoby, która dokonuje transakcji bankowych. Bank również nie jest w stanie stwierdzić, kto dokonuje weryfikacji tożsamości: czy to klient, czy inna osoba. Dotyczy to osoby zarówno fizycznej (użytkownika prywatnego), jak i prawnej (firmy, przedsiębiorstwa, organizacji). Zawsze bowiem znajdzie się ktoś czyhający na chwilę nieuwagi, aby przejąć dane prywatne czy firmowe. Należy więc zachować szczególną ostrożność i dochować należytej staranności w ochronie danych poufnych przy korzystaniu m.in. z bankowości internetowej w ramach legalnych działań transakcyjnych.

Kodeks karny odnosi się bezpośrednio do stwierdzonego przestępstwa kradzieży tożsamości (art. 190a § 2, art. 267, art. 268, art. 269a, art. 269b, art. 270, art. 275).

Ochronie podlega pewność obrotu prawnego, wiarygodność występujących w nim dokumentów stwierdzających tożsamość danej osoby, porządek prawny w zakresie obowiązku posiadania dokumentu tożsamości związany z posługiwaniem się dokumentami stwierdzającymi tożsamość oraz sam dokument stwierdzający tożsamość.

W obowiązujących przepisach „dokument stwierdzający tożsamość" nie jest zdefiniowany. Zgodnie z art. 275 kk za taki dokument można uznać każdy dokument, także w formie elektronicznej, który poświadcza tożsamość[7].

Definicję dokumentu wskazano w art. 115 § 14 kk (Dz.U. z 1997, nr 88, poz. 553 z późn. zm.). To każdy przedmiot lub zapis na komputerowym nośniku informacji, z którym jest związane określone prawo albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne. Na tej podstawie można więc stwierdzić, że dokument da się sfałszować również w systemie teleinformatycznym, np. zmieniając treść e-maila. Sąd Najwyższy uznał, że dokument jest podrobiony, jeżeli nie pochodzi od osoby, w której imieniu został sporządzony[8]. Orzeczenie to jest zatem podstawą do karania za tworzenie e-maili łudząco podobnych do rozsyłanych, np. przez banki, firmy oferujące usługi itp.

Pseudofirma („krzak", „słup", fałszywe zakupy)

Są sytuacje, w których przedsiębiorca prawidłowo funkcjonujący na rynku styka się bezpośrednio, choć niekoniecznie w sposób zamierzony, z działaniami szarej strefy, np. rynku usług ochroniarskich. Towarzyszące temu zjawiska czasami wzbudzają wątpliwości, np.

– zamieszczona w ramach ogłoszeń na specjalistycznych portalach polskich oferta sprzedaży w konkurencyjnych cenach sprzętu ochroniarskiego średniej światowej klasy okazała się próbą wprowadzenia na rynek polski, za pośrednictwem doraźnie utworzonej firmy typu „krzak", materiałów oraz urządzeń z okradzionej kilka tygodni wcześniej hurtowni niemieckiej (sic!);

– nagminne jest wykorzystywanie danych konkretnych osób (firma-słup) nieposiadających materialnego zabezpieczenia do realizacji ryzykownych transakcji materiałowych czy usługowych kończących się przepadkiem kwot wpłaconych *a conto* lub na faktury *pro forma*, na podstawie adresowanych imiennie do przedsiębiorców superofert o wyjątkowo korzystnych cenach sprzętu czy materiałów instalacyjnych, miejscu i czasie dostawy (np. *loco* magazyny firmy) itp. bonusach, m.in. 30-procentowy upust pod warunkiem wpłaty 10% wartości zamówienia (typowy *fraud*).

Przejęcie domeny, strony firmowej (*domain slamming*)

Oszustwo domenowe to łatwy zarobek dla sprytnych wyłudzaczy, którzy na jednej domenie zarabiają rocznie 100, 200 czy 300 zł, a nawet więcej. Niby to niewiele, ale mając kilkudziesięciu czy kilkuset oszukanych w ten sposób klientów, *domain slamming* może być dla nieuczciwych firm lub osób sposobem na łatwy i duży zarobek. Oszustwo domenowe, za granicą znane jako *domain name selling scam*, już trafiło do Polski i ma się tu dobrze.

Schemat jest bardzo prosty. Załóżmy, że prowadzimy firmę, której domena to **costam.pl.** Nagle dzwoni telefon. Pani przyjemnym głosem przedstawia się, mówiąc, że dzwoni z firmy internetowej z pytaniem, czy osoba, do której dzwoni, jest właścicielem domeny **costam.pl**. Po potwierdzeniu ta miła pani zaaferowanym głosem informuje, że właśnie ktoś stara się wykupić domeny: **costam.com.pl**, **costam.net.pl** itd., ale wiedząc, że już wersja .pl należy właśnie do nas, również te domeny może dla nas zamówić.

Dane osoby uzyskane w nielegalny sposób mogą stać się elementem oszustwa finansowego, szantażu zawodowego lub prywatnego bądź kompromitacji w środowisku czy życiu prywatnym.

W obawie przed nieuczciwą konkurencją wyrażamy zgodę, faktura *pro forma* po tej rozmowie zostaje wysłana w ciągu pół godziny i niezwłocznie zostaje opłacona. *Firma uratowana…* Ale okazuje się, że faktura za domenę wyniosła 199 zł + VAT. Nie za drogo? Tak, ok. 20 razy, gdyż w promocji można tę domenę kupić za ok. 10 zł.

Firma sprzedająca domeny na ogół istnieje i rzeczywiście je kupiła, tyle że nie dla klienta, ale dla siebie. Klient ma umowę, że od tej firmy ją dzierżawi. W przekazywanych klientom fakturach pokrętnie napisano, że opiewają one za usługi zamówienia

[5] Ł. Góra, *Ruszają prace nad nowym kodeksem pracy. Co się zmieni?*, „Gazeta Prawna", 15.09.2016.
[6] K.D. Mitnick, W.L. Simon, *Sztuka podstępu. Łamałem ludzi nie hasła*, Helion, Katowice 2016.
[7] Opracowanie: K. Oksiędzka, *Internet. Ochrona własności i bezpieczeństwa*, red. Grażyny Szpor, Wydawnictwo C.H. Beck, Warszawa 2011.
[8] I KZP 6/01 Uchwała Sądu Najwyższego – Izba Karna z 2001-04-27; VI SA/Wa 255/06 – wyrok WSA w Warszawie z 2006-05-25; III KK 67/10 – wyrok Sądu Najwyższego Izba Karna z 5.08.2010.

domeny. Takie firmy nie mają akredytacji NASK ani ICANN. Niestety naiwność ludzi przyczynia się do pomnażania ich majątku, na jednej domenie mogą zarobić ok. 180 zł. Ten proceder jest powtarzany w kolejnych latach. By się przed tym ustrzec, w bazach whois.pl oraz whois.org warto sprawdzić, kto jest właścicielem oferowanych domen[9].
Jak ma sobie z tym poradzić przedsiębiorca?[10] Musi przede wszystkim zgłosić oszustwo policji i NASK. Nieuczciwa firma musi dokonać cesji domeny (wówczas w rejestrze NASK zostanie wpisany właściciel uprawniony do danej domeny). Często zaufane, dobre i tanie firmy, w których można bezpiecznie i uczciwie zarejestrować domenę, nie są bezpośrednim partnerem NASK, a jedynie współpracują z partnerami NASK (tak robi większość firm oferujących hosting). Zazwyczaj na swoich stronach internetowych podają one, z którym partnerem NASK współpracują, np. firma Masternet.
Osoby, które w jakikolwiek sposób zostały oszukane w związku z nazwami domen, mogą kierować sprawy do sądu polubownego lub powszechnego. Są to:
- Sąd Polubowny ds. Domen Internetowych przy Polskiej Izbie Informatyki i Telekomunikacji,
- Sąd Arbitrażowy przy Krajowej Izbie Gospodarczej w Warszawie,
- The World Intellectual Property Organization Arbitration and Mediation Center.

Na podstawie orzeczeń sądów NASK dokonuje zmian abonentów domen internetowych.

Doraźne działania krytyczne w obszarze ochrony danych osobowych w firmie

Działania w obszarze ochrony danych osobowych w firmie mają punkty krytyczne. Problemem nr 1 są sytuacje, w których dochodzi do ujawnienia na terenie firmy lub poza nią istotnych danych osobowych pracownika (pensja, kwalifikacje, awans, informacje na temat zdrowia itp.), powodujące dodatkowe zamieszanie i plotki oraz przypuszczenia co do działań kierownictwa oraz osób funkcyjnych, szczególnie gdy osoba ta zaczyna uważać się za poszkodowaną i dochodzi swoich praw za pośrednictwem GIODO[11].
Problemem nr 2 dla każdego ADO (administratora danych osobowych w rozumieniu wymagań ustawowych) są sytuacje, kiedy trzeba realizować zapisy danych pracowników, klientów lub osób trzecich (kurier, listonosz, konserwator itp.) w związku z zaistniałym na terenie firmy wypadkiem z uszczerbkiem na zdrowiu. Są to kwestie protokołów powypadkowych (bhp, ppoż. i inne), a także pierwsza pomoc i ratownictwo przedlekarskie[12] związane z pomocą przedmedyczną oraz obowiązkiem posiadania w firmie osób przeszkolonych (informacja przy każdej apteczce) w udzielaniu doraźnej pierwszej pomocy osobom poszkodowanym. Informacje o stanie zdrowia należą do zbioru danych wrażliwych, stąd konieczność szczególnego nadzorowania ich przetwarzania i udostępniania (wymagania ustawowe: art. 27 uodo).

> Okazuje się, że faktura za domenę wyniosła 199 zł + VAT. Nie za drogo? Tak, ok. 20 razy, gdyż w promocji można tę domenę kupić za ok. 10 zł.

Za problem nr 3 należy uznać funkcjonowanie na terenie firmy różnych usługodawców zatrudnionych w ramach outsourcingu zadań własnych firmy, takich jak sprzątanie, usługi żywieniowe, wywózka śmieci, konserwacja sprzętu. Wiążą się one pośrednio z poznawaniem danych osobowych personelu macierzystego firmy, a nie są (niestety) dostatecznie zabezpieczone i nadzorowane.
Nagminny jest brak odpowiednich klauzul w umowach, nie dba się o szkolenia i oświadczenia o zachowaniu w poufności informacji uzyskanych w trakcie realizacji prac, często wykonawca umowy (procesor) wprowadza na teren firmy pracownika swojego podwykonawcy, nie informując o tym zleceniodawcy.

