CZASOPISMO RYNKU SECURITY

№ 04
2019 (16)
lipiec / sierpień

a&S POLSKA

bezpieczeństwo → w handlu

www.aspolska.pl

APLIKACJA MOBILNA

a&S POLSKA Available on the iPhone App Store ANDROID APP ON Google play

15 zł
(w tym 8% VAT)

ISSN 2451-5175

KOLOROWY OBRAZ, NAWET W CIEMNOŚCI

Poznaj produkty:
DS-2CE72DFT-F(3.6mm)
DS-2CE10DFT-F(3.6mm)
DS-2CD2347G1-L(4mm)
DS-2CD2T47G1-L(4mm)

Ciesz się żywym, kolorowym obrazem przez całą dobę, dzięki technologii ColorVu

– Jasny obiektyw
Przez obiektyw F 1.0 do przetwornika dociera więcej światła, przez co uzyskasz jaśniejszy obraz

– Wysoka czułość
Dużo lepsze wykorzystanie docierającego światła, dzięki zaawansowanym przetwornikom

– Przyjazne oświetlenie
W pełnej ciemności ciepłe oświetlenie zagwarantuje kolorowy obraz

Dołącz do Programu Partnerskiego Hikvision i uzyskaj dostęp do najnowszych promocji oraz pełnego wsparcia Hikvision!
Wejdź na: **https://partner.hikvision.com/eu/**

Hikvision Poland Sp. z o.o.
ul. Krakowiaków 50
02-255 Warszawa
T +48 22 4600150
info.pl@hikvision.com

1. DOŁĄCZ DO PROGRAMU PARTNERSKIEGO HIKVISION.
2. KUPUJ PRODUKTY HIKVISION I WEŹ FAKTURĘ, NA KTÓREJ BĘDĄ WYŁĄCZNIE PRODUKTY TEJ MARKI. ZA KAŻDY WYDANY 1000 PLN NETTO OTRZYMASZ 1 SZANSĘ NA WYGRANĄ. ZACHOWAJ DOWODY ZAKUPÓW
3. REJESTRUJ SWOJE ZAKUPY NA **LOTERIAHIKVISION.PL**
4. WEŹ UDZIAŁ W LOSOWANIU

5 FIATÓW FIORINO

CZAS TRWANIA LOTERII: **01.06.19 – 15.11.19**
SZCZEGÓŁY I REGULAMIN NA STRONIE ORAGNIZATORA WWW.SMOLAR.PL I WWW.LOTERIAHIKVISION.PL

EDYTORIAL

Drodzy czytelnicy

Wakacje rozpoczęliśmy od branżowego wyjazdu w plener. Pierwsza edycja Security BootCamp to nowa formuła szkoleniowa w branży. Na malownicze podlaskie tereny zaprosiliśmy szefów bezpieczeństwa i dostawców systemów security, by w praktyce przetestowali działanie różnych rozwiązań. Z dużym zaangażowaniem wcielali się też w osoby na różnych stanowiskach, by zarządzać sytuacjami kryzysowymi i im zapobiegać podczas zorganizowanej drugiego dnia gry decyzyjnej. Relację z wydarzenia prezentujemy na str. 16.

Dział Rynek Security otwiera ostatnia część cyklu **optyka dla każdego** (str. 24), w której autor opisuje budowę i klasyfikację obiektywów, uzupełnia informacje o rozdzielczości optycznej oraz wyjaśnia działania migawki i ekspozycji. Systemy dozoru wizyjnego ze względu na swoją specyfikę wymagają dedykowanych rozwiązań do pracy całą dobę, przy dużej odporności na błędy i utratę danych. Coraz popularniejsze staje się **wykorzystanie niezmierzonych pamięci** półprzewodnikowych (str. 30). Czy jednak wiemy, na co zwrócić uwagę przy wyborze właściwych **kart pamięci** do zapisu w systemach telewizji dozorowej (str. 32)?

Według najnowszych raportów do końca roku powierzchnia sprzedażowa w Polsce ma zwiększyć się o 170 tys. m^2. Parki handlowe rozwijają się w coraz szybszym tempie, stanowiąc kolejny krok w ewolucji przestrzeni handlowych. Jednocześnie zwiększa się zapotrzebowanie na nowoczesne rozwiązania do ich zabezpieczania. Dlatego **na temat numeru wybraliśmy bezpieczeństwo w handlu**. Jednym z ważnych zagadnień są systemy do zarządzania **miejscami parkingowymi** w centrach i galeriach handlowych (str. 54). Wysłużone biletowe rozwiązania zastępowane są systemami rozpoznającymi tablice rejestracyjne, które zwiększają przepusowość parkingów i ich bezpieczeństwo. A jeszcze kilka lat temu **systemy ANPR** były skomplikowane, wymagały wykorzystania aplikacji serwerowych i specjalnych kamer generujących wyłącznie obraz czarno-biały. Dzisiaj w większości są to wielofunkcyjne urządzenia będące nie tylko „oczami", ale nawet „mózgiem" (str. 62) systemów rozpoznających numery tablic rejestracyjnych, których przegląd prezentujemy na str. 67. W obiektach handlowych bardzo ważną kwestią jest też **zapewnienie bezpieczeństwa pożarowego** (str. 78) oraz sprawna ewakuacja (str. 82).

Rozważania na temat **bezpieczeństwa w galeriach handlowych** (str. 84), w tym również **cyberbezpieczeństwa** (str. 86), kontynuujemy w dziale **Bezpieczeństwo Biznesu**. O największych skandalach w biznesie z udziałem „białych kołnierzyków" przeczytamy na str. 90, a najnowszą koncepcję wykorzystania planowania urbanistycznego i tzw. małej architektury w celu poprawy bezpieczeństwa miasta przybliża artykuł na str. 96.

Miłej lektury.

Marta Dynakowska
REDAKTOR NACZELNA

Jan T. Grusznic
Z-CA REDAKTORA NACZELNEGO

Mariusz Kucharski
DYREKTOR ZARZĄDZAJĄCY

a&S POLSKA
www.aspolska.pl

Wydawca
A&S Polska Sp. z o.o.
ul. Rondo ONZ 1
00-124 Warszawa

Dyrektor zarządzający
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Z-ca redaktora naczelnego
Jan T. Grusznic

Stały felietonista
Andrzej Popielski

Dział marketingu i reklamy
Iwona Krawiec

Dział eventów i konferencji
Jolanta A. Kucharska
Aleksandra Czapska

Projekt graficzny i skład
Bogusław Kalwala

Redakcja
ul. A. Branickiego 15
Wilanów Office Park, bud. 1
02-972 Warszawa
e-mail: info@aspolska.pl
www.aspolska.pl

Kolegium redakcyjne
Norbert Bartkowiak
Sebastian Błażkiewicz
Marek Domański
Jacek Grzechowiak
Rafał Łupkowski
Przemysław Pierzchała
Janusz Sawicki
Stefan Jerzy Siudalski
Jerzy Sobstel
Jacek Tyburek
Paweł Wittich
Waldemar Wnęk
Aleksander M. Woronow

Korekta
Jolanta Kucharska

Prenumerata
www.aspolska.pl/prenumerata

SPIS TREŚCI

№ 04
2019 (16)
lipiec/sierpień

a&S POLSKA

RYNEK SECURITY

BEZPIECZEŃSTWO W HANDLU

BEZPIECZEŃSTWO POŻAROWE

BEZPIECZEŃSTWO BIZNESU

SERWIS INFORMACYJNY

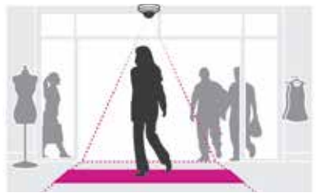
FELIETON O BEZPIECZEŃSTWIE

AXIS COMMUNICATIONS

www.axis.com/pl

AXIS People Counter – inteligentna aplikacja do zliczania osób

Aplikacja AXIS People Counter zlicza automatycznie w czasie rzeczywistym osoby przechodzące pod kamerą i informuje o kierunku, w którym się one udały. Po zintegrowaniu z systemem PoS może gromadzić informacje dotyczące współczynników konwersji, zapewniając przydatne dane umożliwiające podejmowanie kluczowych decyzji.



Kamera z zainstalowanym oprogramowaniem powinna być zamontowana na suficie nad przejściami i wejściami na wysokości co najmniej 2,7 m. Oprogramowanie zamienia kamerę w zaawansowany czujnik gromadzący dane pomagające m.in.:

- **analizować przepływ klientów i trendy,**
- **oceniać wpływ działań reklamowych i promocyjnych,**
- **planować harmonogramy pracy, określić optymalne godziny otwarcia sklepu i zoptymalizować koszty zatrudnienia,**
- **ocenić wpływ pogody na liczbę klientów,**
- **zidentyfikować i nagradzać najlepsze sklepy i pracowników.**

AXIS People Counter to system jednoczesnego dwukierunkowego zliczania osób – wchodzących na korytarz i wychodzących z niego, z pominięciem wózków dziecięcych i sklepowych. Obserwacją można objąć wejścia z drzwiami pojedynczymi lub podwójnymi.

Oprogramowanie opracowano z wykorzystaniem zaawansowanych i sprawdzonych algorytmów firmy Conigmatics, której programy od ponad dekady wiodą prym w branży aplikacji analitycznych dla sklepów. To szybkie i niewymagające wiele pamięci operacyjnej oprogramowanie zainstalowano w tysiącach kamer na całym świecie.

BCS

www.bcscctv.pl

Kamera sferyczna BCS-SFIP21200IR-II

Kamera BCS-SFIP21200IR-II to topowy przedstawiciel rodziny kamer z obiektywem *fisheye* w ofercie marki BCS. Superczuły 12-Mpix przetwornik **Sony STARVIS** oraz szerokokątny obiektyw 1,98 mm sprawiają, że ten model to potężne narzędzie monitoringu wizyjnego. Pozwala uzyskać obraz o kącie widzenia 180° tworzący panoramę bez tzw. martwych stref. Kamera świetnie sprawdzi się, monitorując powierzchnie handlowe – rozległe korytarze centr handlowych, sklepy na wyspach czy w boksach sprzedażowych. Główną korzyścią z zastosowania modelu **BCS-SFIP21200IR-II** jest możliwość zastąpienia wielu kamer stałopozycyjnych jedną kamerą typu *fisheye*. Obraz transmitowany do rejestratora można rozłożyć, tworząc maks. **8 wirtualnych kamer PTZ** i każdą z nich wykorzystać do dokładniejszej obserwacji interesującego obszaru. Kamera oferuje również zaimplementowane funkcje inteligentnej analizy obrazu: przekroczenia linii, naruszenia strefy i tworzenia mapy cieplnej. Umożliwia graficzne zobrazowanie strefy o największym natężeniu ruchu – to cenne dane analityczne, szczególnie użyteczne w handlu, gdyż pomaga w odpowiednim rozłożeniu produktów w sklepie.

Jest wyposażona w promiennik IR umożliwiający monitorowanie obiektu po jego zamknięciu oraz moduł audio nadający komunikaty głosowe. Wandaloodporna obudowa ma klasę odporności **IK10 i klasę szczelności IP67**, dzięki czemu kamera może znaleźć zastosowanie również w monitoringu stref podwyższonego ryzyka (cele więzienne, sale przesłuchań).

DAHUA TECHNOLOGY POLAND

www.dahuasecurity.com/pl

ASI1212D – autonomiczny czytnik linii papilarnych

Użytkownicy systemów zabezpieczeń oczekują od nich przede wszystkim funkcjonalności i bezawaryjnej pracy. Obecnie czynnikiem nie mniej istotnym staje się wygląd – chcemy otaczać się ładnymi rzeczami. Producenci urządzeń podchwycili tę modę i dzięki temu pojawiają się instalacje, na które składają się nie tylko toporne plastikowe pudełka. Coraz częściej montowane elementy są dopracowane wzorniczo nie gorzej niż pod kątem funkcjonalnym.

Przedstawicielem trendu „funkcjonalnie i efektownie" jest autonomiczny czytnik linii papilarnych **Dahua ASI1212D.** Wyposażono go w klawiaturę dotykową i wyświetlacz LCD przekazujący podstawowe informacje. W pamięci urządzenia można przechowywać dane 30 tys. kart zbliżeniowych czy 3 tys. odcisków palca. Komunikację z czytnikiem zapewnia wykorzystanie zarówno protokołów komunikacyjnych **TCP/IP**, jak i **RS-485** czy **Wiegand,** uwierzytelnianie może być realizowana przy użyciu kodu, karty, odcisku palca lub ich kombinacji. Rejestr zdarzeń zmieści do 150 tys. rekordów.

Są dwa warianty urządzenia: obsługujące karty **Mifare 13,56 MHz** lub klasyczne 125 kHz. Użytkownicy mogą być przypisywani do różnych grup (VIP, gość, pracownik ochrony itp.). Dostępne są klasyczne funkcje, np. *anti-passback* czy *multi-interlock*. Dodajmy do tego estetyczną obudowę w klasie **IP55** – otrzymujemy ciekawy element systemu, który może być interesującą propozycją tam, gdzie potrzeba nieskomplikowanego urządzenia o ciekawych możliwościach.

PRODUKT NUMERU

HIKVISION www.hikvision.com/pl

DS-2CD7126G0-IZS

Coraz bardziej rozbudowana analityka to odpowiedź na rosnące potrzeby klientów. Firma Hikvision ma w ofercie model DS-2CD7126G0-IZS z serii DeepinView, który sprosta oczekiwaniom różnych inwestorów. Kamera wyposażona w przetwornik 1/1.8" **Progressive Scan CMOS** z serii **DarkFighter** generuje strumień wizyjny w rozdzielczości **1920 x1080** pix przy **60 kl./s** oraz dodatkowe **5 strumieni wizyjnych**. Wbudowany oświetlacz IR ma zasięg do 30 metrów. Regulowany obiektyw (**2,8–12 mm lub 8–32 mm**), motozoom oraz **WDR 140 dB** pozwalają na zastosowanie kamery w różnych warunkach pracy. Zaawansowane algorytmy wspierane technologią głębokiego uczenia się zapewniają wysoką dokładność wykrywania osób (rozpoznają głowę i ramiona), umożliwiają także śledzenie ruchu osób i tworzenie się kolejek. Kamera może śledzić jedocześnie 64 osoby w trzech niezależnych strefach. Osoba, która wejdzie w kadr, otrzymuje identyfikator, zliczany jest również czas, w jakim pozostaje ona w strefie do momentu jej opuszczenia. Ponadto możliwe jest ustawienie progu alarmowania dla obsługi w sytuacji, gdy w zadanej strefie znajdzie się zbyt dużo osób lub przebywają w niej za długo, i wezwanie wsparcia. Obsługa może też uzyskiwać raporty. Takie informacje przydają się szczególnie w restauracjach czy sklepach – tam dane dotyczące obsługi poszczególnych kas pomogą zoptymalizować pracę i znaleźć oszczędności oraz poprawić wydajność obsługi.