Uwagi końcowe

Przestępczość w obszarze pozyskiwania danych osobowych rośnie lawinowo, szczególnie w sieci. Dane musimy chronić przede wszystkim sami, dlatego warto dokładnie sprawdzić, kto np. jest nadawcą e-maila. Na ogół poważna firma ma adres z własną domeną i nie musi korzystać z bezpłatnych skrzynek. Jeśli strona www tej firmy istnieje, jej właściciela można sprawdzić w bazie whois.org czy dns.pl. Dane ukryte sugerują, że takiej firmie nie można ufać.
Może się zdarzyć, że dane będą fałszywe – w grę może wtedy wchodzić skradziona tożsamość. Sprawdzając wpis w bazie whois.org, można też dowiedzieć się, ile czasu domena istnieje – jeżeli kilka dni, należy zachować szczególną ostrożność, gdyż w przypadku kradzieży tożsamości to właśnie czas istnienia domeny ma duże znaczenie.
Nie należy wierzyć w zbyt dobre oferty, tym bardziej gdy oferent towaru chce zapłaty nie na konto, ale przy użyciu serwisu, np. Western Union czy Escrow Service – na 99,9 proc. oznacza to, że mamy do czynienia z oszustem. Innym sygnałem oszustwa jest pośpiech.
Gdy firma-oferent jest lokowana w Polsce, można i należy sprawdzić jej dane w GUS pod adresem www.stat.gov.pl/regon/.
W przypadku oferenta – osoby fizycznej należy skorzystać z możliwości „Systemu DOKUMENTY ZASTRZEŻONE" (system DZ). Mają do niego dostęp nie tylko podmioty z sektora bankowego, ale także wszystkie instytucje, które w ramach prowadzonej działalności identyfikują osoby na podstawie dokumentów umożliwiających stwierdzenie tożsamości. Warunkiem korzystania jest podpisanie umowy przez firmę. W imieniu Związku Banków Polskich obsługą Systemu DZ zajmuje się Centrum Prawa Bankowego i Informacji Sp. z o.o. (www.cpb.pl).
Zasada postępowania jest prosta. Zawsze licz na siebie, czyli wierz i sprawdzaj! Każdy sam musi bowiem zadbać o powodzenie prowadzonej przez siebie działalności.

9) Materiały informacyjne INFOSEC, http://www.oszustwsieci.pl/oszustwo_domenowe.php.
10) www.nawitrynie.pl/oszukuja-domenach-zobacz-czym-polega-oszustwo-domenowe-2/.
11) GIODO - Generalny Inspektor Ochrony Danych Osobowych, www.giodo.gov.pl.
12) Porady praktyczne - www.ratownictwo.win.plwww.ratownictwo.win.pl.

AGENCJE OCHRONY W XXI WIEKU

Oszukańczo niskie wynagrodzenia, niejasne formy zatrudniania ochroniarzy, „emeryci i renciści" na posterunkach i zdarzające się kradzieże – agencje ochrony nie kojarzą się zbyt pozytywnie. Czy ten wizerunek odzwierciedla stan faktyczny? Czy ma szansę się zmienić? Jak będą wyglądały agencje ochrony w przyszłości?

Krzysztof Moszyński
Konsalnet

Do zmian ustrojowych w 1989 r. ochrona komercyjna w Polsce jako segment prywatnego rynku w zasadzie nie istniała. Czas, w którym tego rodzaju przedsiębiorstwa rozwijały się na świecie (pierwsze prywatne firmy mają ponad 100-letnią historię), spędziliśmy najpierw pod zaborami, później odbudowując kraj, następnie znów walcząc z okupantem i w końcu będąc w okowach „jedynie słusznego" ustroju. W tym czasie prywatni przedsiębiorcy nie mogli świadczyć usług związanych z ochroną, bo wszystko było zarezerwowane dla zaborców, okupanta, a później państwa.
Sektor ochrony komercyjnej w Polsce rozpoczął działanie wraz z przyznaniem pierwszych pozwoleń (koncesji) związanych z wykonywaniem usług z zakresu ochrony osób i mienia w 1989 r., na podstawie ustawy o działalności gospodarczej. Departament Społeczno-Administracyjny MSW wydał blisko 8 tys. pozwoleń umożliwiających świadczenie usług ochrony, natomiast wg danych MSWiA w 1997 r. w tym sektorze było zatrudnionych blisko 125 tys. osób. Podobne dane można uzyskać z innych źródeł, z których wynika, że do 1997 r. w Polsce działało do 6 tys. podmiotów gospodarczych, które łącznie zatrudniały od 130 do 160 tys. pracowników ochrony. Większość z nich szybko jednak zamknęła działalność.
Obecnie ocenia się, że zostało wydanych ponad 6 tys. koncesji, a rynek ochrony liczy ponad 280 tys. pracowników ochrony. Jednak inaczej niż na dojrzałych rynkach zachodnich szacuje się, że jedynie do 35 proc. rynku znajduje się w rękach „wielkiej piątki" firm ochrony, natomiast pozostałe 65 proc. rynku to 99,99 proc. podmiotów. Na Zachodzie, w zależności od kraju, jedna firma potrafi skupić w swoim portfelu nawet do 80 proc. rynku (np. firma Falck w Danii).

Ochrona komercyjna w Polsce - diagnoza

Polski rynek ochrony jest zbyt rozdrobniony, niezbyt skonsolidowany, ze zbyt dużą liczbą podmiotów gospodarczych, co rzutuje na jego kondycję. Najgorszym przejawem tej sytuacji jest fakt, że przy takiej konkurencji ceny usług nieustannie spadają, a przedsiębiorcy robią wszystko, by pozyskać kontrakt, utrzymać się na rynku i jak najwięcej zarobić. Właśnie to jest powodem częstego występowania negatywnych zjawisk, takich jak nieuczciwa konkurencja, dumping cenowy, korupcja, zmowy, nieetyczne postępowanie pracodawców wobec pracowników ochrony, zatrudnianie niezgodne z prawem lub w tzw. szarej strefie, wykorzystywanie pieniędzy pozyskiwanych z PFRON do reperowania kondycji finansowej swoich przedsiębiorstw... Można by długo wymieniać.
Jestem gotów bronić tezy, że statystycznie rynek ochrony komercyjnej w Polsce jest w takiej samej sytuacji, w jakiej były państwowe przedsiębiorstwa PRL-u w latach 80. XX w. Mam tu na myśli wskaźnik zatrudnienia, marnotrawienie materiałów i zasobów oraz małą wydajność i skuteczność pracy.
Do końca ub.r. relatywnie tanie usługi ochrony fizycznej powodowały i potęgowały przekonanie, że ochrona to roboczogodziny przepracowane na obiekcie, czyli „armia" pracowników ochrony.

Statystyczny pracownik ochrony w Polsce

Według danych za 2016 r. roboczogodzina pracownika ochrony wyniosła 6–7 zł netto. Przyjmując zatem, że statystyczny pracownik ochrony przepracowuje średnio w miesiącu 240 roboczogodzin, jego wypłata wynosi 1560 zł. Ta praca (godzinowo porównywalna z 1,5 etatu) to zazwyczaj umowa zlecenie (bez urlopu i często bez możliwości zwolnienia lekarskiego), najczęściej w ciasnym i dusznym pomieszczeniu (np. w przyczepie kempingowej), a pracownik jest odpowiedzialny za mienie kontrahenta, niezależnie od pogody, dnia tygodnia czy święta, poddany stałej kontroli swoich przełożonych.
Jakie nastawienie do takiej pracy ma pracownik? Czy w takich warunkach i przy takim wynagrodzeniu można od niego wymagać uwagi, zaangażowania, chęci do podnoszenia swoich kwalifikacji i wykorzystywania ich w pracy? Czy taka praca zainteresuje osoby mogące wnieść jakieś wartości dodane do firmy, usługi, rynku? Większość zadań służb ochrony to pochodne, rozwinięcia i mutacje siedmiu podstawowych obowiązków *(patrz: ramka poniżej)*.

Paradoks polega także na tym, że zazwyczaj wszystkie działania wykonuje jednocześnie niewielka liczba pracowników ochrony, czasem tylko jeden, który dodatkowo musi rano zamieść lub odśnieżyć chodnik, wymienić przepalone żarówki i skosić trawnik. W tej sytuacji właściwa realizacja tych zadań jest fikcją. Na szczęście istnieje niewielki segment odbiorców usług (głównie korporacje zachodnie), które wchodząc na polski rynek z własnymi standardami, wymuszają na agencjach ochrony podejście do pracowników zgodne z ich standardami dotyczącymi wynagrodzeń, wizerunku, form zatrudnienia, podejścia do pracownika itp. Niestety to wciąż nieliczący się promil rynku.

PODSTAWOWE OBOWIĄZKI STATYSTYCZNEGO PRACOWNIKA OCHRONY

W zależności od rodzaju chronionego obiektu

1. *rejestracja i kontrola ruchu osobowego*, czyli wypisywanie, wydawanie i odbieranie przepustek, wypełnianie formularzy, druków, raportów, sprawdzanie przepustek z tożsamością osoby wchodzącej lub wychodzącej, kontrola bagaży, weryfikacja trzeźwości itp.;
2. *rejestracja i kontrola ruchu samochodowego* – w zasadzie wszystkie powyższe czynności w odniesieniu do pojazdów, a nie osób;
3. *rejestracja i kontrola ruchu towarowego* – jw.;
4. *patrol obiektu chronionego* – przejście wyznaczoną trasą, w wyznaczonym interwale czasowym, stawianie się w określonych miejscach obiektu i „meldowanie się" w punktach kontrolnych systemu kontroli obchodu;
5. *nadzór nad systemami zabezpieczeń technicznych* (systemy telewizji dozorowej, kontroli dostępu, włamania i napadu, ppoż.) – głównie obserwacja obrazu na monitorach i wyświetlaczach poszczególnych systemów;
6. *raportowanie* do osób odpowiedzialnych w chronionym obiekcie i swoich przełożonych, a w razie konieczności – współpraca z właściwymi służbami państwowymi;
7. *podejmowanie interwencji* zgodnie z ustaloną procedurą działania w przypadkach tego wymagających (incydenty: włamanie, napad, pożar, zalanie lub inna sytuacja kryzysowa), mającej na celu minimalizowanie strat i ujęcie sprawcy.

Proces zastępowania poszczególnych funkcji ochrony fizycznej zaczął nabierać tempa. Pojawiły się zaawansowane systemy telewizji dozorowej, kontroli dostępu, sygnalizacji włamania i napadu, platformy integrujące...