LINC POLSKA www.linc.pl

Sklep w chmurze?

Podstawowym zadaniem systemu monitoringu wizyjnego jest czuwanie nad bezpieczeństwem, np. placówki sprzedażowej. Firma się rozwija, potrzeba coraz więcej urządzeń, ale czy za tym rozwojem nadążają systemy zabezpieczeń? Czy urządzenia są odporne na cyberzagrożenia?
Odpowiedzią jest platforma **Eagle Eye Networks (EEN)**, światowy „numer 1" rozwiązań wizyjnych w chmurze. **EEN** to scentralizowany system wizyjny, który oferuje zarządzanie i nagrywanie strumieni wizyjnych bezpośrednio w chmurze. Za bezpieczną komunikację między kamerami a chmurą odpowiadają specjalne bramki wideo, buforujące dane i optymalizujące transmisję do chmury. Dostęp do systemu jest bezpośrednio z przeglądarki internetowej. Centralizacja jednostek ułatwia zarządzanie konfiguracją i wyszukiwaniem danych. Można też wykorzystać funkcje analizy wizji (detekcję przekroczenia linii, zliczanie osób, określenie obszaru zainteresowań klientów i wiele innych). Możliwość integracji na poziomie chmury z innymi systemami sklepowymi, np. POS, ułatwia wdrożenie i daje dużo większe możliwości przeglądania i weryfikacji danych.
System jest w pełni skalowalny, łatwy w rozbudowie i konfiguracji. Na bezpieczeństwo rozwiązania składają się procedury automatycznego połączenia opartego na sieciach prywatnych, certyfikatach, szyfrowaniu itp. Odbywa się to bez ingerencji użytkownika czy instalatora, dzięki czemu system jest łatwy i intuicyjny w obsłudze, zapewniając maksymalną ochronę danych.
Więcej na: **www.linc.pl**

PRO-SERVICE www.pro-service.com.pl

Detektory Tlenu „EurOx G/Lx5+"

Detektory Tlenu „EurOx G/Lx5+" są przeznaczone do stosowania w stacjonarnych systemach detekcji zmian lub pomiaru stężeń tlenu w powietrzu, poza strefami wybuchowymi. Mogą współpracować z szeroką gamą centralek i sterowników. Zasilanie 12 lub 24 V DC.
Parametry użytkowe:
W zależności od wersji mogą posiadać różne rodzaje wyjść:
– prądowe: ciągłe (4-20 mA) lub dwuprogowe 4/8/12 mA,
– napięciowe: typu OC (NC lub NO), dwa wyjścia sygnalizujące przekroczenie progów alarmowych AI1 i AI2,
– cyfrowe: łącze RS485, protokół Modbus RTU, detektor adresowalny.

Stosowane **czujniki**: fotoluminescencyjne, selektywne, o czasie eksploatacji powyżej 5 lat.
Detekcja wzrostu lub spadku **stężenia tlenu.**
Zakres pomiarowy: 0-25% V/V. **Progi alarmowe** (standardowo): 19/18% V/V (spadek stężenia) lub 22/23 % V/V (wzrost stężenia).
Na obudowie detektora **sygnalizacja optyczna (trzy diody): zasilania, przekroczenia progów alarmowych oraz awarii**.
Obudowa z tworzywa sztucznego PS, wpusty kablowe (dławice): PG11 + PG9.

Obszary zastosowań: laboratoria, oczyszczalnie ścieków, kontrola jakości powietrza, przemysł chemiczny itp.

PRO-SERVICE www.pro-service.com.pl

Trójgazowy detektor „Tmaster CO/LPG/NO2 G"

Detektory „Tmaster CO/LPG/NO2 G" stosuje się w stacjonarnych systemach detekcji tlenku węgla (CO), propanu-butanu (LPG) oraz dwutlenku azotu NO2, poza strefami zagrożonymi wybuchem.
Detektory są przeznaczone do współpracy z typowymi centralkami alarmowymi lub sterownikami przemysłowymi. Standardowe zasilanie zawiera się w granicach od 9 do 28 V DC. W zależności od wersji wykonania detektory posiadają wyjścia prądowe 4-20 mA, detekcyjne napięciowe OC (NC lub NO) lub cyfrowe (wyjście RS485 z protokołem Modbus RTU).
Do wykrywania tlenku węgla (CO) zastosowano selektywne, liniowe sensory elektrochemiczne o zakresie pomiarowym 0-500 ppm i progach alarmowych 40/100 ppm lub 30/60/150 ppm (zgodnie z normą PN-EN 50545-1).
Do wykrywania propanu-butanu (LPG) zastosowano nieselektywne sensory półprzewodnikowe o zakresie pomiarowym 0-50% DGW i progach alarmowych 10/30% DGW.
Do wykrywania dwutlenku azotu (NO_2) zastosowano selektywne, liniowe sensory elektrochemiczne o zakresie pomiarowym 0-20 ppm i progach alarmowych 3/6 ppm.
Detektory posiadają sygnalizację optyczną zasilania, przekroczenia progów alarmowych i awarii.
Detektor składa się z dwóch modułów: głównego (CO) i modułu LPG/NO_2 połączonych kablami. Obudowy modułów wykonano z tworzywa sztucznego PS o stopniu ochrony IP-33. Do podłączenia kabli służą wpusty kablowe (dławice) PG11 i PG9.
Głównym zastosowaniem detektorów są systemy detekcji w garażach, parkingach podziemnych i stacjach diagnostycznych pojazdów.

ROGER www.roger.pl

Obsługa parkingu w systemie RACS 5

System RACS 5, oprócz wielu funkcji związanych z kontrolą dostępu i automatyką budynkową, oferuje też kompleksową obsługę parkingów. W najprostszej wersji może być ona realizowana jako prosta kontrola przejścia, w której wjazd i wyjazd są uzyskiwane poprzez odczyt identyfikatora zbliżonego do czytnika znajdującego się w zasięgu ręki kierowcy. Można też zastosować czytnik dalekiego zasięgu (**UHF**), nadajnik radiowy (pilot) z odbiornikiem mającym wyjście Wiegand lub czytnik z funkcją identyfikacji przez Bluetooth (**np. MCT80M-BLE lub MCT-88M-IO**). W ostatnim przypadku identyfikacja użytkownika następuje z poziomu urządzenia mobilnego (smartfonu) z aplikacją **Roger Mobile Key** dostępną w wersji na system Android oraz **iOS** z odległości do 10 m.
Pojazdy można też identyfikować poprzez odczyt numerów rejestracyjnych. Wariant ten wymaga zastosowania kamery **Hikvision DS-2CD4A26FWD-IZSWG/P** podłączonej do kontrolera dostępu i współpracującej z nim bez pośrednictwa serwera.
Standardowe kontrolery Roger serii **MC16-PAC** umożliwiają kontrolę liczby samochodów znajdujących się na parkingu. Wyświetlane są informacje o wolnych miejscach oraz o ich braku, gdy liczba pojazdów osiągnie limit. Bardziej zaawansowaną funkcjonalnie obsługę parkingu zapewniają kontrolery serii **MC16-AZC**, które umożliwiają m.in. ustawienie indywidualnej liczby wjazdów na parking wybranym użytkownikom i limitów grupowych przydzielonych poszczególnym najemcom.

SCHRACK SECONET POLSKA www.schrack-seconet.pl

VISOCALL IP –system przyzywowy i komunikacji

System przyzywowy i komunikacji szpitalnej VISOCALL IP optymalizuje proces opieki w służbie zdrowia. Narzędzie jest w pełni IP, co oznacza, że każde urządzenie zapewnia komunikację głosową IP i jest podłączone do przełącznika sieciowego.
Rosnące wymagania nowoczesnego szpitala wymagają inteligentnych rozwiązań w zakresie planowania, wdrażania i przyszłych remontów.

System VISOCALL IP zapewnia:
- → uszanowanie prywatności pacjentów, którzy mogą decydować, czy chcą rozmawiać z personelem w sposób dyskretny, czy głośnomówiący,
- → możliwość prowadzenia rozmowy przez każdego z pacjentów w tym samym czasie,
- → optymalizację procesów z wykorzystaniem komunikacji głosowej i odbieraniem przywołań na urządzeniach systemowych lub mobilnych, np. smartfonach, telefonach DECT/VoIP itp.,
- → programowanie kierowanych do różnych osób i grup personelu przywołań specjalistycznych na terminalach przyłóżkowych bez konieczności modernizacji okablowania,
- → integrację z urządzeniami medycznymi, systemami bezpieczeństwa, TV, radiem, automatyką budynkową,
- → niskie koszty budowy i modernizacji (wykorzystanie infrastruktury LAN, standardowych przewodów sieciowych itp.).

System działa sprawnie nawet w przypadku uszkodzenia serwera. Jest instalowany w największych i najnowocześniejszych szpitalach, m.in. w nowej siedzibie Szpitala Uniwersyteckiego Kraków-Prokocim (ok. 925 łóżek), Wojewódzkim Szpitalu Zespolonym im. L. Rydygiera w Toruniu (ok. 670 łóżek).

SQUARETEC

www.squaretec.pl

VMS Senstar Symphony™

Buduj pozytywny wizerunek swojej firmy, zniechęcaj złodziei, chroń pracowników i klientów dzięki systemowi do zarządzania obrazem Senstar Symphony™ z wbudowanymi funkcjami analizy obrazu.

VMS idealne sprawdzi się m.in. w placówkach handlu detalicznego, które chcą zabezpieczyć przestrzeń i zbierać informacje biznesowe. Pozwala m.in. na:

- monitorowanie dużych przestrzeni, aby lokalizować kradzież oraz chronić klientów i pracowników;
- gromadzenie informacji biznesowych, aby poprawić obsługę klienta i zwiększyć sprzedaż;
- centralne zarządzanie systemami monitoringu wizyjnego w wielu lokalizacjach poprzez szybkie i łatwe aktualizowanie oprogramowania, zmiany ustawień i monitorowanie stanu systemu z jednej lokalizacji.

Dzięki alertom w czasie rzeczywistym, inteligentnemu wyszukiwaniu, raportowaniu i analizie wizyjnej otrzymujemy narzędzie, które zmienia sposób, w jaki sprzedawcy wykorzystują potencjał monitoringu sieciowego.

Funkcje analizy obrazu oferowane przez Senstar Symphony™:

- People Counter – zliczanie osób wchodzących i wychodzących, śledzenie tendencji w natężeniu ruchu;
- Rozpoznawanie twarzy – identyfikacja osób (znanych i nieznanych) do różnych zastosowań;
- Automatyczne rozpoznawanie numerów tablic rejestracyjnych – rozpoznawanie, śledzenie, zapisywanie i raportowanie ruchu pojazdów;
- Indoor People Tracking – wykrywanie podejrzanego zachowania i schematów poruszania się.

Więcej informacji na:
senstar.com, squaretec.pl/senstar

SYSTEM 7 SECURITY

www.system7.pl

Tagi RFID

Działająca od 29 lat firma System 7 Security z Bielska-Białej poszerzyła asortyment tagów RFID dostępnych natychmiast z jej magazynów. Obecnie do dyspozycji odbiorców hurtowych są praktycznie wszystkie modele identyfikatorów zbliżeniowych powszechnie stosowanych w Polsce.

Dzięki bogatemu doświadczeniu, odpowiednim zasobom finansowo-technicznym i silnym relacjom z najlepszymi fabrykami na Dalekim Wschodzie firma może zaproponować profesjonalnym odbiorcom ceny niespotykane w Europie. Dużym atutem jest zachowanie parametrów jakościowych trudnych do uzyskania przy indywidualnym imporcie, przejęcie obowiązków importera i standardowy jednodniowy termin dostawy na terenie kraju.

Oprócz popularnych tagów **RFID / NFC** dostępnych z magazynu (karty do nadruku, karty grube – *clamshell*, różnorodne breloki i opaski, naklejki, etykiety, dyski itp.), wyposażonych w wybrane chipy dla częstotliwości **100–125 kHz, 3,56 MHz** oraz **865 MHz,** firma **System 7 Security** w ramach swojej specjalizacji może zaprojektować i dostarczyć praktycznie dowolne rozwiązania.

Dostarczane standardowe identyfikatory zbliżeniowe współpracują m.in. z większością systemów kontroli dostępu, domofonowych czy alarmowych oferowanych na rynku.

Oferta jest przeznaczona wyłącznie dla odbiorców profesjonalnych – producentów, importerów i dystrybutorów urządzeń. **System 7 Security** nie prowadzi sprzedaży detalicznej tagów.

TP-LINK

www.tp-link.com.pl

Wydajne i kompaktowe przełączniki do monitoringu wizyjnego w domu

Przełączniki TL-SF1005P i TL-SG1005P zostały zaprojektowane do pracy w systemach monitoringu wizyjnego IP. Znajdujące się w nich porty uplink ułatwiają połączenie przełączników z istniejącą siecią domową. Dzięki zasilaniu PoE instalacja systemu jest łatwiejsza, bezpieczniejsza i mniej kosztowna. Urządzenia nie wymagają żadnej konfiguracji.

Najważniejsze cechy przełącznika TL-SG1005P:

- 5 portów RJ45 10/100/1000 Mb/s
- 4 porty PoE
- zgodność ze standardem IEEE 802.3af
- do 15,4 W mocy na każdym porcie PoE
- do 56 W mocy PoE łącznie
- QoS 802.1p/DSCP
- nie wymaga konfiguracji

Najważniejsze cechy przełącznika TL-SF1005P:

- 5 portów RJ45 10/100 Mb/s
- 4 porty PoE
- zgodność ze standardem IEEE 802.3af
- do 15,4 W mocy na każdym porcie PoE
- do 58 W mocy PoE łącznie
- nie wymaga konfiguracji.

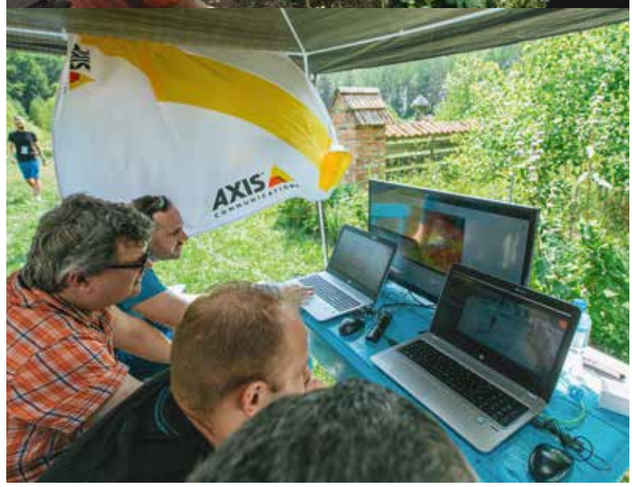
Oba przełączniki mają funkcję priorytetowania, dzięki której zabezpieczają system w momentach przeciążenia. Urządzenia podłączone do portów o wyższym priorytecie są zasilane w pierwszej kolejności.