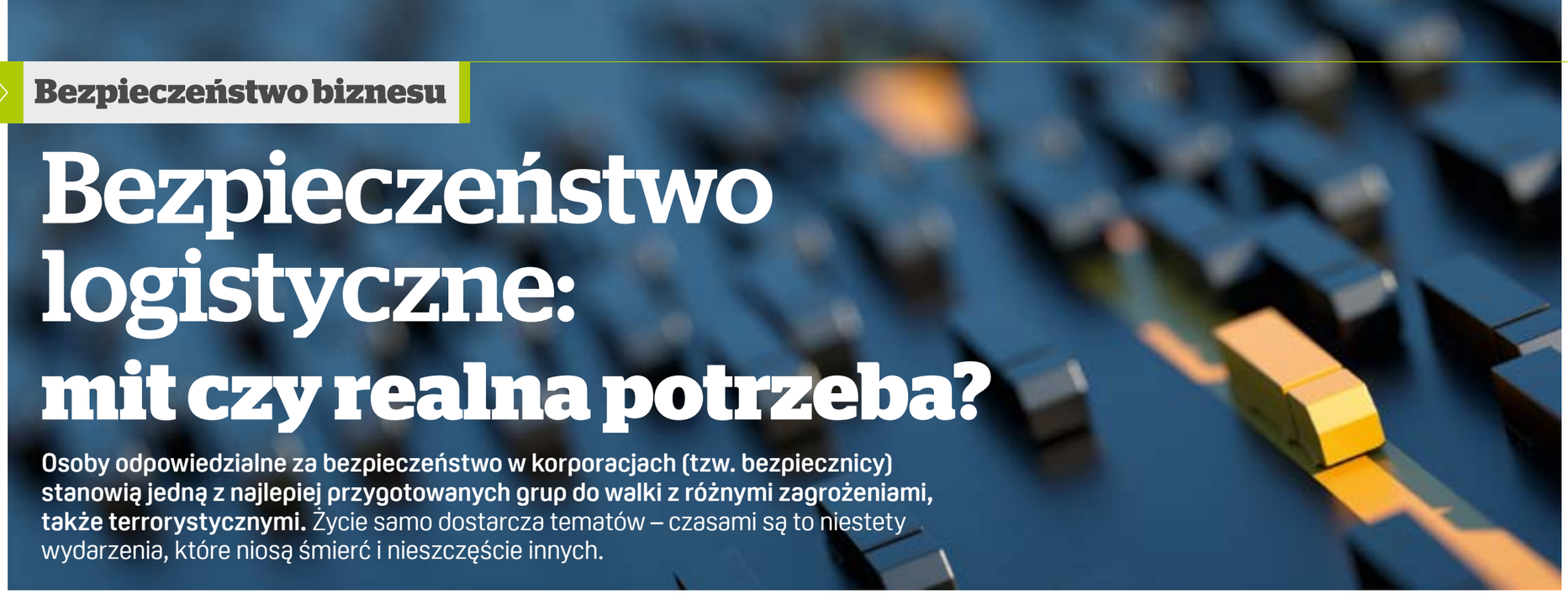
Ochrona komercyjna w Polsce – technikalia

Od początku istnienia komercyjnej branży ochrony osób i mienia w Polsce pracownicy mieli dość szeroki dostęp do narzędzi pracy. Dostęp ten był limitowany (i nadal jest) specyfiką obiektu, wymaganiami i/lub życzeniami klienta oraz ceną.
Na początku były to prymitywne systemy kontroli obchodu, broń i środki przymusu bezpośredniego, rzadziej analogowe systemy telewizji dozorowej, kontroli dostępu, włamania i napadu. W związku z ich wysokim kosztem i niską jakością były to narzędzia rzadko wykorzystywane – jedynie systemy włamania i napadu od początku były instalowane w wielu obiektach.
W pierwszej dekadzie XXI w. rozpoczął się widoczny wyścig producentów zabezpieczeń technicznych, co sprawiło, że stały się one bardziej funkcjonalne, dostępne cenowo, skuteczniejsze i bardziej atrakcyjne dla odbiorcy końcowego. Pojawiły się też pierwsze nieśmiałe zapowiedzi trendu, który w Europie Zachodniej nabierał tempa od wielu lat – zastępowania techniką części funkcji realizowanych przez pracowników ochrony.
Przy czym – co może wydawać się dziwne i niezrozumiałe – w efekcie instalacji nowej techniki zabezpieczenia rzadko redukowano na rynku polskim posterunki ochronne czy ograniczano ich godziny funkcjonowania w chronionych obiektach. Pojawiły się pierwsze centra monitorowania będące zalążkiem obecnych centrów zarządzania ochroną obiektu. W zasadzie każdy duży lub skomplikowany obiekt posiadał już własny monitoring z obsadą osobową, procedurami działania, łącznością z resztą zespołu ochronnego, a pozycja operatora CCTV była umieszczana w strukturach jako podległa jedynie szefom ochrony i kierownikom zmian. Nadal podstawą ochrony był jednak ochroniarz (zwany także strażnikiem lub wartownikiem), którego praca polegała na wypełnianiu dokumentacji papierowej – dziesiątek, setek, a nawet tysięcy ton raportów, których nikt nie czytał, nie analizował i prawdę mówiąc, nie potrzebował. Jego obecność na posterunku stanowiła wówczas gwarancję bezpieczeństwa.
Od początku XXI w. proces zastępowania poszczególnych funkcji ochrony fizycznej zaczął nabierać tempa. Pojawiły się zaawansowane systemy telewizji dozorowej, kontroli dostępu, sygnalizacji włamania i napadu, a (co najistotniejsze) platformy integrujące, oprogramowanie analityczne, oprogramowania CRM przeznaczone dla branży ochrony, aplikacje mobilne itp.
Obecnie systemy zabezpieczeń technicznych, oprócz swoich podstawowych funkcji, zapewniają:
- usprawnienie pracy każdego posterunku ochronnego i kontrolowanie pracownika ochrony realizującego zadania ochronne,
- zastąpienie dużej części zadań realizowanych przez pracowników ochrony,
- analizę zaistniałej sytuacji (z sugerowanym rozwiązaniem) oraz wskazanie operatorowi określonego procedurą działania (łącznie z automatycznym raportowaniem braku działania operatora w określonym czasie).

BIO

Krzysztof Moszyński
Analityk, audytor, konsultant w zakresie systemów bezpieczeństwa i ochrony. Od 2008 r. pracuje w firmie ochrony Konsalnet, obecnie jako dyrektor ds. rozwiązań systemowych.

W kolejnym wydaniu „a&s Polska" opublikujemy 2. część artykułu, w której opiszemy kierunki rozwoju agencji ochrony osób i mienia oraz trendy panujące na tym rynku.



Bezpieczeństwo logistyczne: mit czy realna potrzeba?

Osoby odpowiedzialne za bezpieczeństwo w korporacjach (tzw. bezpiecznicy) stanowią jedną z najlepiej przygotowanych grup do walki z różnymi zagrożeniami, także terrorystycznymi. Życie samo dostarcza tematów – czasami są to niestety wydarzenia, które niosą śmierć i nieszczęście innych.

Sebastian Błażkiewicz
prezes SASMA

Zanim omówię, czym zajmuje się bezpieczeństwo logistyczne i jak ważną część bezpieczeństwa biznesu stanowi, przywołam przykład: 19 grudnia ub.r. ciężarówka na polskich numerach rejestracyjnych wjechała w jarmark bożonarodzeniowy w Berlinie. Zginęło 12 osób, ponad 50 zostało rannych.
Można przyjąć, że wszystko już na ten temat powiedziano, różni eksperci jednoznacznie wskazywali winnych, mówiąc, że można się było tego spodziewać, a służby znowu zawiodły.
Nie chcąc komentować tych opinii, naświetlę temat z innej strony, stawiając pytanie: **czy można było temu zapobiec?**

Najpierw fakty (na podstawie przekazów medialnych i wywiadów z właścicielem firmy transportowej):
- godz. 15.00 – ostatni kontakt z kierowcą (rozmowa telefoniczna z żoną),
- godz. 15.44–19.44 – próby uruchomienia samochodu i jazdy,
- godz. 20.15 – zamach.

Pomiędzy pierwszym odpaleniem silnika a zamachem minęło 4,5 godz. Należy wspomnieć, że auto czekało na rozładunek i żadna jazda nie była już planowana (tak poinformował właściciel firmy). Co można w takim czasie zrobić i jak powinien zareagować system bezpieczeństwa logistycznego?
Każda ciężarówka ma system GPS – to nic nowego, ale jego obecność ma sens tylko wtedy, gdy ktoś je monitoruje w czasie rzeczywistym (tzw. monitoring aktywny). Muszą też być opracowane procedury na wypadek najgorszego, inaczej staje się on drogą zabawką.
W działającym systemie bezpieczeństwa logistycznego przy pierwszej próbie uruchomienia auta powinien pojawić się sygnał informacyjny w stacji monitoringu (zna ona rozkład jazdy pojazdu i wie, że w tym momencie zaplanowano postój), a operator powinien podjąć próbę kontaktu z kierowcą.
Przy nieskutecznej próbie należałoby włączyć mikrofony i kamery w kabinie, by sprawdzić, co się w niej dzieje. Gdyby wspomnianych kamer i mikrofonów nie było w danym samochodzie, nastąpiłaby druga próba kontaktu z kierowcą, także w omawianym przypadku nieskuteczna.
Równocześnie z próbami połączenia telefonicznego wg procedur powinna nastąpić próba kontaktu poprzez e-mail, SMS, Messenger z prośbą o pilną odpowiedź. Takiego modelu postępowania uczy się kierowców podczas szkoleń, które należy przeprowadzać cyklicznie. Pomagają minimalizować ryzyka oraz uświadamiają im potrzebę stałego kontaktu z centrum monitoringu.
Jeśli i te próby się nie powiodą, stacja monitoringu powinna powiadomić agencję ochrony, z którą ma podpisaną umowę na tzw. interwencję w danym kraju czy obszarze. Z reguły czas reakcji grupy interwencyjnej w ciągu dnia wynosi ok. 20 min, a to wystarczająco dużo. W razie braku kontaktu z kierowcą centrum monitoringu może też zadzwonić bezpośrednio na policję. Po wydarzeniach w Nicei nie sądzę, by jakikolwiek funkcjonariusz zbagatelizował sygnał o problemach z ciężarówką.
Równocześnie z powiadomieniem agencji ochrony lub policji należy zdalnie zablokować zapłon (duża część aut ma taką blokadę).
Wszystkie te działania nie powinny zająć więcej niż 20 minut. Otwarte pozostaje więc pytanie: **czy ludzi, którzy zginęli w Berlinie, można było ocalić?**
Oczywiście, taki system funkcjonuje w dużych i dojrzałych firmach czy korporacjach logistycznych. Mniejsze firmy lokalne, „liczące każdy grosz", nie mają takich rozwiązań ze względu na koszty i brak szkoleń lub po prostu nie wiedzą, że istnieją firmy doradcze w tym zakresie. Tylko czy można wycenić koszt życia ludzkiego?
Chcę zaznaczyć, że mój komentarz nie ma na celu wskazania winnych czy oskarżania. Chcę pokazać, że nie jesteśmy bezbronni w takich sytuacjach i od dawna są procedury minimalizujące także ryzyko ataków.
Już w 2007 r. uczestniczyłem w szkoleniu, na którym ćwiczyliśmy przejęcie ciężarówki z zamiarem użycia jej jako broni. Na pewno nie byłem pierwszy, który takie szkolenie odbył.
Ponad 65 proc. wszystkich towarów transportuje się ciężarówkami, dlatego skupię się na związanych z nimi wyzwaniach oraz bezpieczeństwie magazynów logistycznych.

> Pseudodoradcy twierdzący, że ich działania są skuteczne, ale tak tajne, że nie można ich potwierdzić, narażają klienta na straty finansowe.

Liczba napadów na ciężarówki i włamań do magazynów stale rośnie. Wprawdzie nie ma jednej statystyki, ale bazując na danych cząstkowych, można przyjąć, że straty są liczone w setkach mln euro rocznie. Najczęściej kradzione są towary łatwo zbywalne – dla złodzieja najatrakcyjniejszy łup to taki, który można szybko sprzedać. Są to: papierosy, sprzęt RTV/AGD, komputery, telefony komórkowe, perfumy, leki, alkohol, luksusowe towary spożywcze (np. kawa), napoje i odzież.
Jak zatem powinien wyglądać system bezpieczeństwa logistycznego? Ułatwieniem może być standard wprowadzony przez organizację bezpieczeństwa logistycznego TAPA EMEA, dotyczący bezpieczeństwa ładunków przewożonych ciężarówkami i magazynowanych (TSR/FSR).
Taki system powinien być „zintegrowany", co w tym przypadku oznacza połączenie bezpieczeństwa fizycznego, systemów teleinformatycznych i zabezpieczeń technicznych oraz procedur, szkoleń, audytów i postępowań wyjaśniających.
Jeśli te elementy działają prawidłowo, jest duża szansa na zminimalizowanie ryzyka, choć wiadomo – nie ma w pełni bezpiecznego systemu.
System działa sprawnie w dojrzałych korporacjach czy firmach transportowych, w których zajmują się tym wewnętrzne działy bezpieczeństwa wspierane przez agencje ochrony i firmy z zakresu bezpieczeństwa biznesu.
W przypadku mniejszych firm często problemem są kwestie finansowe (budowa systemu bezpieczeństwa i zarządzanie nim kosztuje) oraz świadomość właścicieli firm transportowych, którzy nie wiedzą, że istnieją na rynku wyspecjalizowane podmioty, które mogą pomóc zbudować taki system.
Ważne, by korzystać z usług wyspecjalizowanych firm doradczych, które mają referencje w danym zakresie.
Pseudodoradcy twierdzący, że ich działania są skuteczne, ale tak tajne, że nie można ich potwierdzić, narażają potencjalnego klienta na straty finansowe.

BIO

Sebastian Błażkiewicz
Praktyk z wieloletnim doświadczeniem w branży bezpieczeństwa biznesu w Polsce i zagranicą, zajmuje się różnymi aspektami zapewnienia bezpieczeństwa w działaniu międzynarodowych korporacji.

BEZPIECZEŃSTWO FIZYCZNE

Ochrona (zapewniana najczęściej przez firmy zewnętrzne), której zadaniem jest nadzór nad magazynem, gdzie są składowane nasze towary, oraz grupy interwencyjne, które reagują w przypadku sygnału alarmu ze stacji monitoringu lub przycisku antynapadowego kierowcy.

SYSTEMY BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

- *w przypadku ciągników/naczep* – głównie GPS, mikrofony i kamery w kabinie, przycisk antynapadowy, stacja monitoringu oraz oprogramowanie, które ma m.in. funkcję detekcji użycia zagłuszarek GPS (coraz częstszy sposób ataków na TIR-y), detekcja zjazdu z zakodowanej trasy czy nieautoryzowane próby włączenia samochodu (inny czas lub lokalizacja niż zakodowane), zdalna blokada zapłonu (możliwa tylko w czasie postoju).

SYSTEMY ZABEZPIECZEŃ TECHNICZNYCH

- *w przypadku ciągników/naczep* – głównie różnego rodzaju zamki i sztaby chroniące naczepy przed nieautoryzowanym otwarciem, bardzo często wyposażone w zamki i plomby elektroniczne, których działanie jest stale nadzorowane przez stację monitoringu;
- *w przypadku magazynów* – kamery telewizji dozorowej, czujki ruchu, systemy kontroli dostępu, sygnalizacji pożarowej, sygnalizacji włamania i napadu – wszystko zintegrowane i stale monitorowane.

PROCEDURY

Powinny obejmować wszystkie wymagane działania. Jeśli jednak wystąpią problemy, należy spokojnie reagować na kryzys.

Procedury muszą być regularnie testowane i weryfikowane pod kątem aktualności zawartych w nich założeń. W tym zakresie pomocą służy organizacja TAPA EMEA, która podaje, jakie konkretne procedury są wymagane.

SZKOLENIA

Człowiek był, jest i będzie najsłabszym ogniwem systemu bezpieczeństwa, stąd tak ważne są regularne szkolenia. Powinny odbywać się cyklicznie i obejmować nie tylko nowych pracowników, ale także:
- *kierowców* (szkolenia w zakresie minimalizowania ryzyka oraz zachowania w sytuacjach kryzysowych),
- *pracowników stacji monitoringu* (prawidłowe reakcje na sygnały),
- *pracowników ochrony magazynów*,
- *spedytorów*.

AUDYTY

- *w przypadku ciągników/naczep* – audyty tras (główna i alternatywna), parkingów (tu jest najwięcej kradzieży), postępowania wyjaśniające w przypadku napadu oraz ustalenie i schwytanie sprawców (wspólnie z policją);
- *w przypadku magazynów* – audyty magazynów (kompleksowe), procedur awizacji, przyjmowania i wydawania towarów, postępowania wyjaśniające w przypadku kradzieży towarów oraz ustalenie i schwytanie sprawców (wspólnie z policją).

Aby biznes mógł się rozwijać zgodnie z oczekiwaniami, wymaga wielu czynników, wśród których istotny jest poziom bezpieczeństwa. **Bezpieczeństwo jest dla biznesu niezbędne, a jednocześnie niezauważalne.**

COŚ SIĘ ZMIENIŁO

CZYLI O...

ZALETACH ŻYCIA W CIEKAWYCH CZASACH

Janusz Syrówka
innogy Polska

Dotychczas w naszym kręgu kulturowym i geograficznym było na tyle bezpiecznie, że nie trzeba było o tym myśleć, a co dopiero w to inwestować. Te czasy jednak właśnie minęły. Musimy przyjąć, że problemy już tu są i zagrażają nam niemal z każdej strony. Mechanizmy rynkowe powodują, że dobra deficytowe są w cenie. W niepewnych czasach towar o nazwie „bezpieczeństwo" staje się coraz trudniej dostępny.

Cyberbezpieczeństwo

Ostatnio odmieniane przez wszystkie przypadki – konferencje o cyberbezpieczeństwie, spotkania, szkolenia. Zaangażowanie władz i informacje medialne o atakach hakerskich świadczą, że coś jest na rzeczy. Co konkretnie? Zostawmy zmagania wielkich graczy, ataki na elektrownie, wyłączanie prądu w całym kraju czy kradzieże technologii wojskowych. W to są zaangażowane państwa ze swoimi specsłużbami. Skupmy się na funkcjonowaniu biznesu.
To nie przestępczość cyfrowa jest nowym zjawiskiem. Nowym zjawiskiem jest zmiana stylu naszego życia. Nawet nie zauważyliśmy, kiedy zostaliśmy podłączeni cyfrowym łączem do sieci wzajemnych powiązań. Przestępcy z tego korzystają, a uczciwi ludzie w obliczu zagrożenia cyberprzestępczością muszą zmienić swoje obyczaje.
Czytałem kiedyś fascynujący artykuł o „wojnie" między włamywaczami a producentami kas pancernych i zamków w XIX-wiecznej Anglii. Współcześni odbierali to jako wyścig nowoczesnych technologii. Dzisiaj z tamtej kasiarskiej technologii możemy się śmiać, jednak schodząc do poziomu motywacji: jednej strona chce ukraść pieniądze, druga – nie dać się okraść. Dawniej było jednak o tyle łatwiej, że z sejfem złodziej musiał się zmierzyć fizycznie. Dziś nawet środki na koncie są wirtualne...
Cokolwiek zrobimy w zakresie cyberbezpieczeństwa, musimy pamiętać o prawdziwych motywacjach. A te są tak stare, jak ludzkość. Musimy, rzecz jasna, nadążać z zabezpieczeniami technicznymi, trzeba jednak pamiętać, że atakuje człowiek. Nadal obowiązuje też zasada, że jeśli sejf jest zbyt mocny, to zaatakowane zostanie najsłabsze ogniwo – człowiek, który trzyma do niego klucz.
Przed odpowiedzialnymi za bezpieczeństwo IT stoi dziś karkołomne wyzwanie połączenia ognia z wodą. Z jednej strony mamy wolność, swobodę, elastyczność i efektywność korzystania z najnowszych technologii – zdalna praca, rozwiązania chmurowe czy Internet Rzeczy to zupełnie nowa jakość prowadzenia biznesu. Z drugiej – zasady bezpieczeństwa stają temu na drodze: reguły bezpieczeństwa ograniczają korzystanie z wielu opcji. Wszystko to przyprawia brzydką „gębę" idei bezpieczeństwa. Jedno jest pewne – zamykanie w dyby reguł bezpieczeństwa jest skazane na porażkę. Należy kierować się zdrowym rozsądkiem i uświadamiać innych.
Problemem jest zmiana sposobu myślenia o cyberbezpieczeństwie. To pojęcie nie jest wirtualne, ale jak najbardziej realne. Potrzebne jest kompleksowe spojrzenie, które pozwoli dostrzec ważny komponent fizyczny. Kwestie systemowe bez fizycznego zabezpieczenia zasobów wirtualnych tracą na znaczeniu. Infekowanie złośliwym oprogramowaniem jest równie groźne jak fizyczna ingerencja w sieć czy sabotaż serwerów bądź destrukcja przechowywanych danych.
Specjaliści dbający o cyberbezpieczeństwo muszą od nowa zdefiniować swoją rolę, rozumieć wymogi przeciwstawiania się wirtualnym zagrożeniom, a jednocześnie szerzej pojmować zagrożenia, także te o charakterze niecyfrowym. Wyzwaniem będzie też umiejętność mówienia o sprawach technologicznych do zwykłych ludzi i przekonywanie do rozwiązań, które nie należą do najbardziej przyjaznych użytkownikom. A to właśnie oni powinni tworzyć odpowiednio skomplikowane hasła, regularnie je zmieniać i stosować różne wersje do różnych zastosowań.