Pierwsza edycja SECURITY BOOTCAMP 2019

To zupełnie nowa formuła szkolenia w branży. Security managerowie z największych w kraju firm i instytucji spotkali się na Security BootCamp, by w praktyce przetestować działanie różnych rozwiązań security w terenie.

Security BootCamp odbył się 13-14 czerwca w gospodarstwie Ziołowy Zakątek na Podlasiu. W wiejskim i leśnym otoczeniu uczestnicy mogli osobiście przekonać się o działaniu różnych rozwiązań security. Urządzenia dostarczyli partnerzy technologiczni, którzy służyli na miejscu poradami eksperckimi – stoiska z różnymi rodzajami zabezpieczeń zorganizowały firmy Axis Communications, Linc Polska, Nedap Security Management, Novatel, OPTEX Security i Securitas.

Drugiego dnia szkolenia odbyła się gra decyzyjna, podczas której uczestnicy wcielali się w osoby na różnych stanowiskach w firmie i organizacji, by zarządzać sytuacjami kryzysowymi lub im zapobiegać.



Mariusz Kucharski

a&s Polska

→ ***Jesteśmy w Korycinach na Podlasiu.*** *W tych okolicznościach przyrody zorganizowaliśmy Security BootCamp. To pierwsza edycja spotkania dla szefów bezpieczeństwa i osób odpowiedzialnych za bezpieczeństwo w firmach i instytucjach z całego kraju. Dopisała frekwencja, dopisała pogoda, dopisała też natura, w której mogliśmy testować rozwiązania security w praktyce.*

Jacek Wójcik

Optex

→ *Optex jest producentem czujek zewnętrznych, więc to jest naturalne środowisko, w którym nasze produkty powinny być prezentowane. W tych warunkach najlepiej pokazują swoje możliwości, swoją technologię, swoje różnice względem innych produktów.*

Karol Dominiczak

Axis Communications

→ *Na tym wydarzeniu przedstawiamy aplikacje analityczne, głównie związane z ochroną obwodową, które możemy zainstalować w kamerach. Dzięki takiej aplikacji kamera staje się detektorem, wspomaga nas w ochronie perymetrycznej.*

Jakub Sobek

Linc Polska

→ *Korzystając z tych pięknych okoliczności natury, przedstawiamy rozwiązania, które rzeczywiście w terenie możemy zaprezentować najlepiej, i te, które są właśnie do zastosowania zewnętrznego. Pokazujemy naszą wieżę do monitoringu wizyjnego, która jest odpowiedzią na potrzeby klientów oczekujących rozwiązania na tu i teraz. Wszędzie tam, gdzie nie ma infrastruktury technicznej, gdzie trzeba uruchomić system monitoringu wizyjnego, a infrastruktura lokalna na to nie pozwala, właśnie tam sprawdzi się wieża HiTower, którą jesteśmy w stanie uruchomić u klienta tak naprawdę w ciągu 15 minut.*

Paweł Grzywa

Securitas

→ *Platforma ma głowicę wyposażoną w sześć kamer, w tym dwie kamery termowizyjne. Potrafimy ustawić analizę, która ma na celu ochronę perymetryczną danego obszaru. Jest to wejście w obszar lub przekroczenie danej linii. Jeśli pojawi się intruz, wówczas nasz operator ma możliwość wydania komunikatu głosowego. Platforma jest skuteczną formą ochrony zdalnej i – jeśli jest taka potrzeba – może optymalizować koszty ochrony fizycznej stałej.*

Piotr Oleksiewicz

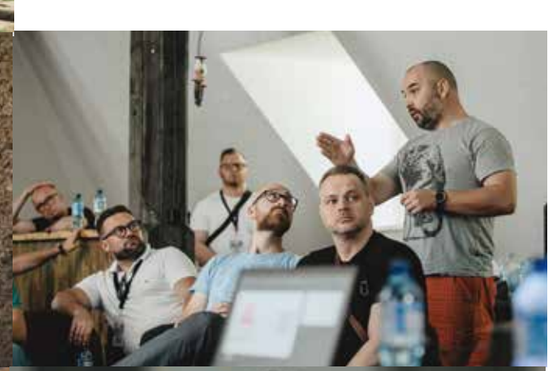
Nedap Security Management

→ *Dla naszych gości, uczestników BootCampu przygotowaliśmy skrzynię pełną cudów, prezentację produktową i łamigłówkę logiczną, którą uczestnicy muszą rozwiązać po to, żeby dostać się do nagród, które właśnie w tej skrzyni się znajdują.*

Artur Kreihs

Novatel

→ *Pokazujemy przede wszystkim system Pablo. Jest to system służący do lokalizacji osób na stanowiskach swojej pracy, który obsługuje również zdarzenia alarmowe. Dzięki nim możemy zapewnić pracownikom bezpieczeństwo, ponieważ wiemy, gdzie kto przebywa, i jeżeli potrzebuje pomocy, jesteśmy od razu o tym powiadamiani.*



Tomasz Ciećwierz

PKP Cargo

→ *Pierwszy dzień był fenomenalny. Bardzo mi się podobały prezentacje poszczególnych firm.*

Paweł Macheta

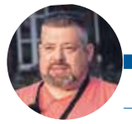
Dębica / Goodyear

→ *Jest to mus dla każdej dużej korporacji, dla każdej firmy, żeby szukać innych rozwiązań. Na pewno takie dziś zobaczyłem.*

Tomasz Goliszek,

BNP Paribas

→ *Tutaj pojawia się większa interakcja pomiędzy nami, możemy zapoznać się, wymienić się doświadczeniami. Jest rewelacyjnie, o wiele lepiej niż na zwykłych szkoleniach.*



Mirosław Lukowski,

Carrefour

→ ***Żaden PowerPoint nie jest w stanie pokazać**, jak sprzęt powinien działać w terenie. Tu mamy taką możliwość.*

Mirosław Miniszewski

BlackOnion

→ ***Gra decyzyjna jest to taki rodzaj RPG-a biznesowego**, gdzie wymyślamy sobie pewną sytuację, komplikujemy ją i gramy w różne wersje, które mogą się w trakcie tej gry wydarzyć.*

Tomasz Guzikowski

Ciech

→ ***Każdy z uczestników ma swoje spojrzenie**, swój pogląd na sytuacje, które zostały w tej grze zaprezentowane.*

Daniel Piórkowski,

Alior Bank

→ *Menedżer może nie dostrzec jakiegoś ryzyka, jakiegoś niebezpieczeństwa, którego ktoś już doświadczył, na podstawie konkretnego przypadku.*

Michał Kilian

Comarch

→ *To szkolenie jest efektywne, jest fajne, jest przyjemne. Na pewno warto tu być.*

Stanisław Bałda

PWPW

→ *Można się podzielić wiedzą i doświadczeniem. Potem przełożyć to na swoje środowisko.*

Piotr Kiliszek

Jastrzębska Spółka Węglowa

→ *BootCamp to nowa forma, nowe działanie. Wyjdźmy z sal szkoleniowych w plener, poznajmy mocne i słabe strony systemu. To kolejny krok do przodu „a&s”.*

Statystyki

Najnowsze dane branżowe i analizy rynku security

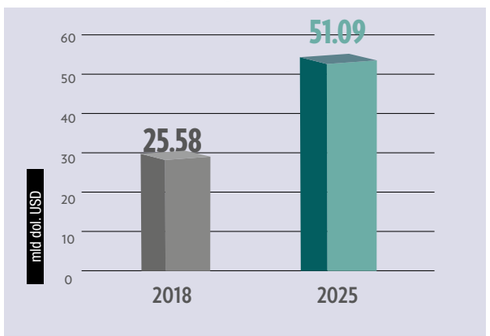
TEKST
a&s International

Rynek ITS osiągnie do roku 2025 wartość 51,09 mld USD

Światowy rynek inteligentnych systemów transportowych (ITS) został wyceniony w 2018 r. na 25,58 mld USD. Według prognozy firmy Grand View Research w 2025 r. ma on osiągnąć 51,09 mld USD. Analitycy spodziewają się, że sprzedaż zaawansowanych systemów transportu publicznego będzie rosła najszybciej – przy średniej rocznej stopie wzrostu wynoszącej 12,1 proc. w latach 2019–2025.

Siłą napędową rynku ITS jest wykorzystanie tych systemów do zwiększenia bezpieczeństwa i zmniejszenia liczby wypadków drogowych. Oczekuje się, że surowe przepisy mające na celu poprawę bezpieczeństwa kierowców w Europie i Ameryce Płn. przyczynią się do rozwoju branży i większego wykorzystania ITS-ów. Z kolei w regionie Azji i Pacyfiku w prognozowanym okresie ma być notowany wzrost nawet o 13-proc. rocznie, na co będą miały wpływ inicjatywy rządowe zmierzające do wdrożenia systemów ITS. Skupione wokół ITS stowarzyszenia oceniają, że zastosowanie zaawansowanych systemów zarządzania ruchem (ATMS – *Advanced Traffic Management Systems*) skutecznie skraca czas jazdy (o 25 proc.) oraz czas oczekiwania na zmianę sygnalizacji świetlnej (od 20 do 30 proc.). Przyczynia się również do ograniczenia emisji gazów cieplarnianych.

Wartość światowego rynku ITS



Źródło: Grand View Research

Globalna wartość rynku kamer do monitoringu domu wzrośnie do
→ 1,3 mld $
Źródło: Allied Market Research

Światowy rynek ANPR w 2025 r. osiągnie
→ 1,7 mld $
Źródło: Research and Markets

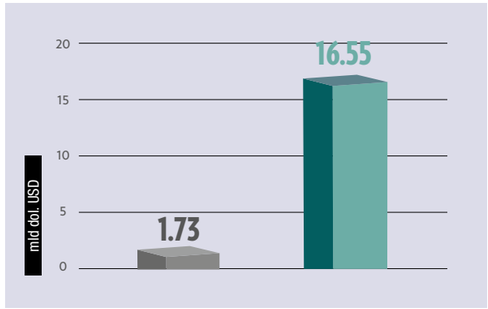
Globalny rynek edge computing osiągnie do 2025 r. wartość 16,55 mld USD

Globalny rynek urządzeń brzegowych (*edge computing*) osiągnie do 2025 r. wartość 16,55 mld USD przy średnim rocznym wzroście wynoszącym 32,8 proc.

Według raportu Allied Market Research światowy rynek przetwarzania w urządzeniach brzegowych sieci w 2017 r. osiągnął wartość 1,73 mld USD, do 2025 r. może wzrosnąć do 16,55 mld USD (przy średniej rocznej stopie wzrostu w latach 2018–2025 szacowanej na 32,8 proc.). W prognozowanym okresie segment usług ma osiągnąć jeszcze większy przyrost, nawet 35,6 proc., na co wpłynie większe zapotrzebowanie na zarządzanie danymi analitycznymi w całym okresie użytkowania.

Jeśli chodzi o zastosowania, przewiduje się, że najwyższym tempem wzrostu ocenianym na 35,9 proc. w latach 2018–2025 wykaże się segment samochodów na stałe połączonych z Internetem (*connected cars*). Będzie to wynikać z rosnącego zapotrzebowania na systemy typu audionawigacyjne (*infotainment*) oraz inne usługi działające w czasie rzeczywistym. Prognozuje się także, że silną pozycję w zakresie urządzeń brzegowych utrzyma branża zabezpieczeń, generując niemal jedną piątą światowych przychodów do 2025 r. Wpłyną na to korzyści z wykrywania zagrożeń w czasie rzeczywistym i zmniejszania opóźnień sieci.

Wartość światowego rynku Edge Computing



W ujęciu geograficznym region Azji i Pacyfiku odnotuje w prognozowanym okresie średni wzrost sprzedaży urządzeń brzegowych na poziomie 35,1% w związku ze wzrostem zapotrzebowania na urządzenia mobilne i technologie komórkowe w gospodarkach wschodzących (Chiny i Indie).

Największym rynkiem w 2017 r. była Ameryka Płn. (blisko dwie piąte globalnego rynku). Do 2025 r. ten region powinien odnotowywać największe przychody w opisywanej branży.

Światowy rynek inteligentnych czujników dymu do 2024 r. wzrośnie do ponad
→ 2 mld $
Źródło: Arizton

Światowy rynek kart SD ma do 2022 r. przekroczyć
→ 8,9 mld $
Źródło: Persistence Market Research

Optyka dla każdego

cz. 4

To już ostatni artykuł z cyklu „Optyka dla każdego”. Pora na opisanie budowy i klasyfikacji obiektywów, uzupełnienie informacji dotyczących rozdzielczości optycznej, wyjaśnienie działania migawki i ekspozycji oraz na krótkie podsumowanie.

TEKST
Piotr Rogalewski

MTF obiektywu

W poprzednim artykule poruszyłem kwestię rozdzielczości optycznej obiektywu. W uzupełnieniu tego zagadnienia postanowiłem omówić jeszcze jeden bardzo istotny parametr, który jest z rozdzielczością optyczną ściśle powiązany, a którego w opracowaniach dotyczących telewizji dozorowej szukać ze świecą. Chodzi o MTF obiektywu (*Modulation Transfer Function*), czyli w dosłownym tłumaczeniu funkcję przenoszenia (przekazywania) modulacji. Pomimo złożonej nazwy znaczenie tego parametru stosunkowo łatwo wyjaśnić. Otóż MTF określa procentową zmianę kontrastu po przejściu obrazu przez obiektyw w stosunku do obrazu oryginalnego przed obiektywem [1] i wyraża się wzorem:

$$MTF = \frac{Kp}{Ko}\,100\% \qquad (1)$$

gdzie: MTF to współczynnik przenoszenia modulacji obiektywu,
Kp – kontrast obrazu po przejściu przez obiektyw,
Ko – kontrast obrazu oryginalnego przed obiektywem.

Czym jest kontrast? Najkrócej rzecz ujmując, to stosunek jasności najjaśniejszego do najciemniejszego punktu obrazu. Aby lepiej to wyjaśnić, wróćmy do rozdzielczości optycznej i testowej tablicy rozdzielczości z pionowymi liniami [2]. Można łatwo zdefiniować kontrast dla pary linii czarna + biała. Opisuje to wzór:

$$Ko\ (lub\ Kp) = \frac{Lmax - Lmin}{Lmax + Lmin} \qquad (2)$$

gdzie: Ko – kontrast dla pary linii czarna + biała,
Kp – kontrast po przejściu obrazu przez obiektyw,
Lmax – maksymalna jasność linii białej,
Lmin – minimalna jasność linii czarnej.