Człowiek vs. maszyna

O przewadze maszyny nad człowiekiem w sektorze bezpieczeństwa dyskutuje się od dawna.
Nie ma wątpliwości, że wiele zadań maszyna wykona lepiej: nie męczy się, nie śpi, niczego nie przeoczy. Do niedawna była jednak droższa. Zmiany na rynku pracy i nowe regulacje dot. wynagrodzeń powodują, że dotychczasowe kalkulacje przestają obowiązywać. Tym bardziej jeśli dodać do tego postęp technologiczny i dostępność wielu usprawnień.
Mam wrażenie, że istnieją obecnie dwie bariery dla masowego wspierania pracy człowieka przez systemy. Pierwsza jest natury technicznej i tymczasowa – nikt rozsądny nie wyrzuci, ot tak, posiadanych narzędzi tylko po to, by zastąpić je nowymi. Należy opracować plan rozłożony w czasie, znajdując na ten cel środki – to trudne, ale wykonalne. Druga bariera jest znacznie trudniejsza do pokonania. To brak świadomości, brak wizji, brak wyobraźni... Typowo fordowska sytuacja – nie można ulepszać konia, zamiast budować samochód. Nie chodzi o dosłowne zastępowanie człowieka, istotą jest znalezienie obszarów do zagospodarowania przez maszyny. Pierwsze będą zapewne czynności proste, np. odźwierni, operatorzy szlabanów i inni, którzy dziś są kojarzeni z obszarem bezpieczeństwa. Zmiana ta nie będzie postrzegana jako nowinka technologiczna, lecz konieczność wymuszona przez warunki ekonomiczne.

> Nie ma wątpliwości, że wiele zadań maszyna wykona lepiej: nie męczy się, nie śpi, niczego nie przeoczy. Do niedawna była jednak droższa.

Stare nowe zagrożenia

Zmieni się także tzw. bezpieczeństwo publiczne. Zagrożenia terrorystyczne są coraz bliżej naszych granic, a niepokoje społeczne o charakterze politycznym czy związane z kryzysem imigracyjnym nie są już wyłącznie rozważaniami teoretycznymi. Powstaje nowy obszar aktywności o bezpieczeństwie biznesu, który musi zapewnić przetrwanie w warunkach niepokoju. Zarządzanie kryzysowe i zapewnienie ciągłości działania przerodzą się w „żywy" proces biznesowy i wyjdą z hibernacji, jakiej je poddano, umieszczając w formie nieczytanych przez nikogo planów w zakurzonych segregatorach.
Do niedawna termin „bezpieczeństwo podróży" wywoływał w naszym kraju uśmiech politowania. Był odbierany jako kreatywna metoda na „wyciśnięcie" z firm kolejnych pieniędzy. Czy dzisiaj można to bagatelizować? Bezpieczeństwo pracowników w podróży służbowej nie jest ekstrawagancją, a dotyczy zarówno prezesa, jak i kierowcy ciężarówki. Okazuje się, że o tym aspekcie trzeba myśleć nie tylko w odniesieniu do podróży do Kabulu, ale także do Berlina...

Co na to biznes?

Bezpieczeństwo biznesu wymaga zdefiniowania na nowo. Powodem nie jest kumulacja nowych zagrożeń, ale sam biznes. Zmiany dokonujące się w strukturach firm niosą wiele konsekwencji, mających ogromny wpływ na bezpieczeństwo. Zmiany te w jakimś stopniu są kreowane przez nowe pokolenie pracowników, które tworzy nowe reguły. Otoczenie biznesu wraz ze swoimi „wrogimi" elementami nie różnicuje firm według sposobu ich zarządzania (tradycyjny czy nowatorski). Organizacja hierarchiczna z mocno sformalizowaną strukturą jest tak samo narażona na zagrożenia jak płaska hierarchicznie i nieformalna organizacja „turkusowa" (bez szefa). Jednak sposoby zapewniania bezpieczeństwa w obu organizacjach będą zupełnie inne.
Odpowiedzialni za bezpieczeństwo biznesu muszą wykształcić cechy, które wcześniej nie były brane pod uwagę. Bycie fachowcem to dziś zdecydowanie za mało. Zamiast dawnego „wdrażania" bezpieczeństwa musi pojawić się coś nowego – „pozyskiwanie" do bezpieczeństwa. Procedura uchwalona przez zarząd i rozesłana z poleceniem stosowania zwyczajnie nie zadziała. Bo jak ma zadziałać, gdy część pracowników jest zatrudniona na umowę o pracę, a część to niezależni eksperci na równorzędnych stanowiskach. Współpracują oni z wieloma firmami, które pozostałych pracowników i usługi pozyskują od dostawców zewnętrznych. Nie zapominajmy też o sporej grupie „wolnych strzelców" angażowanych *ad hoc* do projektów. Często firma nie ma też stałej siedziby (jedynie biuro współdzielone), a wszyscy funkcjonują na zasadzie *home office*. Czy to brzmi jak koszmar? To rzeczywistość wymagająca dostosowanych do niej rozwiązań.
Dotychczas dużo mówiło się o działaniu prewencyjnym, że każda złotówka wydana na bezpieczeństwo z pewnością się zwróci. Rzeczywiście, mówiło się dużo, ale niewiele robiło...
Dziś świat działa szybciej, a każda luka w murze bezpieczeństwa jest błyskawicznie odkrywana i wykorzystywana.
Doniesienia medialne nie nastrajają optymistycznie. Spokój, jaki panował w naszym regionie jeszcze nie tak dawno, prysnął jak bańka mydlana. Powstały nowe warunki, w których musimy nauczyć się funkcjonować. Tylko od nas zależy, czy życie w „ciekawych czasach" będzie przekleństwem, czy szansą.

BIO

Janusz Syrówka
Ekspert ds. *corporate security,* twórca wdrożeń systemów bezpieczeństwa. Specjalizuje się m.in. w *loss prevention,* bezp. informacji i procesów operacyjnych, zarządzaniu kryzysowym.

OBNIŻYSZ KOSZTY, UNIKAJĄC OSZUSTÓW

Dzisiaj oszuści potrafią wcielić się w przedstawicieli różnych profesji i firm, do realizacji swoich planów wykorzystując pośpiech i obciążenie pracą potencjalnych ofiar. Mogą się także podszyć pod każdego z nas, oszukując naszych kontrahentów i pracowników. **Czujność jest więc zawsze wysoce wskazana i po jakimś czasie wchodzi w krew.**

Michał Czuma

Opowieści o oszustwach są często odbierane jako anegdoty, a nie przestroga i zapowiedź tego, co może spotkać każdego...

Na targach żywności w Amsterdamie do firmy produkującej wodę podszedł dobrze ubrany, świetnie mówiący po angielsku rzekomy (jak się później okazało) kupiec jednego z dużych brytyjskich detalistów. Zostawił wizytówkę, a później e-mailem umówił transport. Woda w Wielkiej Brytanii jednak wyparowała, a wraz z nią kilkadziesiąt tysięcy funtów – opisuje Leszek Banaszak z Wydziału Promocji i Handlu polskiej ambasady w Londynie.

◆◆◆

Pewnego razu z firmy, od której wypożyczam samochody, zgłosił się pracownik chcący w naszych autach służbowych zamontować wieszaki na marynarkę. Był zdziwiony, gdy poprosiłem go o dokument potwierdzający, że jest przedstawicielem tej firmy. Ja jednak nie zapomniałem historii, kiedy to w podobny sposób mojemu klientowi ukradziono połowę jego floty. „Pan z wypożyczalni" był jeszcze bardziej zdziwiony, gdy zadzwoniłem do jego szefa, by potwierdzić oddelegowanie go do wykonania tego zlecenia.

◆◆◆

Niedawno zadzwoniła do mnie pani, która poinformowała mnie, że dzwoni z banku, w którym mam rachunek. Miłym głosem wyrecytowała swoją kwestię: „Proszę o podanie imienia, nazwiska i nazwiska panieńskiego matki celem identyfikacji". Tym razem nie odmówiłem przekazania jej tych informacji, jak robię to w większości przypadków, wiedząc, że podając swoje dane, można w kilka chwil stracić wszystkie pieniądze z konta. Skojarzyłem bowiem, że dzień wcześniej dokonałem transakcji zagranicą, a bank zapewne chce potwierdzić, czy to ja wydałem kilkaset dolarów, a nie oszust posługujący się moimi danymi lub kartą.

Żyjemy w czasach, w których oszustwo stało się doskonałym sposobem na osiągnięcie niebotycznych zysków przy niewielkim poziomie ryzyka. Każde zainwestowane 1000 zł w ciągu miesiąca może zapewnić nawet 30 tys. zł. Mistrzowie w tym fachu potrafią pomnożyć w ciągu jednego dnia 100 zł o 10 tys. procent. O takich zyskach mogą zapomnieć nawet najbardziej sprawni lichwiarze.
Straty, jakie ponosi statystyczna polska firma z tytułu oszustw, wynoszą 3–8 proc. jej obrotów. Oszustwa dotykają każdego – w zależności od branży i stopnia zastosowanych zabezpieczeń antyfraudowych szacuje się, że 78–94 proc. firm w Polsce jest regularnie okradanych w wyniku oszustw zarówno wewnętrznych (przez pracowników), jak i zewnętrznych. Około 62 proc. pracodawców twierdzi, że się przed tym broni. Gdy jednak dochodzi do poważnych strat, zabezpieczenia przed nieuczciwymi pracownikami czy kontrahentami okazują się nieskuteczne.

> Oszustwo stało się doskonałym sposobem na osiągnięcie niebotycznych zysków przy niewielkim poziomie ryzyka.

Firmy dotknięte oszustwem zazwyczaj poszukują kolejnego specjalisty ds. bezpieczeństwa. Niektórzy właściciele czują się bezradni, ale boją się głośno powiedzieć o swoim problemie, by nie nadszarpnąć wizerunku firmy. A przecież przeciwdziałanie wyłudzeniom pozwala na szybkie obniżenie kosztów i wypracowanie dodatkowych zysków. Czekanie na wielomilionowe straty wynikające z czyjejś nieuwagi lub wyjątkowego sprytu oszustów specjalizujących się w tym procederze nie jest dobrym wyjściem. Przestępcy, bogacąc się, stosują coraz bardziej wyrafinowane metody i kosztowne narzędzia wyłudzeń. Wtedy już nie można mówić o drobnym cwaniaczku, ale o groźnej korporacji przestępczej.
Z ciekawością słucham opowieści o klientach, uczciwych i majętnych przedsiębiorcach, dysponujących bardzo drogą flotą limuzyn. I wciąż mam w pamięci historię zaginięcia leasingowanych ciągników siodłowych, które zniknęły po przekroczeniu południowej granicy UE i przepadły na zawsze wraz z przewożonym towarem. Nawet w śledztwie prowadzonym we współpracy z ABW nie zdołano ustalić losu kilkunastu zestawów. Co się stało, przecież firma działała w Polsce i miała właścicieli? Owszem, miała... Nawet złożyli obszerne wyjaśnienia na policji, ale po przesłuchaniu okazali się tzw. słupami. Byli zdziwieni, że *w firmach, które pozwolili uruchomić znajomym za 3 tys. zł, ktoś wynajął tyle ciężarówek.*

Czasy się zmieniają, zmienia się też otoczenie biznesowe i warunki na rynku. Aby się rozwijać, należy zarówno zadbać o nowe działania biznesowe, jak i inwestować w zabezpieczenie przed oszustami. W obu przypadkach warto podejść do tematu profesjonalnie. Jeśli robi się to nieostrożnie lub nie podejmuje żadnych działań, trzeba się liczyć ze stratami.