Jeśli jako jasność minimalną przyjmiemy wartość 0, a maksymalną wartość 100, otrzymamy Ko równe 1. Załóżmy, że po przejściu przez obiektyw maksymalna jasność linii białej jest równa 70, a minimalna jasność linii czarnej wynosi 10. Po podstawieniu do wzoru (2) otrzymamy *Kp* równe 0,75. Po podstawieniu wartości *Kp* i *Ko* do wzoru (1) otrzymamy współczynnik MTF równy 75%. Oznacza to, że kontrast obrazu odwzorowanego przez obiektyw stanowi 75% kontrastu obrazu oryginalnego (lub inaczej: kontrast obrazu oryginalnego zmalał o 25% po przejściu przez obiektyw).
Dlaczego współczynnik MTF jest tak ważny? Po pierwsze dlatego, że uwzględnia wpływ na kontrast całej konstrukcji obiektywu – wszystkich soczewek, przysłony, powłoki antyrefleksyjnej itd. Po drugie dlatego, że rozdzielczość optyczna obiektywu, określana jako para linii na milimetr (lpmm lub lp/mm) [2], jest często podawana „w komplecie” z MTF, dzięki czemu możemy określić, przy jakiej procentowej utracie kontrastu można mówić o danej rozdzielczości. Jeśli wartość MTF nie została podana, przyjmuje się, że rozdzielczość optyczna lp/mm jest określona dla współczynnika MTF równego 50. Po trzecie – producenci obiektywów często w materiałach katalogowych prezentują wykres MTF w funkcji liczby przysłony, co od razu pozwala ocenić, jak obiektyw radzi sobie z przenoszeniem obrazu w różnych warunkach oświetleniowych i przy różnej głębi ostrości.

Obiektyw

Obiektyw to przyrząd optyczny przenoszący obraz obserwowanego obiektu na matrycę światłoczułą przetwornika obrazowego kamery. Jest okiem kamery, a jego jakość i charakterystyka mają pierwszorzędne znaczenie dla wszystkich procesów obróbki obrazu. Inwestycję w najdoskonalszą kamerę bardzo wysokiej rozdzielczości, wyposażoną w wysokiej jakości procesor DSP może zniweczyć obiektyw słabej jakości. Dla obiektywu nie ma uniwersalnego wzoru matematycznego opisującego jego działanie, gdyż poszczególne modele mogą się od siebie znacznie różnić liczbą soczewek, ich rodzajem, materiałem, z którego są wykonane, odległościami pomiędzy soczewkami itd. Wzorem przybliżonym, który można zastosować, jest równanie soczewki opisane w 2. części cyklu „Optyka dla każdego”. Na szczęście podstawowego parametru obiektywu, jakim jest ogniskowa, nie musimy wyliczać samodzielnie, producent zawsze go podaje.
Przykładowy obiektyw w przekroju przedstawiono poniżej na *fot.*

Przekrój obiektywu fotograficznego. Źródło: www.pinterest.com

OBIEKTYWY DLA TELEWIZJI DOZOROWEJ (Grafika: Piotr Rogalewski)

Pole widzenia			
Telefoto Pole widzenia >20°	Standardowe Pole widzenia ~50°	Szerokokątne Pole widzenia ≥90°	Rybie oko Pole widzenia ≥180°

Przekątna przetwornika				
1"	2/3"	1/2"	1/3"	1/4"

Przysłona			
Stała	Ręczna	DC	P-Iris

Ogniskowa	
Stałoogniskowe	Zmiennoogniskowe

Regulacja ogniskowej i ostrości	
Ręcznie	Elektrycznie (silnik)

Rozdzielczość kamery	
Standardowa (PAL)	Megapikselowa

Korekcja do pracy w podczerwieni	
Z korekcją IR	Bez korekcji IR

Jego budowa może być złożona – automatyka przysłony, sterowanie ostrością, wiele różnych soczewek, pierścieni itd. Jeszcze bardziej skomplikowany jest obiektyw z elektryczną regulacją ogniskowej i ostrości. Wszystko zależy od konkretnego rodzaju obiektywu i wymaganego zestawu funkcji i parametrów. Ogólne podsumowanie klasyfikacji obiektywów podano w *tabeli*.

Kryteriów klasyfikacji jest kilka. Pierwszym i chyba najbardziej oczywistym jest pole widzenia. Kolejnym jest wielkość przetwornika obrazu, do którego dobierany jest obiektyw. I tu na chwilę warto się zatrzymać i zastanowić: co się stanie, gdy do kamery z przetwornikiem 1/2" zamontujemy obiektyw 1/3"? Powierzchnia obrazowania obiektywu jest mniejsza od powierzchni przetwornika, więc w efekcie na obrazie z kamery otrzymamy obraz nie tylko „za obiektywem", ale także krawędzi obudowy samego obiektywu, co nie jest zjawiskiem pożądanym. W sytuacji odwrotnej, czyli w przypadku zamontowania obiektywu 1/2" do kamery z przetwornikiem 1/3", otrzymamy wprawdzie obraz normalny, ale o mniejszym polu widzenia niż wynikałoby to z ogniskowej obiektywu (część pola widzenia obiektywu jest w takim przypadku niewykorzystana). Najlepszym pomysłem jest zatem dobór wielkości powierzchni obrazowania obiektywu równej wielkości przetwornika.

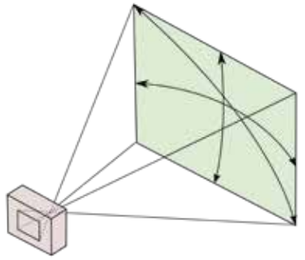
Następnym kryterium klasyfikacji obiektywów jest rodzaj przysłony. Jest tu spory wybór, począwszy od najprostszej przysłony stałej, przez regulowaną ręcznie, na automatyce typu DC i P-Iris skończywszy. W przypadku przysłony automatycznej typu DC mechanizmem przysłony steruje kamera. Podobnie jest w przypadku przysłony typu P-Iris, ale mamy tu dużo większą precyzję kontroli głębi ostrości [2].

Innym kryterium jest ogniskowa. Obiektywy stałoogniskowe narzucają stałe pole widzenia, ale są tańsze od zmiennoogniskowych, gdyż nie mają mechanizmu zmiany ogniskowej (zoom), dodatkowych soczewek, mechanizmu przesuwania ich względem siebie itd. W wielu przypadkach wybór kamery z wbudowanym obiektywem stałoogniskowym (np. kopułkowe) pozwala na spore oszczędności, szczególnie przy większej liczbie kamer. Ogniskowa w obiektywach zmiennoogniskowych może być regulowana ręcznie lub za pomocą miniaturowego silnika, podobnie jak ostrość.

Kolejne kryterium to rozdzielczość kamery, dla której dany obiektyw jest właściwy. Rozdzielczość można umownie podzielić na standardową (właściwą np. dla starych kamer analogowych o rozdzielczości 720 x 576 pikseli) i megapikselową. Podkreślam, że jest to podział bardzo umowny, a temat rozdzielczości optycznej poruszałem szczegółowo w poprzedniej części cyklu.

Pole widzenia

Po ogniskowej drugim niezwykle ważnym parametrem obiektywu jest jego pole widzenia. Typowy przetwornik obrazu w kamerze telewizji dozorowej ma kształt prostokąta, można zatem określić dla niego trzy obszary pola widzenia: poziome, pionowe lub po przekątnej (rys. 1).



Rys. 1. Pole widzenia obiektywu może być poziome, pionowe lub po przekątnej. Źródło: www.wikipedia.org (autor: Dick Lyon, USA)

Jak pokazano na *rys. 1*, pole widzenia zależy nie tylko od ogniskowej obiektywu, ale także od wielkości matrycy przetwornika obrazowego. Kąt widzenia dla każdego boku pola widzenia można obliczyć z prostego wzoru, korzystając z funkcji arcus tangens [3]:

$$\alpha = 2arctg\,\frac{d}{2f} \qquad (3)$$

gdzie: α – szukany kąt widzenia,
d – rozmiar przetwornika obrazowego dla boku odpowiadającego szukanemu kątowi (poziomy, pionowy lub przekątna),
f – ogniskowa obiektywu.

W praktyce nie musimy robić obliczeń „na piechotę", ponieważ chyba każdy producent kamer dozorowych ma obecnie w swoich zasobach różnego rodzaju kalkulatory pola widzenia. Dostępne są też programy wspomagające projektowanie, które potrafią automatycznie wyrysować pole widzenia na podkładzie graficznym (np. mapa terenu) na podstawie wprowadzonych danych o ogniskowej, przetworniku i odległości.

Dobór obiektywu do uzyskania pożądanego pola widzenia jest jednym z kluczowych elementów procesu projektowania systemu telewizji dozorowej, szczególnie w kontekście norm i rozporządzeń precyzujących wymogi na takie systemy w zakresie detekcji, identyfikacji, obserwacji ogólnej itd.

Przejdę teraz do zagadnień związanych *stricte* nie tyle z optyką, ile z elektronicznym przetwarzaniem obrazu. Są jednak tak bardzo istotne, że w ujęciu dotyczącym kamer telewizji dozorowej nie sposób ich pominąć.

Migawka

W profesjonalnych aparatach fotograficznych migawka jest urządzeniem fizycznie otwierającym dopływ światła do przetwornika (lub kliszy fotograficznej) na ściśle określony czas. W zależności od typu może to być np. zestaw prostokątnych płytek (migawka szczelinowa), listków w kształcie sierpa (migawka centralna) lub inna konstrukcja. W niektórych rozwiązaniach migawka centralna może być jednocześnie przysłoną (np. w cyfrowych aparatach kompaktowych starszej generacji). Zrobieniu zdjęcia profesjonalnym aparatem towarzyszy najczęściej wyraźnie słyszalny trzask lub pstryknięcie (w tanich aparatach kompaktowych jest on emulowany odtworzeniem dźwięku przypominającego takie pstryknięcie). Jest to właśnie moment zadziałania mechanizmu migawki (a przycisk, którym robimy zdjęcie, nosi nazwę spustu migawki).

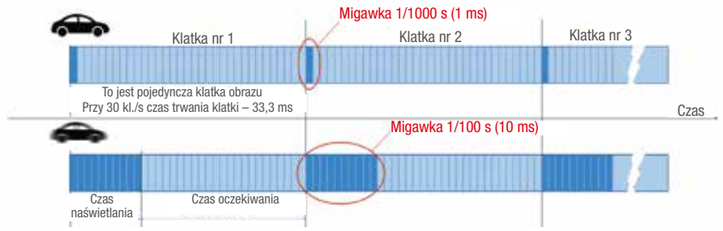
Nas jednak interesuje migawka w kamerze telewizji dozorowej, gdzie można ją w zasadzie zaliczyć do cyfrowej, elektronicznej obróbki obrazu. Stąd też pochodzi jej nazwa – migawka elektroniczna, często oznaczana skrótowcem AES (*Automatic Electronic Shutter*). Rola migawki ma na tyle duży wpływ na finalny obraz generowany przez kamerę, że należy jej poświęcić uwagę, szczególnie że migawki typu AES są obecnie powszechnie stosowane w aparatach fotograficznych smartfonów, a nawet modelach profesjonalnych jako uzupełnienie migawki mechanicznej (migawka hybrydowa). Rozwiązanie to zapewnia wiele korzyści w porównaniu z migawką mechaniczną – bardzo duże prędkości działania, bezgłośna praca (ważne np. przy fotografowaniu dzikich zwierząt), brak elementów mechanicznych (skracających trwałość układu), duży zakres regulacji czasu ekspozycji.

Jak zatem jest realizowana funkcja migawki elektronicznej? Otóż przetwornik obrazu „zbiera" dane o obrazie tylko w momencie podania odpowiednich sygnałów elektrycznych na jego wejścia sterujące. Ich częstotliwość określa czas, w jakim przetwornik odczytuje dane o oświetleniu swojej powierzchni. Regulacja tego czasu odpowiada regulacji czasu migawki mechanicznej. W praktyce proces sterowania migawką przetwornika jest dość złożony w zależności od układu może to być „przemiatanie" kolejnych wierszy matrycy (migawka postępowa) lub całościowa obsługa wszystkich pikseli (migawka globalna). Migawka elektroniczna ma jeszcze jedną zaletę wynikającą z prędkości jej działania: **szybka migawka przy dobrym oświetleniu pozwala na zmniejszenie otworu przysłony, co daje dużą głębię ostrości obrazu.**

Dla uzyskania właściwej ostrości i wyrazistości szybko poruszających się obiektów o wiele większe znaczenie ma czas migawki niż liczba klatek na sekundę

Migawka, liczba klatek i WDR – jak to pogodzić?

Omawiając migawkę, nie sposób pominąć dwóch bardzo istotnych zagadnień ściśle z nią związanych – liczby klatek obrazu generowanych przez kamerę oraz funkcji WDR (*Wide Dynamic Range*), czyli szerokiego zakresu dynamiki obrazu. Do napisania tego podrozdziału zainspirowało mnie dość powszechne wśród instalatorów przekonanie, że duża liczb klatek na sekundę przekłada się na lepiej uchwycone, ostre i wyraźne szybko poruszające się obiekty. Rzeczywiście, duża liczba klatek czasem się przydaje, np. gdy trzeba szczegółowo zobrazować poszczególne fazy ruchu dynamicznie poruszającego się obiektu. Jednak dla uzyskania właściwej ostrości i wyrazistości obiektu w tych fazach ruchu o wiele większe znaczenie ma prędkość migawki. Posłużę się tu przykładem kamer do rozpoznawania tablic rejestracyjnych (LPR – *License Plate Recognition* lub ANPR – *Automatic Number Plate Recognition*). Aby uzyskać wyraźny, a przede wszystkim ostry obraz tablicy rejestracyjnej, lepszą konfiguracją będzie prędkość 10 kl./s + migawka 1/1000 sekundy niż prędkość 60 kl./s + migawka 1/250 sekundy. I to nie tylko ze względu na przetwarzanie danych w algorytmie rozpoznawania tablic. W wyjaśnieniu pomoże *rys. 2*.



Rys. 2. Relacja czasu migawki i liczby klatek na sekundę generowanych przez kamerę
Grafika: Piotr Rogalewski

Przy prędkości 30 kl./s czas trwania pojedynczej klatki obrazu wynosi 33,3 ms (30 · 33,3 ms ≈ 1000 ms). Czy to oznacza, że przez całe 33,3 ms przetwornik „czyta" obraz? Nie. To oczywiście zależy od aktualnej prędkości migawki. Jeśli kamera obserwuje szybko poruszający się obiekt, np. samochód na drodze, a migawka jest ustawiona na 1/1000 s, to przetwornik będzie „łapał" obraz właśnie przez ten czas i już po upływie 1 ms zamknie okno naświetlania, czekając kolejne 23,3 ms na następną klatkę obrazu.