BIO

Michał Czuma
Prezes i współwłaściciel G+C Kancelaria Doradców Biznesowych. Wcześniej stworzył i zarządzał pierwszymi w kraju Biurami Antyfraudowymi w spółkach grupy PKO BP. Były wieloletni z-ca dyrektora Departamentu Bezpieczeństwa PKO BP.

10 ZASAD JAK ZADBAĆ O BEZPIECZEŃSTWO SWOJEJ FIRMY

Każdy powinien dbać o swój majątek i nie dać się oszukać przez kontrahenta, wspólnika, klienta czy firmę, w której zamówił towar lub dostawę albo której wysłał swoje wyroby. Mając to na względzie, warto podjąć rozsądne i niezbyt kosztowne działania.

1. Współpraca ze sprawdzonymi klientami nie stanowi gwarancji bezpieczeństwa. Wielu oszustów, znając ich bazę, może się pod nich podszyć albo przejąć zlecenia lub towar (czasami we współpracy z pracownikami firmy, która stanowi ich cel). Oszuści udają wiarygodnych klientów, realizują kilka zleceń na mniejsze kwoty po to, by awansować do grona „klientów VIP". Później dokonują „skoku" na dużą kwotę i wszystko, co wydali na poprzednie zlecenia, zwraca się im z nawiązką. Należy więc monitorować, co robią klienci, i reagować na każdą zmianę w ich zachowaniu i praktykach. Można w tym zakresie skorzystać z firmy wyspecjalizowanej w tego typu usługach.
2. Kolejne działania polegają na zweryfikowaniu każdego nowego kontrahenta, czyli sprawdzeniu jego dokumentów. Nie dysponując własną komórką antyfraudową, należy poszukać odpowiedniej osoby lub wynająć firmę specjalistyczną. Nie można polegać tylko i wyłącznie na pierwszym wrażeniu nowego klienta.
3. Monitorowanie pojazdów, sprawdzanie delegacji, kosztów zakupów, kontrolowanie pracowników na różnych stanowiskach – o tym nie może zapomnieć właściciel firmy, któremu na sercu leży nie tylko jej dobro, ale także zysk finansowy. Po prostu: ufaj, ale kontroluj.
4. Ulubionym dniem oszustów jest piątek. Tuż przed weekendem pracownicy zazwyczaj myślą już o odpoczynku, mniej angażują się w wykonywanie zadań służbowych, spada poziom ich koncentracji. I to właśnie ten dzień tygodnia jest wręcz idealny do robienia przekrętów.
5. Niskie stawki również powinny być sygnałem do zastanowienia. Niestety często to, co jest tanie, może okazać się nierzetelne lub nieuczciwe. Należy analizować też ceny zakupu, które mogą okazać się bezpodstawnie wysokie.
6. Zasada, której nie powinien nikt pomijać, dotyczy każdorazowego sprawdzania numerów kont odbiorców. Oszust bowiem może podłożyć sfałszowaną fakturę z innym numerem konta. Niestety nie można również w pełni ufać pracownikom działu księgowego, którzy mogą dać do podpisu polecenie przelewu z numerem prywatnego konta.
7. Statystyki wskazują, że oszuści najczęściej pochodzą z Bułgarii, Rumunii, Słowenii, Węgier i Włoch. Dlatego zlecając transport, warto zachować czujność przy podejmowaniu współpracy z firmami z tych państw.
8. Każdy lubi okazje. Jednak korzystając z nich, należy pamiętać, by wcześniej sprawdzić je wyjątkowo czujnie i skrupulatnie.
9. Należy unikać propozycji, które mogą prowadzić do złamania prawa. Wprowadzanie w obieg fałszywych faktur wcześniej czy później skończy się dotkliwymi karami, i to nie tylko finansowymi.
10. Przepisy prawa zmieniają się w szybkim tempie. Jego aktualizacje muszą być na bieżąco wprowadzane w dokumentach firmy. Brak kontroli w tym zakresie (np. sprawdzanie, czy pracownicy nie działają na szkodę skarbu państwa lub współpracują z oszustami) może skończyć się przeprowadzeniem kontroli krzyżowych urzędu skarbowego i podjęciem działań policji. Aby do tego nie dopuścić, warto zaangażować specjalistę, który zadba o bezpieczeństwo biznesu.

Sprzedaż podrabianych towarów to problem, który dotyka coraz więcej firm z różnych branż. Lawinowo rosnąca liczba tego typu nadużyć sprawia, że ich kontrola jest nierozerwalną częścią polityki bezpieczeństwa czołowych firm na świecie.

BRAND PROTECTION

OPŁACALNA INWESTYCJA CZY NIEPOTRZEBNY KOSZT?

Agnieszka Socha
SASMA

W dobie globalizacji ofiarami tego typu przestępstw są nie tylko firmy produkcyjne. Rozwój handlu internetowego przyczynił się do zwiększenia możliwości sprzedaży podrobionych towarów. Zagadnienia ochrony marki i walki z podróbkami to tematy, które należy uwzględnić w tworzeniu skutecznego systemu bezpieczeństwa firmy i poświęcić im coraz więcej uwagi.

Aby ukazać skalę problemu i jego realny wpływ na gospodarkę, należy przytoczyć kilka danych zaprezentowanych przez unijny Urząd ds. Własności Intelektualnej. Badania na temat światowego handlu podrobionymi produktami pozwoliły pozyskać informacje dotyczące liczby oraz wartości podrabianych produktów, a także zakresu i kierunku ich rozprzestrzeniania. Podrabia się produkty z różnych branż, począwszy od towarów luksusowych, takich jak ekskluzywna odzież, kosmetyki, biżuteria czy zegarki, przez produkty pośrednie, np. maszyny, części zamienne lub środki chemiczne, kończąc na dobrach konsumpcyjnych, które mają realny wpływ na zdrowie i bezpieczeństwo, do których należą leki, napoje, żywność i zabawki. Z badania wynika, że międzynarodowy handel podrabianymi produktami stanowił w 2013 r. do 2,5 proc. światowego handlu, osiągając kwotę ok. 338 mld euro. W Unii Europejskiej podrobione produkty stanowiły do 5 proc. wszystkich importowanych do Wspólnoty towarów, o łącznej wartości ok. 85 mld euro. Markami najbardziej cierpiącymi z powodu procederu podróbek są przeważnie firmy zarejestrowane w krajach UE, a podrabiane towary pochodzą z różnych krajów, najczęściej z Chin. Ze względu na wzrost popularności e-handlu, popularnym środkiem transportu podrobionych towarów, zmniejszającym ryzyko wykrycia podróbek, są coraz częściej klasyczne przesyłki listowe lub paczki wysyłane w niewielkiej liczbie, lecz dość często.

Podrabia się produkty z różnych branż, począwszy od towarów luksusowych, jak kosmetyki czy zegarki, po dobra konsumpcyjne, które mają realny wpływ na zdrowie i bezpieczeństwo.

Czy podróbki są groźne?

Choć podrabia się wszystko, do najbardziej niebezpiecznych fałszywych produktów należą te, które stanowią realne zagrożenie życia lub zdrowia ludzi. To żywność, leki i kosmetyki.

Bezwartościowe mleko w proszku

W roku 2008 w Chinach miała miejsce tzw. afera melaminowa ze skażonym mlekiem dla dzieci. Podrabiane tam mleko dla niemowląt zawierało melaminę – środek, który z powodu wysokiej zawartości azotu bywa używany do fałszowania wyników badań na zawartość białka w mleku. W rzeczywistości w mleku było znacznie mniej białka niż powinno, co spowodowało niedożywienie dzieci. Nie był to niestety jedyny problem. Melamina jest substancją wykorzystywaną do wyrobu płyt drewnopochodnych, klejów, farb i lakierów, a także produkcji przedmiotów gospodarstwa domowego. Nie jest przeznaczona do spożycia i może wywołać poważne zatrucie organizmu, jest jednak stosunkowo tania i łatwo dostępna. Efektem rozprowadzenia podrobionego i skażonego mleka było zatrucie ok. 300 tys. osób i hospitalizacja ok. 50 tys. niemowląt. Najtragiczniejszym skutkiem afery melaminowej była śmierć 11 noworodków.

Plastikowy ryż

W 2011 r. było głośno o podrobionym ryżu, który wykryto w chińskim mieście Taiyuan. Zawierał on mieszankę ziemniaków i plastiku. Ten syntetyczny produkt był łudząco podobny do oryginału, ale jego spożycie zagrażało zdrowiu. Oszuści próbowali sprzedawać go w normalnych cenach, przedstawiając jako pełnowartościowy. Stowarzyszenie Chińskich Restauratorów oznajmiło, że zjedzenie trzech miseczek tak spreparowanego ryżu było równoznaczne ze spożyciem plastikowej reklamówki.

Podrabiane leki

Fałszowanie leków to bardzo rozwinięty i dobrze zorganizowany proceder występujący na całym świecie. Fałszerze podrabiają wszystkie rodzaje leków, zarówno przeciwbólowe, jak i specjalistyczne przeznaczone do leczenia groźnych chorób. W krajach wysoko rozwiniętych najczęściej podrabiane są drogie leki wpływające na poprawę jakości życia, takie jak tabletki nasenne, preparaty na odchudzanie, viagra itp., w krajach uboższych natomiast – leki przeznaczone do leczenia chorób zagrażających życiu.

Leki z DNA człowieka

W 2011 r. olbrzymi skandal wywołała sprawa tabletek, w których po badaniach laboratoryjnych wykryto ludzkie DNA. Koreańskie władze poinformowały o znalezieniu dużej liczby takich tabletek w bagażach turystów i przesyłkach międzynarodowych. Zarekwirowano 17,5 tys. kapsułek zawierających wysuszoną i sproszkowaną ludzką tkankę. Miał to być lek zwiększający witalność i popęd seksualny.

Fabryka podróbek w Polsce

Problemy fałszywych leków występują nie tylko na Dalekim Wschodzie. W 2016 r. policjanci z CBŚP zlikwidowali nielegalną fabrykę leków pod Bydgoszczą. Zabezpieczono sterydy i sfałszowane leki o wartości ponad 17 mln zł. Fabryka była bardzo dobrze zaopatrzona – m.in. w maszyny do produkcji i profesjonalnego pakowania medykamentów. Przestępcy podrabiali leki czterech znanych koncernów farmaceutycznych i sprzedawali je przez internet.