Konsekwencje tego są dwie. Po pierwsze, szybko poruszający się obiekt będzie eksponowany na przetworniku przez krótką chwilę, więc jego obraz w ruchu będzie ostry i wyraźny. Po drugie, czas „zbierania" światła z przetwornika jest bardzo krótki, a więc obraz będzie miał słabą jasność. Scena musi być zatem bardzo dobrze oświetlona światłem widzialnym (np. słoneczny dzień) lub promieniowaniem podczerwonym, gdy pracuje w trybie czarno-

Zawsze trzeba znaleźć równowagę między czasem migawki, czułością i wartością przysłony, a zmianę jednego z tych parametrów powinniśmy niejako skompensować dostosowaniem dwóch pozostałych

-białym (tak się właśnie dzieje w kamerach ANPR). Jeśli prędkość migawki zmniejszymy dziesięciokrotnie, do 1/100 s, to przetwornik będzie „czytał" obraz przez 10 ms i czekał 13,3 ms na kolejną klatkę. Obraz uzyska lepszą jasność, gdyż czas ekspozycji przetwornika będzie 10x dłuższy, ale szybko poruszający się pojazd stanie się w kadrze rozmazany, bo jego faza ruchu będzie się eksponować 10x dłużej niż w poprzednim przypadku.

Sytuacja ta wyjaśnia także efekt „smużenia" (w żargonie często nazywanego „duchem") występującego np. w nocy, gdy automatyka ekspozycji kamery stara się maksymalnie naświetlić matrycę przetwornika, korzystając z dłuższych czasów migawki. W fotografii długie czasy migawki dla ekspozycji szybko poruszających się obiektów wykorzystuje się nieraz celowo, np. by uzyskać efektowne zdjęcia „rozciągniętych" świateł samochodowych w nocnym ruchu ulicznym.

Drugie zagadnienie dotyczy relacji prędkości migawki i działania funkcji WDR, która tak balansuje kontrast, aby na obrazie nie występowały miejsca prześwietlone ani ukryte w cieniu. Przykładowo, sylwetka człowieka stojącego w ciemnym pomieszczeniu na tle szklanych drzwi, przez które wpada ostre światło słoneczne, „zginie" na obrazie i nie będzie można rozpoznać takiej osoby – światło z zewnątrz oślepi kamerę, nie pozwalając także dostrzec szczegółów za drzwiami.

Rozwiązaniem jest właśnie funkcja WDR, która radzi sobie z taką sytuacją. Kluczem jest tu migawka. Spójrzmy ponownie na rys. 2. Jak widać 33,3 ms to całkiem sporo, bo można w czasie trwania jednej klatki wykonać (jedno po drugim) dwa, a nawet trzy lub cztery ujęcia z różnymi czasami migawki. Wracając do przykładu ze szklanymi drzwiami, wykonanie ujęcia z prędkością np. 1/1000 s pozwoli uchwycić elementy skąpane w świetle, za drzwiami, ponieważ krótki czas migawki to ciemniejszy obraz. Z kolei drugie ujęcie z prędkością np. 1/50 s pozwala na dobre naświetlenie sylwetki osoby stojącej w ciemnym pomieszczeniu. Złożenie tych dwóch ujęć i uśrednienie kontrastu z obu z nich da w efekcie wyraźny obraz zarówno osoby, jak i tła za drzwiami. Tak

właśnie w wielkim skrócie działa funkcja WDR (w rzeczywistości proces składania ujęć jest bardziej złożony niż proste uśrednianie). **Mamy przy okazji wyjaśnienie, dlaczego często po włączeniu funkcji WDR maksymalna liczba generowanych przez kamerę klatek na sekundę spada o połowę (o czym producenci kamer najczęściej nie wspominają w karcie katalogowej).** Otóż aby przetwornik „zdążył" wygenerować klatkę obrazu, w trakcie której wykonuje dwa ujęcia z dwiema (lub więcej) prędkościami migawki, potrzebuje na to więcej czasu. Czasu, który można uzyskać, zwiększając długość trwania klatki, co oczywiście automatycznie skutkuje spadkiem liczby generowanych klatek. Nie zawsze musi tak być, wszystko zależy od rodzaju zastosowanego w kamerze przetwornika obrazu i pożądanej prędkości odświeżania (są kamery, które potrafią generować 30 czy nawet 60 kl./s przy włączonej funkcji WDR). Ta sama kwestia wyjaśnia również, dlaczego bardzo często po włączeniu funkcji WDR zakres ręcznej regulacji prędkości migawki elektronicznej kamery zostaje zawężony lub w ogóle możliwość regulacji migawki zostaje zablokowana (zależy to od konkretnego modelu kamer i producenta).

Trójkąt ekspozycji

Wiadomo już, co to są przysłona, migawka, czułość i głębia ostrości. Jedną z najistotniejszych kwestii związanych z optyką – zarówno w fotografii, jak i telewizji dozorowej – jest zrozumienie wzajemnych zależności między tymi parametrami ekspozycji. Ekspozycja to ilość światła padającego na powierzchnię światłoczułą przetwornika obrazu (w fotografii analogowej na powierzchnię kliszy fotograficznej), przy czym ta ilość jest zdeterminowana przez trzy czynniki: wielkość przysłony, migawkę i czułość [4]. W zrozumieniu zależności między tymi parametrami pomoże trójkąt ekspozycji przedstawiony na *rys.* 3.

Rys. 3. Trójkąt ekspozycji Grafika: Piotr Rogalewski

W sytuacji, gdy skuteczność działania systemu zależy od wielu powiązanych ze sobą parametrów, najczęściej pojawia się kwestia kompromisu pomiędzy wartościami tych parametrów. Tak też jest w przypadku trójkąta ekspozycji. Każdy bok trójkąta oznacza parametr ekspozycji mający bezpośredni związek z określoną wielkością fizyczną. Zaczynając od lewego boku – prędkość migawki ma wpływ na odwzorowanie ruchu, co wyjaśniłem, opisując działanie migawki. Prawy bok trójkąta to czułość ściśle związana z poziomem szumów przetwornika obrazu. Dolny bok natomiast to przysłona, od której zależy ilość światła padającego na przetwornik, a także głębia ostrości. Najważniejsza jest jednak wzajemna zależność wszystkich tych parametrów.

Przykładowo, aby uzyskać dobrej jakości obraz szybko poruszającego się obiektu, potrzebujemy szybkiej migawki. To jednak spowoduje spadek jasności obrazu, bo czas ekspozycji będzie krótki. Powstaje zatem problem właściwego obrazowania ruchu w słabych warunkach oświetleniowych. Można to skompensować większym otwarciem przysłony, ale im bardziej ją otworzymy, tym krótsza będzie głębia ostrości obrazu i mniejszy zasięg skutecznej obserwacji. Trzeba więc wykorzystać trzeci bok trójkąta i przy optymalnej wartości przysłony zwiększyć czułość, ale też w granicach rozsądku, bo w przeciwnym razie popsujemy obraz dużą zawartością szumów. Z powyższego przykładu wynika, że zawsze trzeba znaleźć równowagę między czasem migawki, czułością i wartością przysłony, a zmianę jednego z tych parametrów powinniśmy niejako skompensować dostosowaniem dwóch pozostałych.

W praktyce telewizji dozorowej sprawa się nieco komplikuje. O ile czułość można regulować w szerokim zakresie w aparatach fotograficznych (tzw. wartość ISO), o tyle w kamerach CCTV/VSS takiej możliwości nie ma. Czułość jako wartość katalogowa wyrażona jednostką lux jest podawana w parze z liczbą przysłony (i czasami także wartością IRE)[1]. W kamerach z mechanicznie odsuwanym filtrem podczerwieni jest podawana odrębnie dla trybu kolorowego i czarno-białego. To wartość stała, a mechanizm „podciągania" jasności bazuje na automatycznej regulacji wzmocnienia sygnału wizyjnego ARW (AGC – *Automatic Gain Control*). Poziom wzmocnienia można najczęściej regulować skokowo, jednak zbyt duże wzmocnienie AGC (analogicznie jak zbyt duża wartość ISO w aparacie fotograficznym) może spowodować wzrost „śnieżenia" na obrazie, bo oprócz wzmocnienia użytecznego sygnału wzmocnieniu ulegną także szumy przetwornika i elektroniki obróbki obrazu. Ponadto w obiektywach z przysłoną automatyczną (DC lub P-Iris) automatyka kamery musi znaleźć „złoty środek" między czasem elektronicznej migawki a wartością przysłony. Zdarza się, że niedbale napisane oprogramowanie układowe (*firmware*) kamery rujnuje bardzo dobre parametry jej przetwornika i drogiego obiektywu.

[1] Kwestie dotyczące sposobów pomiaru i podawania parametrów czułości w kamerach CCTV są na tyle obszerne, że wymagają szczegółowego opisu, wykraczającego poza ramy tego artykułu.

Na zakończenie

Kończąc cykl „Optyka dla każdego", warto poświęcić chwilę na podsumowanie. Wiemy, czym jest światło, jakie zjawiska mogą zachodzić z jego udziałem, co to jest widmo i fala elektromagnetyczna, jak ogólnie działa ludzkie oko i czemu zawdzięczamy widzenie barwne. Wiemy, co to jest optyka geometryczna, promień, soczewka, refrakcja, dyfrakcja oraz dlaczego dzięki dyspersji możemy zobaczyć tęczę. Poznaliśmy także pojęcia rozdzielczości optycznej, przysłony, głębi ostrości, aberracji sferycznej i chromatycznej oraz wiemy, jak te aberracje kompensować. Wiemy, co to jest plamka Airy'ego i czym się różni od dysku Airy'ego, jak działa i do czego służy mechanicznie odsuwany filtr podczerwieni w obiektywie, co to jest migawka, kontrast, MTF, ekspozycja i trójkąt ekspozycji. To sporo informacji i solidne podstawy do dalszego zgłębiania wiedzy w różnych fachowych źródłach.

Czego nie wiemy? Optyka to tak obszerny dział fizyki, że nie sposób poruszyć wszystkich zagadnień, nawet ograniczając się do zakresu telewizji dozorowej. Czułość i IRE, Bokeh, koma, astygmatyzm, temperatura barwowa, soczewka Fresnela to przykładowe pojęcia, których znaczenia warto poszukać choćby w Wikipedii. Budowa i działanie przetworników obrazowych, transmisja obrazu, strumienie i kompresja danych – te aspekty, choć niewątpliwie ściśle związane z telewizją dozorową, należy jednak przypisać do kategorii przetwarzania obrazu i teorii sygnałów, a nie optyki sensu *stricto* (a zagadnienia te są na tyle obszerne, że każde zasługuje na osobny cykl artykułów).

BIO

Piotr Rogalewski

W branży zabezpieczeń od 19 lat, obecnie w Hikvision Poland. Audytor wewnętrzny ISO/IEC 27001 SZBI. Programista C/C++, C# i PHP, pasjonat sztucznej inteligencji i lotnictwa.

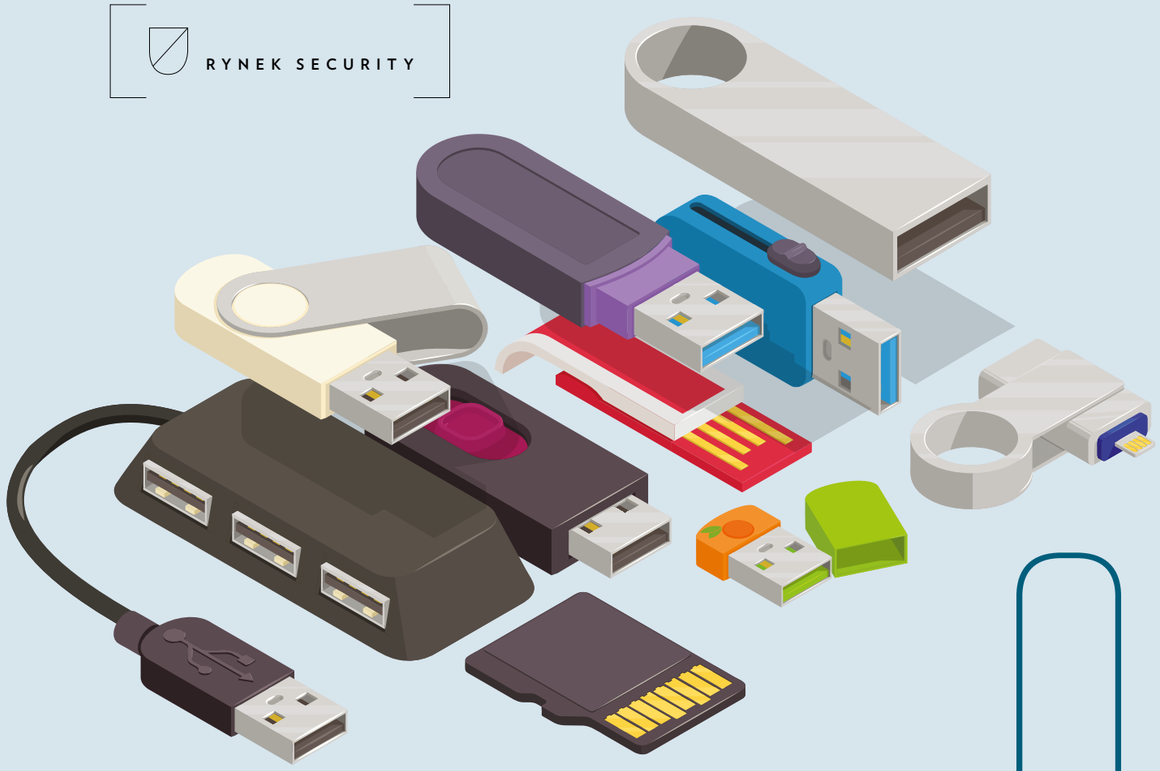
LITERATURA:

[1] C.S. Williams, Introduction to the Optical Transfer Function, SPIE – The International Society for Optical Engineering, Bellingham, Washington 2002.

[2] Zob. Optyka dla każdego. Część 3. „A&S Polska" nr 3/2019.

[3] D.G. Hunder, C.E. West, Last-Minute Optics. A Concise Review of Optics, Refraction, and Contact Lenses, Slack Incorporated, wydanie 2, Thorofare 2010.

[4] Hsien-Che Lee, Introduction to Color Imaging Science, Cambridge University Press, Cambridge 2005.