Fałszywe kosmetyki

W 2015 r. brytyjski „Independent" opublikował informacje dotyczące podrabianych perfum i kosmetyków do makijażu. Zawierały m.in. arszenik i rtęć, a nawet ludzki mocz. W niektórych próbkach, prawdopodobnie z powodu niehigienicznych warunków produkcji, znaleziono szczurze odchody i trutkę na gryzonie. Te substancje mogą wywołać poważne problemy skórne i zdrowotne.

Podobne procedery mają miejsce także w Polsce. Pod koniec ub.r. policjanci z Łodzi zlikwidowali laboratorium, w którym na wielką skalę produkowano podrobione kosmetyki i perfumy. *Była to kompletna linia technologiczna, półprodukty, chemia, pojemniki z cieczą o zapachu spirytusu, mieszalniki, menzurki, dozowniki i słoje z różnokolorowymi cieczami. Ponadto policjanci zabezpieczyli ponad 2 tys. flakonów perfum przygotowanych do dystrybucji oraz puste flakony, atomizery, zakrętki i koncentraty.*

Podrobione zabawki

Zabawki są równie często podrabianymi produktami jak dobra luksusowe. Popyt na nie wzrasta zwłaszcza w okresie przedświątecznym, kiedy klienci chcą kupić prezent dobrze wyglądający i stosunkowo tani, nie sprawdzając źródła jego pochodzenia ani atestów czy etykiet CE oznaczających spełnienie wymogów unijnych.

Podrabiane zabawki często do złudzenia przypominają oryginały, jednak mogą okazać się nie tylko słabej jakości bublem, lecz – co gorsza – zawierać szkodliwe i groźne dla dzieci substancje. Taka sytuacja miała miejsce w Polsce w 2015 r., gdy matka kupiła podrobioną masę plastyczną. Zawarte w niej toksyczne substancje wywołały u dziecka mocną reakcję alergiczną i tylko szybkie działanie rodziców pozwoliło na uniknięcie poważnych konsekwencji. Takich przypadków z roku na rok jest niestety coraz więcej.

BRAND PROTECTION...

to nie tylko opłacalna, ale także potrzebna inwestycja. Podejmując działania z zakresu ochrony marki, chronimy nie tylko ciężką pracę związaną z jej budowaniem, lecz również – a może przede wszystkim – ludzi, którzy kupują u nas markowy produkt i chcą mieć pewność, że płacą za jakość i sprawdzony towar. Tak ciężko budowane i trudne w dzisiejszych czasach do podtrzymania zaufanie klienta przekłada się bezpośrednio na wzrost sprzedaży i zysk firmy.

BIO

Agnieszka Socha
Analityk i starszy konsultant ds. ryzyka w SASMA EUROPE, licencjonowany detektyw. Specjalizuje się w *due diligence*, prowadzi projekty w Polsce i zagranicą m.in. z zakresu ochrony marki, bezpieczeństwa logistycznego i audytów.

W kolejnych wydaniach „a&s Polska" opiszemy efektywne działania walki z podróbkami, podpowiemy, jak powinien wyglądać program ochrony marki oraz przedstawimy prawne aspekty i polskie przepisy w tym zakresie.

Nowe kamery sieciowe Canon w dystrybucji Axis Communications

We wrześniu ub.r. Axis Communications przejął marketing i sprzedaż produktów Canon z zakresu sieciowych rozwiązań dozorowych w regionie EMEA (Europa, Bliski Wschód, Afryka).
Zgodnie z zawartym porozumieniem Axis wprowadza na rynek 7 nowych kamer firmy Canon. Wszystkie oferują pracę w rozdzielczości HDTV 1080p. Sześć z nich jest przeznaczonych do pracy na zewnątrz. Są odporne na uszkodzenia oraz trudne warunki atmosferyczne.

Nowe modele w kanałach dystrybucyjnych Axis:
VB-H761LVE – bullet z 20x zoomem optycznym i zintegrowanym oświetlaczem podczerwieni. Przeznaczony do zabezpieczenia infrastruktury krytycznej, budynków komercyjnych i przemysłowych.
VB-H760VE – bullet z 20x zoomem optycznym. Przeznaczony do monitoringu infrastruktury krytycznej i przemysłowej, budynków komercyjnych.
VB-H751LE – bullet z 2,4x zoomem i zintegrowanym oświetlaczem podczerwieni. Idealny do monitorowania budynków komercyjnych, magazynów i infrastruktury krytycznej – nawet w kompletnych ciemnościach.
VB-H651VE – kopułka PTRZ z ultraszerokim obiektywem. Kamera stworzona z myślą o monitoringu centrów handlowych, budynków komercyjnych i banków.
VB-S30VE – miniaturowa kopułka PTZ z wbudowanym mikrofonem i 3,5x zoomem. Przeznaczona do dyskretnego monitoringu sklepów, szkół i magazynów oraz przestrzeni, wymagających aktywnej zmiany kąta obserwacji w trakcie pracy kamery.
VB-S800VE – miniaturowa kopułka PTZ z wbudowanym mikrofonem. Przeznaczona do dyskretnego dozoru w handlu, bankowości czy placówkach edukacyjnych.
VB-S910F – bullet do pracy wewnątrz budynków, z 3,5x zoomem i mikrofonem. Stworzony z myślą o dyskretnym monitoringu przestrzeni handlowych, szkół czy banków.

Panasonic: Monitoring środków transportu

Panasonic oferuje dwie wytrzymałe kamery IP do pociągów, autobusów i samochodów dostawczych.
Modele full HD WV-SBV131M oraz HD WV-SBV111M mają funkcje *High Light Compensation* (HLC) oraz *Adaptive Black Stretch* (ABS) poprawiające widoczność zaciemnionych obszarów i tłumiące jasne światło, np. reflektorów samochodowych. Dzięki temu dłużej utrzymują tryb koloru.
Zamontowane na zewnątrz pojazdu są w stanie przetrwać najtrudniejsze warunki, np. w myjni wysokociśnieniowej. Mają obudowę zintegrowaną z kloszem odpornym na zarysowania. Pracują w szerokim zakresie temperatury.
Są wytrzymałe na wstrząsy i wibracje (IP6K9K oraz IP66). Zapewniają szeroki kąt widzenia, umożliwiając monitorowanie obszaru 11 m wzdłuż boku pojazdu, bez martwych pól. Możliwy jest podgląd do 20 m za pojazdem, dający wiarygodne zdjęcia w razie wypadku.

Nowa kamera panoramiczna Samsung WiseNet P z H.265 i kompresją WiseStream

Hanwha Techwin powiększa rodzinę kamer Samsung WiseNet P, wprowadzając do oferty model panoramiczny o rozdzielczości 7,3 Mpix.
W kamerze PNM-9020V, zaprojektowanej do monitorowania dużych przestrzeni, zastosowano kilka przetworników obrazu pozwalających pozyskiwać z kamery obraz o kącie widzenia 180°. Cztery przetworniki o rozdzielczości 2 Mpix każdy, współpracujące z obiektywami o ogniskowej o długości 3,6 mm, zamontowano na ruchomym ramieniu umożliwiającym uzyskanie właściwego ustawienia kamery w każdych warunkach obserwacji.
Panoramiczna kamera wysokiej rozdzielczości PNM-9020V może zastąpić trzy lub cztery kamery HD, dając nie tylko znaczące oszczędności przy zakupie kamer, ale również podczas jej instalacji – powiedział Tim Biddulph, Head of Product Management w Hanwha Techwin Europe.

Kluczowe funkcje
Posiadająca cyfrowy zoom i obsługę cyfrowego PTZ kamera PNM-9020V jest odporna na warunki środowiskowe (stopień ochrony obudowy IP66) i akty wandalizmu (IK10).
Zaimplementowano w niej szereg innowacyjnych i praktycznych funkcji dostępnych w serii P: cyfrowego śledzenia obiektów, WDR oparty na działaniu elektronicznej migawki oraz korekcję zniekształceń obiektywu. Dzięki temu kamera dostarcza użyteczny obraz w każdych warunkach. Ma też dwukierunkowy tor audio, maski prywatności oraz gniazdo na karty pamięci.

Otwarta Platforma - Open Platform
W kamerze PNM-9020V zaimplementowano fabrycznie funkcje analityki obrazu wideo: przekroczenie wirtualnej linii, pojawienie się i zniknięcie przedmiotu oraz tworzenie map ciepła. Moc obliczeniowa procesora DSP kamery pozwala użytkownikom na wybór dodatkowych aplikacji realizujących analitykę wideo, która spełnia indywidualne potrzeby użytkownika.
WiseStream
Długą listę innowacyjnych funkcji uzupełnia WiseStream – opracowana przez Hanwha Techwin technologia pozwalająca na dynamiczne sterowanie procesem kompresji, w zależności od zawartości ruchu w obserwowanej scenie. Kompresja H.265 wraz z WiseStream jest w stanie obniżyć zapotrzebowanie kamer IP na pasmo sieciowe nawet o 75% w stosunku do powszechnie stosowanej w kamerach techniki kompresji obrazu H.264.

WiseNet STAR 2017

To już piąta, jubileuszowa edycja Samsung STAR, tym razem pod nową nazwą i marką. Polski zespół Hanwha Techwin Europe (dawniej Samsung) zaprasza 29 marca do Centrum Olimpijskiego w Warszawie.
Nowe kamery 4K serii P, premiera serii X z procesorem WiseNet 5, najnowsza panoramiczna kamera wieloobiektywowa, rodzina nowych rejestratorów sieciowych serii P, innowacyjne technologie w nowej wersji oprogramowania SSM 1.6 czy nowy system rozpoznawania tablic rejestracyjnych z identyfikacją kraju i kontrolą dostępu – to tylko zapowiedź spotkania.
Imprezę uświetni brytyjska firma Veracity, której rewolucyjny system rejestracji sekwencyjnej, zintegrowany z oprogramowaniem Hanwha SSM, zyskał uznanie międzynarodowych ekspertów.
Wśród uczestników zostanie wylosowana nagroda, gwarantująca moc adrenaliny i lotniczą przygodę.
Formularz rejestracyjny i więcej informacji na stronie: **www.wisenetstar.pl**

Komitet Techniczny ds. Usług w Ochronie Osób i Mienia

W Polskim Komitecie Normalizacyjnym powstał nowy Komitet Techniczny KT323 ds. Usług w Ochronie Osób i Mienia. Będzie on kontynuował prace prowadzone dotychczas w komitecie PKN/KZ 501.

Zakres prac obejmuje współpracę z dwoma europejskimi komitetami technicznymi :
CEN/CLC 4 *Services for fire safety systems and security systems,*
CEN TC 439 *Private security services.*
W komitecie CEN/CLC 4 powstała norma EN 16763:2017 *„Services for fire safety systems and security systems”.* Określa ona wymagania stawiane firmom usługowym zajmującym się poszczególnymi fazami wdrażania systemów zabezpieczeń technicznych: planowaniem, projektowaniem, instalacją, uruchamianiem, sprawdzaniem, przekazywaniem i konserwacją systemów. Obejmuje usługi związane z systemami alarmowymi, takimi jak systemy sygnalizacji włamania i napadu, kontroli dostępu, telewizji dozorowej itd., a także z systemami elektronicznymi stosowanymi w ochronie pożarowej, takimi jak systemy sygnalizacji pożaru, stałe instalacje gaśnicze wodne i gazowe, systemy sterowania ciepłem i dymem itd. Norma określa także wymagania dotyczące kwalifikacji pracowników usługodawców, odnosząc je do europejskiego systemu EQF.

Norma EN 16763 została opracowana jako dokument odniesienia przy certyfikacji firm usługowych. Mamy nadzieję, że jej polska wersja będzie dostępna wkrótce po jej opublikowaniu.

Z kolei komitet CEN TC 439 *Private security services* opracowuje normy europejskie dotyczące wymagań jakościowych stawianych firmom ochrony fizycznej. W pierwszej kolejności dotyczy to ochrony infrastruktury krytycznej, europejskiej i narodowej.

Wymagania dotyczące firm oferujących podstawowe usługi ochrony fizycznej, np. sklepów wielkopowierzchniowych, zakładów przemysłowych itd. powinny być przedmiotem norm krajowych.

Opracowanie takich norm wchodzi też w zakres komitetu KT 323 ds. Usług w Ochronie Osób i Mienia.

Pierwsze, inauguracyjne posiedzenie KT 323 PKN odbyło się 27 stycznia br.

SUMA otwiera showroom Vivotek w Krakowie

W Krakowie otwarto pierwszy showroom firmy Vivotek. To miejsce zostało stworzone, aby ułatwić naszym klientom prezentowanie produktów Vivotek w działaniu – można dotknąć, poznać parametry, sprawdzić, jak działają różne funkcje.

Mogą tu przyjechać nie tylko instalatorzy, by sprawdzić jak zaprojektowane rozwiązanie będzie funkcjonować, ale także zabrać swoich klientów, aby pokazać działanie oferowanych urządzeń.

W salonie można umówić się ze specjalistami Vivotek, którzy pomogą zaplanować system monitoringu, wyjaśnią działanie poszczególnych technologii, podpowiedzą, co się najlepiej sprawdzi w danej sytuacji.

Firma zaprasza na ul. Bulwarową 31 w Krakowie, od poniedziałku do piątku.
Infolinia: 801 084 044

Fire Sentry – czujki płomienia Honeywell

Honeywell wprowadza do oferty dwie nowe rodziny czujek płomienia Fire Sentry:
• czujki serii FSL100 do typowych zastosowań w obiektach handlowych, publicznych i przemyśle lekkim oraz
• czujki serii FSX do zastosowań w trudnych warunkach przemysłowych i w projektach wymagających jak najszybszej detekcji pożarów płomieniowych.

Czujki serii FSL100 są dostępne w 3 wersjach: z sensorem UV, z sensorami UV i IR lub z trzema sensorami IR. Są standardowo wyposażone w uchwyt, dławnicę kablową i zawór do wyrównania ciśnienia i zapobiegania kondensacji wilgoci wewnątrz czujki w zastosowaniach zewnętrznych.

Czujki serii FSX są dostępne w 2 wersjach: FS20X z trzema sensorami płomienia UV/IR/IR i FS24X z trzema sensorami płomienia IR. Wszystkie są też wyposażone w sensor światła widzialnego do adaptacji charakterystyki czułości czujki do warunków pracy.

Serie FSL100 i FSX mają certyfikaty zgodności CE (EN 54-10), ATEX oraz FM, a seria FSX dodatkowo klasyfikację niezawodności na poziomie SIL2.

REDSCAN mini – nowy zewnętrzny laser skanujący OPTEX

OPTEX rozszerza serię czujek laserowych REDSCAN o nową zewnętrzną czujkę średniego zasięgu – RLS-2020S. Model S jest wyposażony w mikroprocesor, który zapewnia bardziej efektywną obróbkę danych.

Zastosowaną wewnątrz budynku czujkę można tak skonfigurować, aby wykrywała obiekty poruszające się z dużą prędkością (nawet do 16,2 km/h przy montażu prostopadle do podłoża lub 45 km/h przy montażu pod kątem 30°). Umożliwia wykrywanie obiektów o niewielkiej średnicy – nawet 2,5 cm.

Wszystkie te parametry sprawiają, że RLS-2020S można stosować w obiektach wysokiego ryzyka (lotniska, budynki rządowe czy centra danych).

Czujka może być stosowana na zewnątrz ze względu na użycie specjalnego algorytmu kompensującego wpływ niekorzystnych warunków środowiskowych, co minimalizuje liczbę fałszywych alarmów.

RLS-2020S może być zasilana z wykorzystaniem Power over Ethernet (PoE) lub 12 VDC i wysyłać alarmy za pomocą tradycyjnych wyjść przekaźnikowych lub używając komunikacji IP zintegrowanej ze wszystkimi głównymi programami VMS.

REDSCAN Manager – oprogramowanie dedykowane zarówno do wersji zewnętrznej, jak i wewnętrznej czujki RLS-2020 – umożliwia szerokie możliwości konfiguracji parametrów, dopasowanie kształtu obszaru detekcji do wymagań użytkownika, rozmieszczenie stref alarmowych, wybór algorytmu pracy.

Sprzedaż i instalacja RLS-2020S jest realizowana poprzez certyfikowanych partnerów.

Więcej informacji na temat programu certyfikacji można uzyskać w firmie OPTEX Security: tel. 22 598 06 60, optex@optex.com.pl

Bosch z projektantami w Centrum Olimpijskim

Uczestniczyliśmy w drugim spotkaniu dla projektantów systemów niskoprądowych, zorganizowanym przez Bosch Security Systems w warszawskim Centrum Olimpijskim. Było ono elementem rozpoczętego w kwietniu 2015 r. międzynarodowego programu *Architecture & Engineering Partner Program* (A&E Partner Program). Program opiera się na trzech filarach: edukacja, wiedza ekspercka i technologie.

Podczas corocznej konferencji edukacyjnej i przez portal internetowy jego członkowie mają dostęp do wiedzy nie tylko na temat portfolio urządzeń i systemów Boscha, ale także dotyczących trendów produktowych i technologicznych, norm i przepisów oraz dostęp do ekspertów, poradnictwa projektowego, wsparcia technicznego i narzędzi informatycznych.
Programowi patronują autorytety branżowe: CNBOP i PISA. Uczestniczy w nim już 320 osób. Polska była dla niego poligonem pilotażowym, obecnie w A&E bierze udział kilkanaście krajów. Krzysztof Góra, dyrektor handlowy Bosch Security Systems, wspomniał, że w czerwcu w krakowskim Centrum Konferencyjnym ICE zgromadzi się ponad 100 projektantów z całego świata.
Bieżące odbyło się w efektownym architektonicznie obiekcie, siedzibie Polskiego Komitetu Olimpijskiego. Ciekawa była jego logistyka. Tradycyjny układ widowni zastosowano przy wystąpieniach początkowych i końcowych. Pomiędzy nimi, w pustej już sali, wydzielono stanowiska ze sprzętem demonstracyjnym dla CCTV, alarmówki, kontroli dostępu, pożarówki oraz BIS (integracji). Projektanci podzieleni na grupy co pół godziny zmieniali punkty prezentacji nowości produktowych. Karuzela wiedzy.
Marek Pyc, opiekun polskiego programu A&E, podpowiedział projektantom, jak korzystać z możliwości portalu. Poinformował też o konkursie na najbardziej innowacyjny projekt. Trwa od stycznia br. do czerwca 2018 r. Nagrodzeni projektanci obejrzą ciekawą inwestycję zagraniczną.
Treści corocznych konferencji zawierają sporą dawkę fachowej wiedzy pozaproduktowej. Na pierwszej, w warszawskim Pałacu Kultury i Nauki, dużo uwagi poświęcono technologii BIM – *Building Information Modelling* (modelowanie informacji o budynkach i obiektach inżynierskich). Dane konstrukcyjne są w niej przechowywane cyfrowo, zintegrowane w sieci i przedstawiane na modelach trójwymiarowych.
W bieżącej interesujące było wystąpienie Artura Bogusza, szefa działu bezpieczeństwa w Muzeum Żydów Polskich „Polin". Dotyczyło kwestii „Projektu i jego realizacji – jak zaprojektowane systemy sprawdzają w codziennym funkcjonowaniu obiektu?". Według prelegenta kluczowymi elementami projektu systemów zabezpieczeń z punktu widzenia użytkownika końcowego i administratora obiektu oprócz koncepcji są kosztorys inwestorski, rysunki, schematy działania, opisy, instrukcje obsługi, certyfikaty, poświadczenia zgodności, uwagi praktyczne itd. Usłyszeliśmy m.in. o konfrontacji wizji architektonicznej z możliwościami technicznymi systemów zabezpieczeń, roli projektanta na etapach tworzenia koncepcji i przy uzgadnianiu jej z inwestorem projektu. Nie jest bowiem wskazane rozpoczynanie prac projektowych bez koncepcji zabezpieczenia obiektu. Tę tematykę podjął też Michał Borzęcki z Boscha, omawiając tworzenie koncepcji i specyfikacji projektowych. Wspomniano o nowym rynkowym związku Boscha z Sony. Poinformowano o certyfikacie dla DSO PAVIRO oraz o systemie AVIOTEC (technologia wideo dla wczesnego wykrywania pożaru), Smart linku – do szybkiej integracji centrali SSP z DSO, najnowszych algorytmach inteligentnej analityki obrazu, adresowalnych SSWiN powyżej tysiąca elementów, integracji systemów, nowych kamerach i rejestratorach.

Tekst i foto: Andrzej Popielski

XVR

Przywracamy znaczenie słowa standard

Cechy

- Multi-standard: HDCVI / AHD / TVI / IP / CVBS
- Przyjazny interfejs, szybka konfiguracja
- Zwiększony zasięg transmisji oraz odporność na zakłócenia
- Zabezpieczenia przeciwprzepięciowe i przeciwprzesłuchowe
- Obsługa RAID, IVS, VQD

Dostępne produkty:

- XVR seria 7000/5000/4000

ISO 9001:2000

www.dahuasecurity.com/pl

Dahua Technology Poland Sp. z o.o.

ul. Salsy 2, 02-823 Warszawa
tel. +48 22 395 74 00, fax +48 22 395 74 10
e-mail: biuro.pl@global.dahuatech.com
www.dahuasecurity.com/pl