Niezmierzona pamięć

Czym jest pamięć masowa? To nośnik, który w trwały sposób przechowuje dane przez długi czas. W odróżnieniu np. od typowej pamięci RAM komputera PC ma wielokrotnie dłuższy dostęp oraz większą trwałość przechowywania informacji. Czy jednak wiemy, które z pamięci masowych można i warto stosować w rozwiązaniach monitoringu wizyjnego?

TEKST
Michał Marciniak

Obecnie rynek opiera się na dwóch głównych podzespołach bazowych, z których składa się dysk:

- **nośniki magnetyczne** (wirujący talerz i głowica odczytująca informację z jego powierzchni) – dyski z długą historią, produkowane bez większych zmian od wielu lat. Największe opóźnienia powstają w momencie wyszukiwania lub zapisywania informacji na nośniku przez głowicę, która potrzebuje czasu, aby odnaleźć konkretny sektor (zasada działania podobna do ramienia w gramofonie);
- **nośniki typu FLASH** – zbudowane na bazie układów scalonych pamięci (bez elementów mechanicznych, co ma znaczenie w przypadku środowisk narażonych na wibrację lub wstrząsy). Dotychczasową bolączką tego rozwiązania były: zawodność oraz wysoki koszt dysku (w przeliczeniu na 1 GB przestrzeni dyskowej). Zawodność polegała na krótkim i mało przewidywalnym cyklu zapisu i odczytu bloków, które powodowały utratę danych i brak możliwości ich odzyskania.

Na podstawie powyższych standardów ewoluowało wiele elementów związanych z technologią pamięci masowych: złącza (np. SATA, SCSI, SAS, NVMe itd.), prędkości obrotowe dysków talerzowych, dodatkowe proaktywne zabezpieczenia (np. S.M.A.R.T.) i tak bardzo pożądana pojemność. Obecne zapotrzebowanie na przestrzeń dyskową rośnie logarytmicznie, co wiąże się z wieloma czynnikami: coraz szybsze komputery przetwarzające coraz większą liczbę danych, praca z materiałami wizyjnymi o coraz większych rozdzielczościach (4K/8K), kopie bezpieczeństwa zawierające przyrastające bazy danych itp.

Które zatem nośniki stosować i na czym skupić uwagę w przypadku pamięci masowych stosowanych w systemach dozoru wizyjnego?

Rozwiązania bazujące na NVR *(Network Video Recorder)*

Każdy wiodący producent zaleca stosowanie określonej gamy dysków ze swojego (bądź z firmy współpracującej) portfolio. Nie oznacza to oczywiście, że żaden inny nośnik nie zadziała, ale kupując dysk ze wskazanej listy, możemy mieć pewność, że zadziała on w naszym rejestratorze bez najmniejszych problemów.

Co ważne, wiele profesjonalnych rozwiązań wykorzystuje macierze dyskowe RAID, które powinny bazować na dyskach ze specjalnie przygotowanym oprogramowaniem bezbłędnie realizującym działania w ramach dedykowanej puli pamięci. Najpopularniejszym rozwiązaniem nadal pozostają dyski talerzowe z interfejsem SATA, oferujące zadowalające wartości pojemności i prędkości w relacji do ceny za 1 GB przestrzeni dyskowej.

Dlaczego zatem nie powinniśmy stosować nowoczesnych i wciąż taniejących dysków SSD, które są szybsze, wydajniejsze i coraz bardziej opłacalne? Z jednego powodu – technologia dysków FLASH wymusza równomierne rozłożenie w czasie operacji odczytu oraz zapisu danych – oznacza to (w skrócie), że w trakcie całej eksploatacji dysku powinniśmy mniej więcej tyle samo danych zapisywać oraz odczytywać. Jak wiadomo, w przypadku rozwiązań wizyjnych nacisk kładziemy głównie na nagrywanie (zapis) materiału, a odczyt stanowi znikomą część wszystkich operacji. Dlatego też w praktyce dyski takie „wytrzymują" rok bądź dwa lata i w spektakularny sposób kończą swój żywot (tracąc wszystkie zapisane dane).

Niewątpliwą nowością są dyski z serii AI (*Artificial Intelligence*) przeznaczone do systemów wspierających rozwiązania, np. uczenia maszynowego (*machine learning*). Charakteryzuje je wysoka przepustowość, odporność na wielokrotne losowe wyszukiwanie materiału, powiększona pamięć podręczna cache i – co dla wielu odbiorców bardzo ważne – dłuższa gwarancja.

> Specyficzne wymagania systemów dozorowych wymagają dedykowanych rozwiązań do pracy w trybie 24/7 oraz odporności na błędy i utratę danych

Rozwiązania serwerowe – VMS

W tym przypadku możemy stosować model hybrydowy i rozdzielić poszczególne operacje pomiędzy odpowiednie pule dyskowe. I tak sam system operacyjny wraz z bazowym oprogramowaniem VMS może funkcjonować na dyskach FLASH (bezpośrednio na maszynie fizycznej lub z wykorzystaniem oprogramowania hypervisor, np. Vmware/Hyper-V), nagrania zaś mogą być nadal przechowywane na pulach zbudowanych z dysków magnetycznych.

Czy to ostateczne i jedyne rozwiązanie? Absolutnie nie. Zarówno w przypadku NVR, jak i VMS możemy wspierać się dodatkowymi urządzeniami, np. sieciowymi dyskami NAS (*Network Attached Storage*) pozwalającymi na podłączenie puli dyskowych poprzez lokalną sieć (LAN). W tym przypadku powinniśmy jednak pamiętać o zapewnieniu odpowiedniej przepustowości oraz stabilności połączenia (generowany przez kamery strumień wizji zostaje przechwycony przez oprogramowanie zarządzające VMS i przekazany – w tym przypadku przez sieć – do centralnego repozytorium NAS/iSCSI).

A co w przypadku chmury?

Rozwiązania chmurowe zdobywają coraz większą rzeszę zwolenników (a@s Polska nr 6/2018, *Obserwacja z chmury*), jednak jak je stosować w praktyce i czy na pewno są bezpieczne?

Przede wszystkim w większości tych rozwiązań możemy pominąć kwestie redundancji i ogólnie pojętej opieki nad grupami dyskowymi (a więc rozwiązania RAID nie są już wymagane, chociaż nadal można je stosować), gdyż SLA (*Service Level Agreement*) jest na bardzo wysokim poziomie (wszystkie niezbędne operacje w przypadku awarii dysków wykonuje za nas operator). Obecnie coraz więcej producentów umożliwia integrację swoich produktów z dedykowanymi rozwiązaniami typu cloud (Axis – Camcloud, Dahua – Imou itd.) lub pozwala na podłączenie rozwiązań firm trzecich (np. OneDrive, Google Drive itd.). Nadal należy jednak przeanalizować możliwości techniczne łącza internetowego i bazując na kalkulacjach, budować środowisko tak, aby spełniało wymagania, pamiętając przy tym o zakładanym marginesie błędu (szczególnie przy łączach komórkowych LTE, które są znane z niestabilności w zależności od lokalizacji).

Co nas czeka w niedalekiej przyszłości?

Rynek pamięci masowych zmienia się bardzo dynamicznie, jednak wiele rozwiązań, które świetnie zdają egzamin w przypadku baz danych, systemów operacyjnych czy *big data*, nie zawsze sprawdza się w monitoringu wizyjnym. Specyficzne wymagania (ciągły zapis, rzadki odczyt) wymagają dedykowanych rozwiązań do pracy w trybie 24/7 oraz odporności na błędy i utratę danych.

Współczesne dyski wykonane w technologii FLASH mogą stanowić jedynie dodatek, ale na pewno nie podstawę systemów wizyjnych. Przewagę rozwiązań talerzowych nadal stanowi pojemność (obecne dyski 3,5" mają pojemności 14...16 TB), co pozwala na budowę coraz pojemniejszych macierzy ze względu na fizyczne zapotrzebowani na przestrzeń w lokalnych serwerowniach. Nie wolno również zapomnieć o chmurze, która przy obecnych prędkościach łączy internetowych oraz coraz niższych cenach za 1 TB przestrzeni dyskowej stanowi ciekawą alternatywę, szczególnie w kontekście bezpieczeństwa i zarządzania (brak lokalnego repozytorium – nagrania pozostają dostępne nawet po kradzieży urządzenia).

BIO
Michał Marciniak

Architekt rozwiązań CCTV, twórca i autor bloga www.10cctv.pl; od 20 lat w branży IT i security – promotor, wdrożeniowiec i pasjonat nowych technologii z pogranicza monitoringu wizyjnego oraz IT.

Postaw na właściwą kartę

Jan T. Grusznic

Możliwość przechowywania danych wideo bezpośrednio w kamerach, bez konieczności instalowania dodatkowych urządzeń do zapisu, takich jak rejestratory (DVR, NVR) lub sieciowe zasoby dyskowe (NAS) sprawia, że budowanie wizyjnych systemów dozoru stało się wygodniejsze i tańsze. Jednak niezawodność przechowywania danych wideo w urządzeniu końcowym była i nadal jest kwestionowana. Duża część tych obaw wynika z niewłaściwego doboru kart pamięci do systemów dozoru wizyjnego i złych doświadczeń instalatorów. W poprawie sytuacji nie pomaga również ograniczona liczba materiałów informacyjnych dostarczanych przez samych producentów, które byłyby pomocne we właściwym wyborze.

Ostatnio wiele się mówi o nowych technologiach i ich wpływie na rozwój naszej branży. Podczas dyskusji przy okazji organizowanych (również przez redakcję a&s Polska) konferencji wymienia się: uczenie maszynowe, AI, IoT, robotyzację, *blockchain* czy *edge computing*. Co ciekawe, niezwykle rzadko przy tej okazji wspomina się o wykorzystaniu kart pamięci, które leżą u podstaw wszystkich wymienionych trendów technologicznych.

Karty pamięci opracowane i znormalizowane przez SD Association[1] – stowarzyszenie wiodących firm w branży ustanawiających standardy kart pamięci – od lat stanowią główną część dostarczanych rozwiązań dla konsumentów i przemysłu. Obecnie karty pamięci są stosowane w wielu urządzeniach, np. telefonach komórkowych, dronach, samochodach, amatorskich aparatach fotograficznych, jak również kamerach dozoru wizyjnego.

Oczekuje się, że postęp w technologii NAND[2] znacząco wpłynie na coraz większe zastosowanie kart SD (*Secure Digital*). Pomoże również producentom w opracowywaniu kart lepiej dostosowanych do potrzeb systemów dozoru wizyjnego. Kamery dozorowe mają ściśle określone wymagania dotyczące przechowywania: ciągły zapis danych przez 24 godziny na dobę, 7 dni w tygodniu niezależnie od warunków instalacji. Tymczasem zdecydowana większość kart pamięci dostępnych na rynku jest przeznaczona do przechowywania danych w urządzeniach powszechnego użytku. Liczne nieudane próby ich użycia w VSS spowodowały, że rynek zabezpieczeń elektronicznych postrzega zapis bezpośrednio w kamerach IP w profesjonalnych systemach zabezpieczeń jako mało wiarygodny.

Żywotność i jakość kart SD znacznie różni się zależnie od typu użytej technologii NAND czy sposobu optymalizacji do nagrywania wideo 24/7. Wybór niewłaściwej będzie skutkować awariami, które mogą pojawić się nawet w ciągu kilku miesięcy od momentu wdrożenia. Producenci kamer zalecają na ogół wybór karty o wysokiej wytrzymałości i zabezpieczonej przed zagrożeniami środowiskowymi (np. różnice temperatury, wilgoć), dostosowanej do nagrywanych obrazów o określonej rozdzielczości i poklatkowości. Aby instalatorom sprawę nieco ułatwić, Axis, Bosch czy Hanhwa wprowadziły do oferty karty SD optymalizowane pod kątem ciągłego zapisu wideo w swoich kamerach.

Problem spróbowało rozwiązać również SD Association, wprowadzając w 2016 r. specyfikację SD 5.0, która ustanowiła nowe klasy prędkości zapisu sekwencyjnego, nazwane Video Speed Class. Video Speed Class poszerzyła już zdefiniowane klasy kart pamięci (*tabela*). Pod pojęciem klasy skrywają się trzy konkretne protokoły: nowo wprowadzony Video Speed Class (V6, V10, V30, V60 i V90), UHS Speed Class (U1 i U3) oraz Speed Class (C2, C4, C6 i C10). Video Speed Class wprowadza odpowiednik dla istniejących już klas, jak i nowe prędkości zapisu: 60 i 90 MB/s[3].

Idei wprowadzenia nowego standardu przyświecało optymalne wykorzystanie najnowszej technologii NAND. Istniejące klasy szybkości zawierały stałe parametry, które były zbyt sztywno powiązane z dotychczasową technologią NAND, co utrudniało zaprojektowanie rozwiązań zgodnych z najnowszymi osiągnięciami na rynku pamięci flash. Dzisiejsze zaawansowane możliwości wideo znacznie się różnią w zależności od aplikacji. Różne rozdzielczości, kodowanie wideo (w tym powszechne wykorzystanie tzw. smartkodeków optymalizujących zużycie pasma), dynamicznie zmieniający się poziom kompresji, liczba przechwytywanych klatek/s i możliwy jednoczesny zapis dodatkowych informacji (np. metadane z analizy obrazu) powodują, że dotychczasowe wytyczne dla kart SD stają się trudne w użyciu w nowych aplikacjach. Jeśli zatem kamera umożliwia zapis wielu danych jednocześnie najlepszym wyborem jest karta pamięci SD zgodna z Video Speed Class.

Klasy szybkości wspierane przez interfejs SD oraz prędkości przechwytywania

Minimalna sekwencyjna prędkość zapisu	Klasy prędkości			Zgodny format wideo
	Speed Class	UHS Speed Class	Video Speed Class (nowa)	Niezbędna prędkość zależy od stanu nagrywania/odtwarzania nawet dla takiego samego formatu. Rozszerzone zakresy widoczne poniżej są możliwe i zależą od możliwości samego urządzenia (wyższa rozdzielczość nawet przy mniejszych prędkościach)
90 MB/s			V90	8k Video
60 MB/s			V60	
30 MB/s			V30	4k Video
10 MB/s	10	3	V10	Full HD / Video
6 MB/s	8	1	V6	
4 MB/s	4			Standard Video
2 MB/s	2			

Trochę o technice

Jedną z podstawowych cech chipów pamięci NAND używanych w kartach SD jest asymetryczny dostęp do pamięci, co skutkuje:

- tym, że operacja zapisująca dane trwa dłużej niż operacja odczytująca taką samą ilość danych
- łatwością zapisów stosunkowo niewielkiej porcji danych (np. 4 KB), przy czym ponowny zapis takiej niewielkiej porcji danych może wymagać znacznie większego zapisu (np. 4 MB), co może potrwać dłużej, niż oczekiwano.

Protokół Video Speed Class rozwiązuje te problemy, wprowadzając obsługę równoważenia zużycia komórek pamięci (*wear levelling*). Żywotność pamięci jest związana ze sposobem jej funkcjonowania: każdą czynność zapisu danych poprzedza konieczność skasowania dotychczasowej zawartości komórki. To wpływa na ich stopniowe zużywanie. *Wear levelling* eliminuje mankament przedwczesnego zużycia, stosując oprogramowanie równoważące wykorzystanie komórek – zapis nie rozpoczyna się od pierwszej komórki i nie posuwa systematycznie do kolejnych, ale jest rozłożony na wszystkie komórki pamięci. Zapewnia to równomierne i optymalne zużycie wszystkich komórek i wydłuża żywotność pamięci. Warto przy tym zauważyć, że tradycyjne systemy plików, takie jak FAT, ext2 czy NTFS były projektowane z myślą o dyskach magnetycznych, które wielokrotnie wykonują operacje nadpisywania swoich struktur danych (np. katalogi) w to samo miejsce pamięci. Gdy te systemy są używane na nośnikach pamięci flash, powstaje niemały problem. Dlatego korzystanie z kart pamięci ma sens tylko w tych aplikacjach, które wykorzystują system plików EXT4, exFAT, F2FS, NILFS2 i BTRFS.

Układy pamięci NAND są zbudowane ze stron i bloków – strony mają określoną liczbę bajtów (np. 512, 2048, 4096) i łączą się w bloki (np. 32, 64 lub 128 stron). Zapisują jedynie zera i tylko na poziomie całej strony. Modyfikacja danych polega na dodaniu nowego zera, a jeśli nie jest to możliwe, nowej strony w nowym miejscu – poprzednia strona zostaje oznaczona do wykasowania. Kasowanie przebiega na poziomie bloku. Gdy wszystkie strony bloku zostaną przeznaczone do skasowania, cały blok zostanie zapisany jedynkami[4]. W typowych aplikacjach, jeśli zapis na karcie ulegnie przerwaniu (np. wskutek ponownego uruchomienia urządzenia lub utraty zasilania), blok zostaje przeznaczony tylko-do-odczytu, nawet jeśli została zapisana tylko jedna strona. Jest to tym boleśniejsze, im większy jest sam blok. SD 5.0 przewiduje wznowienie zapisu w tym samym bloku, zapewniając pełne jego wykorzystanie.

Według specyfikacji SD 5.0 karty pamięci SD obsługujące protokół Video Speed Class określają swój własny rozmiar bloku, wykorzystując architekturę wewnętrznej pamięci NAND i użytych w karcie pamięci SD chipów NAND do identyfikacji danych logicznych, które mogą zostać fizycznie usunięte bez wpływu na inne dane zapisane na karcie. Aplikacje wykorzystują te informacje do wybrania logicznego zakresu adresów danych na karcie pamięci, która ma zostać usunięta. Po pierwsze, aplikacja zapewnia, że wszystkie prawidłowe dane w tym zakresie adresów zostaną przeniesione w inne miejsce na karcie pamięci SD. Po drugie, nakazuje karcie pamięci SD usunięcie danych z tego zakresu adresów. Następnie aplikacja może zapisywać sekwencyjnie ten zakres adresów z maksymalną prędkością karty pamięci, bez ograniczania lub przyspieszania operacji zapisu. □

BIO

Jan T. Grusznic

Z-ca red. naczelnego „a&s Polska". Z branżą wizyjnych systemów zabezpieczeń związany od 2004 r. Ma bogate doświadczenie w zakresie projektowania i wdrażania rozwiązań dozoru wizyjnego w aplikacjach o rozproszonej strukturze i skomplikowanej dystrybucji sygnałów. Ceniony diagnosta zintegrowanych systemów wspomagających bezpieczeństwo.

1) SD Association nie produkuje ani nie sprzedaje żadnych produktów. Rolą stowarzyszenia jest tworzenie standardów i ich promowanie, rozwój i nakłanianie do stosowanie standardów SD przez producentów produktów, którzy wytwarzają interoperacyjne karty pamięci i urządzenia je wykorzystujące.
2) Ze względu na rodzaj bramki logicznej realizowany przez komórkę, pamięć flash dzieli się na dwa typy: NOR (NOT- OR), w którym komórki pamięci łączone są równolegle, oraz NAND (NOT-AND) mająca szeregowo łączone komórki. Konsekwencją jest brak komunikacji z pojedynczymi komórkami pamięci NAND – w tym przypadku komórki mogą być odczytywane porcjami (tzw. stronami), w efekcie ten rodzaj pamięci jest znacznie szybszy. Pamięć NAND oferuje krótsze czasy dostępu, większą gęstość (posiada około 60% mniejsze komórki), trwałość (10x większa liczba cykli kasowania niż w przypadku NOR) oraz niższy koszt produkcji w przeliczeniu na jednostkę pojemności nośnika. Z tych właśnie powodów większość pamięci dostępnych na rynku jest rodzaju NAND.
3) Video Speed Class: The new capture protocol of SD 5.0, Luty 2016
4) https://klinikadanych.pl/

HONEYWELL: MAXPRO® Cloud – ochrona danych w chmurze

MAXPRO® Cloud firmy Honeywell jest rozwiązaniem umożliwiającym użytkownikom końcowym podłączenie systemów sygnalizacji włamania i napadu, kontroli dostępu i telewizji dozorowej lub kombinacji tych systemów do chmury. Od chwili, gdy Honeywell dostarcza hosting dla MAXPRO Cloud i przechowuje dane personalne za zgodą użytkowników końcowych, automatycznie staje się podmiotem przetwarzającym dane (Data Processor). Firma Honeywell traktuje temat danych personalnych w usłudze MAXPRO Cloud bardzo poważnie. Dzięki temu jest w stanie zagwarantować, iż przepisy o ochronie danych osobowych mają tutaj zastosowanie. W artykule zostaną opisane najważniejsze zadania stawiane przed dostawcą zintegrowanych rozwiązań w chmurze.

TEKST
Michał Mielczarek
Honeywell Security

Prywatność poprzez odpowiednie zaprojektowanie usługi *(Privacy by design)*

W rozwiązaniach systemów bezpieczeństwa IT (opartych na sieciach) przetwarzających dane osobowe stosuje się wiele różnych technik ochrony tych danych. Wśród nich najbardziej rekomendowane do używania są pseudonymizacja (nadawanie priorytetów) oraz anonimizacja (zachowanie anonimowości). Zastosowanie tych technik pozwala znacząco zmniejszyć ryzyko dostępności do danych.

W przypadku rozwiązań firmy Honeywell anonimizacja, maskowanie, rozmazanie czy pikselizacja twarzy osób zostały zaprojektowane i wdrożone w celu ochrony wizerunku tych osób w systemach monitoringu wizyjnego. Dane osobowe (jak zdefiniowano w RODO) wprowadzone przez użytkownika końcowego są zabezpieczane poprzez anonimizację i maskowane, a następnie zapisywane w chmurze na okres zdefiniowany przez użytkownika. Po tym czasie są usuwane.

Odpowiedzialność za dane wrażliwe

GDPR zapewnia, że osoby fizyczne mają prawo do ochrony swoich danych osobowych i kontroli nad śladami cyfrowymi zostawianych w sieci. Podobnie jak w przypadku każdego systemu wizyjnego, kontroli dostępu lub sygnalizacji włamania, użytkownicy końcowi muszą stosować się do postanowień ustawy, informując swoich pracowników, gości, klientów i inne strony, których to dotyczy, poprzez odpowiednie oznakowanie oraz wcześniejsze powiadomienie i uzyskanie ich zgody, aby upewnić się, że wszystkie zainteresowane osoby są świadome, w jaki sposób systemy zabezpieczeń mogą mieć na nich wpływ, szczególnie gdy materiał wideo jest pobierany w określonym obszarze.

Użytkownik końcowy musi również skonfigurować procedury postępowania z dowolnym rodzajem żądania dostępu i zarządzania nim. Uzyskuje dostęp do chmury Honeywell po zaakceptowaniu i wyrażeniu zgody na warunki prawne, a następnie ma możliwość eksportowania klipów wideo, raportów itp. na indywidualne żądania, tak jak w przypadku rozwiązania innego niż w chmurze. Pomaga to zapewnić łatwą i odpowiednią reakcję na prawo dostępu do żądań.

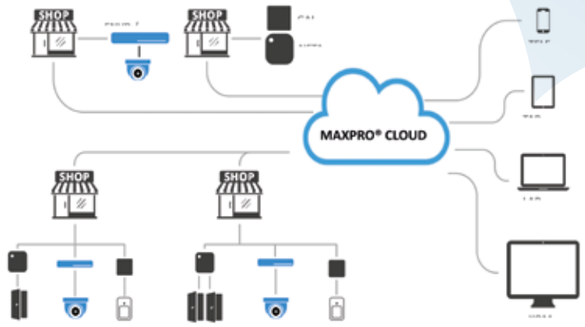
Gromadzenie danych

GDPR ma znaczący wpływ na sposób, w jaki systemy bezpieczeństwa zbierają, przechowują i zabezpieczają dane osobowe. Wszelkie dane osobowe gromadzone za pomocą systemów dozoru wizyjnego, kontroli dostępu i sygnalizacji włamania powinny być przetwarzane w sposób uczciwy i zgodny z prawem oraz wyłącznie w określonych, jednoznacznych i legalnych celach, nie mogą też być dalej przetwarzane w sposób niezgodny z tymi celami (ograniczenie celu).

Rozwiązanie Honeywell MAXPRO Cloud przechowuje klipy wideo na podstawie alarmów i zdarzeń. Korzystając z odpowiedniej kombinacji harmonogramów zapisu, administrator danych może zminimalizować przetwarzanie i przechowywanie zbędnych danych osobowych i zachować zgodność z zasadą minimalizacji danych.

Podobnie jak w przypadku niektórych systemów kontroli dostępu i sygnalizacji włamania firmy Honeywell, użytkownik końcowy może wprowadzić określone dane, aby spełnić ich potrzeby biznesowe i bezpieczeństwa. Jeśli użytkownik końcowy lub administrator danych zdecydują się wprowadzić dane osobowe do rejestru posiadacza karty, obowiązkiem użytkownika końcowego jest upewnienie się, że ma do tego podstawę prawną (taką jak uzasadniony interes użytkownika końcowego). We wszystkich przypadkach użytkownik końcowy będzie musiał poinformować zainteresowane osoby z wyprzedzeniem o przetwarzaniu ich danych, w tym m.in. o rodzaju przetwarzanych danych i sposobie ich wykorzystania. Muszą mieć pewność, że minimalizują gromadzenie danych i skupiają się na danych, które są wystarczające i istotne dla celu.

MAXPRO® CLOUD – PRZYKŁADOWY SCHEMAT ZASTOSOWANIA



Techniczne i organizacyjne środki bezpieczeństwa

Honeywell wdrożył w MAXPRO Cloud zarówno techniczne, jak i organizacyjne środki bezpieczeństwa, aby pomóc użytkownikowi końcowemu w spełnieniu wymogów RODO. Organizacyjne środki bezpieczeństwa obejmują zarządzanie dziennikami, zarządzanie kontami, procedury weryfikacji i zarządzanie dostępem.

Zarządzanie dziennikiem zdarzeń. Dzięki Honeywell MAXPRO Cloud klient może prowadzić rejestr przetwarzania danych i bezpiecznie przechowywać dane w bezpiecznym miejscu, aby zapobiec naruszeniu poufnych informacji. Dostęp do przechowywanych danych jest kontrolowany przez standardowe polityki bezpieczeństwa.

Zarządzanie kontami. Rozwiązania Honeywell Cloud umożliwiają organizacjom wybór użytkownika lub grupy użytkowników, którzy mogą mieć dostęp do różnych profili i zarządzać nimi. W ramach swojego systemu użytkownik końcowy musi zdefiniować **odpowiedni poziom dostępu do systemu dla różnych** użytkowników lub grup użytkowników. Rozwiązania Honeywell zapewniają różne poziomy uprawnień, aby pomóc w łatwym przyznaniu użytkownikom odpowiedniego poziomu uprawnień do przeglądania, uzyskiwania dostępu, wyszukiwania, eksportowania, usuwania lub wprowadzania poprawek (zgodnie z wymaganiami).

Procedury weryfikacji. Dzięki rozwiązaniom w chmurze Honeywell informacje o kontach użytkowników i hasłach są chronione zgodnie z praktykami branżowymi. Dane powinny być ujawniane wyłącznie na zasadzie „niezbędnej wiedzy". Rozwiązania Honeywell Cloud chronią dostęp do danych za pośrednictwem dobrze zaprojektowanych systemów kontroli uprawnień. Zarządzający może również pytać i otrzymywać raporty z systemu chmurowego o różnych czynnościach (np. dodawanie poświadczeń) wykonywanych przez użytkowników, aby zapewnić odpowiednie zarządzanie danymi.

Oprócz organizacyjnych środków bezpieczeństwa Honeywell wspiera odpowiednie techniczne środki bezpieczeństwa. Szyfrowanie danych jest jednym z najważniejszych technicznych środków bezpieczeństwa sugerowanych przez RODO. System Honeywell MAXPRO Cloud został zaprojektowany zgodnie z solidną praktyką bezpieczeństwa cybernetycznego oraz standardami uwierzytelniania i szyfrowania. Dane użytkownika są przechowywane w wiodącej chmurze publicznej w branży platformy oraz zabezpieczone certyfikowanym oprogramowaniem przemysłowym i odpowiednimi narzędziami. Dostęp do platformy chmury, pamięć masowa i transmisja wykorzystują najnowsze standardy bezpieczeństwa. Standardy i praktyki bezpieczeństwa są stale aktualizowane, aby sprostać aktualnym wyzwaniom bezpieczeństwa.

Czas przechowywania danych

Rozwiązanie Honeywell MAXPRO Cloud pozwala użytkownikowi końcowemu na wybór czasu przechowywania nagrań wideo, uprawnień, alarmów z kontroli dostępu i systemu alarmowego. Proces jest kontrolowany i może być zmieniany przez użytkownika poprzez wybór odpowiednich pakietów licencyjnych i zdefiniowanie ich w profilach użytkowników. Efektem jest całkowite usunięcie danych z chmury po określonym czasie przechowywania.

Na ochronę danych osobowych korzystających z chmury składa się wiele czynników. Są to zarówno zabezpieczenia techniczne, programowe, jak i odpowiednio wdrożone procedury. System MAXPRO Cloud został tak zaprojektowany, aby spełniać wszystkie wymagania stawiane systemom bezpieczeństwa w odniesieniu do rozporządzenia o ochronie danych osobowych.

Honeywell
ul. Domaniewska 39,
02-672 Warszawa
www.security.honeywell.com/ee/

WinGuard X4 PSIM+ Jeszcze więcej możliwości

C&C Partners poszerzyła portfel produktowy o WinGuard X4 – wiodący na rynku europejskim system klasy PSIM+, którego producentem jest Advancis Software GmbH. Ponad 1500 projektów zrealizowanych w ponad 70 krajach świadczy o stabilności i elastyczności oferowanej platformy. WinGuard został w pełni przygotowany przez zespół C&C Partners do wprowadzenia na polski rynek zgodnie z jego oczekiwaniami i potrzebami.

Połączenie unikalnej wiedzy specjalistów z Advancis w zakresie rozwoju systemu PSIM ze znajomością lokalnego rynku i kompetencjami zespołu C&C Partners, a także własnym potencjałem rozwoju oprogramowania skutkuje unikatową na polskim rynku ofertą w ramach produktu klasy PSIM – podkreśla Artur Hejdysz, prezes Zarządu C&C Partners.

Czym jest PSIM+?

Aplikację WinGuard definiujemy jako oprogramowanie PSIM+, co oznacza, że jest to rozwiązanie daleko wykraczające poza ramy standardowych wizualizacji, oferujące możliwość głębokiej dwustronnej integracji wszystkich technologii zabezpieczeń, systemów przemysłowych, automatyki budynkowej czy komunikacji.

Neutralność i skalowalność

Kluczowymi cechami WinGuard X4 są neutralność i otwartość względem integrowanych technologii. Pozwala to na integrację i wizualizację autonomicznych systemów zabezpieczeń w ramach jednolitego interfejsu użytkownika. W ofercie podstawowej jest oferowanych ponad 400 interfejsów natywnych, wsparcie protokołów otwartych (Modbus, BacNet, OPC, KNX itd.) oraz narzędzia do opracowywania nowych interfejsów.
Modułowa budowa systemu oraz dostępność rozwiązania w czterech wersjach licencjonowania pozwalają na optymalny kosztowo dobór funkcjonalności oraz dalszy rozwój aplikacji w miarę pojawiania się nowych potrzeb i oczekiwań użytkownika.

Cyberbezpieczeństwo

WinGuard X4 spełnia najwyższy standard bezpieczeństwa w zakresie dystrybucji i zarządzania danymi. Bez względu na wersję wspiera szyfrowanie komunikacji oparte na standardzie 256 bit AES oraz, w przypadku aplikacji mobilnych, zabezpieczenie komunikacji oparte na standardzie TLS (*Transport Security Layer*). WinGuard może zostać zintegrowany z usługą Active Directory (LDAP), co pozwala na ergonomiczne i bezpieczne zarządzanie dostępem do aplikacji na poziomie operatorów.

Redundancja

W przypadku instalacji o znaczeniu krytycznym, w celu zapewnienia maksymalnego poziomu dostępności aplikacji, WinGuard wspiera wieloserwerową redundancję (funkcja Standby) – pełna baza danych systemu jest stale przechowywana na jednej lub kilku niezależnych maszynach. Opcjonalnie, w przypadku przyjęcia struktury z jednym serwerem nadrzednym. system umożliwia definiowanie tzw. segmentów danych (wydzielonego zakresu), które są synchronizowane pomiędzy poszczególnymi lokalizacjami a Centrum Zarządzania. Pozwala to zarówno na optymalizację parametrów połączenia sieciowego, jak i nieobciążanie Centrum danymi uznanymi za mniej istotne.

Mobilność

WinGuard oferuje dostęp do aplikacji mobilnych (Android i iOS), które są dostępne do pobrania i skonfigurowania z poziomu App Store lub Play Store. Aplikacja oferuje również dostęp do interfejsu webowego, co w każdym przypadku zapewnia uprawnionym użytkownikom możliwość łatwego i efektywnego dostępu w trybie online do wszystkich zdarzeń i zadań.

Podsumowując, WinGuard to nowa, aczkolwiek sprawdzona na światowych rynkach propozycja w zakresie integracji i wizualizacji systemów, wspierająca podejście procesowe do zarządzania bezpieczeństwem. W ramach uruchomionego programu partnerskiego C&C Partners zapewnia program szkoleń produktowych, pełne dostosowanie (lokalizację) produktu oraz wsparcie sprzedażowe. uruchomieniowe i serwisowe. □

C&C Partners

ul. 17 Stycznia 119, 121, 64-100 Leszno
www.ccpartners.pl

E-business w UTC

UTC FIRE & SECURITY EMEA JEST CZĘŚCIĄ UTC CLIMATE, CONTROLS & SECURITY, JEDNOSTKI UNITED TECHNOLOGIES CORPORATION

– wiodącego dostawcy rozwiązań dla budownictwa, przemysłu lotniczego i kosmicznego. Zatrudnia ponad 201 tys. fachowców w 18 krajach Europy, Bliskiego Wschodu i Afryki, pracujących dla zapewnienia bezpieczeństwa ludzi, majątku i infrastruktury. Produkuje i dostarcza większość technologii zabezpieczeń, oferując zintegrowane rozwiązania dla aplikacji mieszkaniowych, komercyjnych i korporacyjnych z zakresu:.

- kontroli dostępu,
- zamków mechanicznych,
- wykrywania pożaru,
- systemów alarmowych,
- telewizji dozorowej,
- systemów transmisji,
- rozwiązań zintegrowanych,
- akcesoriów.

Ewa Formela, Customer Service Manager w firmie UTC, przybliża nowy projekt e-business.

Na czym polega nowa inicjatywa firmy UTC?

Zakupy online są znakiem czasów, ale przede wszystkim udogodnieniem dla klientów, dlatego w ostatnim kwartale ubiegłego roku uruchomiliśmy wersję pilotażową platformy e-business dla wybranych klientów, z którymi wspólnie ją udoskonalaliśmy. Fazę testów ukończyliśmy z sukcesem w drugim kwartale tego roku i wystartowaliśmy z wersją produkcyjną. Polska dołączyła do wielu krajów projektu e-business UTC.

Jakie są korzyści z przystąpienia do tego projektu?

Nasi klienci, którzy dołączają do e-commerce, zyskują przede wszystkim elastyczność, jaką jest możliwość składania zamówień 24 godziny na dobę, 7 dni w tygodniu. Mogą to zrobić w dowolnym czasie i miejscu, potrzebny jest tylko dostęp do Internetu. Ponadto dokonując zakupów online, klienci mogą liczyć na okresowe promocje czy dodatkowe rabaty. Zakupy online są dodatkową opcją do standardowej ścieżki zamówień, która cały czas obowiązuje. Klienci mają więc wybór.
Odkąd wystartowaliśmy, grono naszych klientów e-commerce rośnie w błyskawicznym tempie, co bardzo nas cieszy.

Kto może przystąpić do projektu e-business?

Zapraszamy klientów zgodnych z profilem naszej działalności. Sprzedajemy w modelu B2B. W dużym uproszczeniu możemy powiedzieć, że są to firmy instalacyjne i integratorzy z branży systemów zabezpieczeń. Każde zgłoszenie jest weryfikowane przez nas zespół i wymaga autoryzacji. Platforma jest więc dedykowana dla obecnych i nowych klientów, którzy otrzymają naszą autoryzację.

Co trzeba zrobić, aby zostać klientem e-business UTC?

Rejestracja jest bardzo prosta. Wystarczy złożyć wniosek, wypełniając formularz rejestracyjny na naszej stronie: https://pl.firesecurityproducts.com/pl/login. Serdecznie zapraszamy. □

UTC Fire & Security EMEA

ul. Sadowa 8
80-771 Gdańsk
https://pl.firesecurityproducts.com/pl/

Specjalizacja retail

Rola firm ochrony w handlu

Kilkanaście lat temu na jeden sklep spożywczy przypadało trzech pracowników ochrony. Dzisiaj jeden pracownik jest przydzielany dynamicznie do trzech sklepów. Działania współczesnej ochrony wspierają rozwiązania techniczne, analiza napływających w trybie ciągłym danych i wyniki przeprowadzanych audytów bezpieczeństwa. Szerokie kompetencje pracowników są zarazem dopasowane do wysublimowanych potrzeb klientów w różnych segmentach rynku retail. O zauważalnych zmianach na rynku ochrony w segmencie handlu detalicznego, wyzwaniach i oczekiwaniach rozmawiamy z Adamem Kowalskim i Łukaszem Purzeczko, menedżerami ochrony fizycznej stałej specjalizujących się w segmencie retail w firmie Securitas.

→Na czym polega specyfika ochrony fizycznej w sektorze handlu detalicznego?

Adam Kowalski (A.K.): Ochronę sprawują pracownicy, którzy odbyli dedykowane szkolenia przygotowujące do ochrony obiektów handlowych. W ten sposób przygotowujemy pracowników do pełnienia obowiązków w centrach handlowych, ekskluzywnych salonach i sklepach sieciowych. Każdy obiekt wymaga jednak innych kompetencji pracowników.

Czy mógłbyś doprecyzować jakich?

A.K.: Przykładowo w centrach handlowych pracownicy muszą posiadać kompetencje techniczne. Wymaga tego nadzór nad kluczowymi systemami utrzymującymi ciągłość działania centrum. Właściwa interpretacja sygnałów dostarczanych przez systemy jest niezbędna do podejmowania prawidłowych działań. Bardzo ważny jest czas reakcji, który często decyduje o zdrowiu, a nawet życiu. Często udzielamy pomocy przedmedycznej i już wielokrotnie uratowaliśmy życie. Przykładem może być 25-latek z zatrzymaną akcją serca. Nasz pracownik po pojawieniu się na miejscu zdarzenia natychmiast rozpoczął masaż serca, a następnie użył AED. Lekarze, którzy przybyli, stwierdzili, że użyty defibrylator uratował życie, dlatego tak ważna jest umiejętność udzielania pierwszej pomocy.

Łukasz Purzeczko (Ł.P.): Zarządzanie bezpieczeństwem w centrum handlowym wykonywane jest z poziomu systemów wspomagających takich jak SSP, CCTV, SKD czy SSWiN, a zadaniami pracowników ochrony kierują operatorzy BMS (*Building Management System*) z centrum zarządzania bezpieczeństwem. W ostatnich 15 latach liczba pracowników ochrony przypadających na obiekt handlowy o powierzchni 150–200 tys. m² została mocno zredukowana. Dzisiaj jest to 13 osób zarządzających bezpieczeństwem, z czego 1/3 odpowiedzialna jest za nadzór systemów zabezpieczeń i automatyki budynkowej. W mniejszych obiektach nie jest inaczej, choć skala jest mniejsza i do dyspozycji mamy tylko jednego pracownika ochrony analizującego sygnały z systemów wspomagających zarządzanie bezpieczeństwem.

Czy zatem rola pracownika ochrony polega na analizie wskazań systemów?

Ł.P.: Głównym zadaniem pracownika ochrony jest zapewnienie bezpieczeństwa klientowi, personelowi oraz zapobieganie stratom. Dzięki wykorzystaniu systemów bezpieczeństwa wspomagających pracę pracowników, jesteśmy w stanie szybciej i efektywniej podjąć działania. Wiele z naszych działań jest niewidocznych dla klientów sklepów...

A.K.: ...ponieważ część czynności wykonuje się z poziomu centrum monitoringu oraz w nocy po zamknięciu obiektu.

A w ciągu dnia?

A.K.: Handel detaliczny jest „żywym organizmem", każdy dzień jest inny i przynosi nowe wyzwania. Każdego dnia nasi pracownicy pomagają odnaleźć samochód na parkingu, zgubione dokumenty czy portfel. Głośnym echem odbił się w mediach fakt odnalezienia przez naszych pracowników w jednym z centrów 80 tys. dolarów pozostawionych w torbie sportowej. Zdarza się też, że nasi pracownicy szkoleni przez Wydział Ruchu Drogowego zarządzają ruchem pojazdów na parkingu w okresie świątecznym.

Ł.P.: Prawdziwą plagą w centrach handlowych są zaginione dzieci. Komunikaty nadawane przez DSO na niewiele się zdają, ponieważ rodzice zaaferowani zakupami nie słyszą ich. Dopiero po jakimś czasie, gdy na monitorach systemu dozoru wizyjnego widzimy biegających nerwowo ludzi, wiemy, że najprawdopodobniej „znaleźli się" rodzice. Często też zdarzają się alarmy z systemu ppoż. spowodowane paleniem papierosów w niedozwolonych miejscach.

Łukasz Purzeczko

Adam Kowalski

Jan T. Grusznic, a&s Polska

Zakładam, że w mniejszych sklepach kompetencje pracownika ochrony są inne?

A.K.: Oczywiście. Zwłaszcza, gdy chodzi o obiekty zlokalizowane w strefach podwyższonego ryzyka. Są to miejsca o zwiększonej liczbie przestępstw lub wykroczeń w porównaniu do średniej miejskiej. Wykonując analizę zagrożeń i ryzyka, wiemy, że bywają tam klienci bardziej agresywni, częściej również dochodzi do użycia środków przymusu bezpośredniego, większa jest też skala kradzieży. Nasi pracownicy dobierani do ochrony sklepów w tych lokalizacjach muszą umieć sobie radzić z takimi zagrożeniami. Oczywiście istotna jest też rola prewencyjna.

À propos prewencji – statystyczny klient sklepu stereotypowo kojarzy pracownika ochrony ze starszym panem – emerytem. Czy tak jest?

A.K.: Zacznijmy od ustawy (ustawa z 22 sierpnia 1997 r. o ochronie osób i mienia – przyp. red.), która reguluje wymagania kwalifikacyjne pracowników ochrony. Wśród nich oprócz wymaganej nienagannej opinii wydanej przez komendanta powiatowego ważne są predyspozycje fizyczne i psychiczne do wykonywania zadań potwierdzone orzeczeniami lekarskimi, jak również przygotowanie teoretyczne i praktyczne w zakresie m.in. samoobrony, technik interwencyjnych i znajomości przepisów prawa.

Ł.P.: Klient sklepów lub centrów handlowych o wielu problemach nie wie i wielu nie zauważa, stąd ich powierzchowna ocena. Najważniejsze, aby czuł się bezpiecznie i bez obaw dokonywał zakupów. Za jego poczuciem bezpieczeństwa stoją przeszkolone osoby, umiejętność udzielania pierwszej pomocy, predyspozycje psychologiczne. Co do wieku pracownika ochrony bardzo często wiąże się on z latami doświadczeń pracownika w branży. Tacy pracownicy są doceniani przez nas i przez klientów.

Firma ochrony pomaga także w realizacji działań loss prevention. W jaki sposób?

A.K.: Wszystko zaczyna się od zdiagnozowania, gdzie takie działania są rzeczywiście potrzebne. Ich dobór zależy od zdefinio-

wanego ryzyka i efektu, jaki chcemy osiągnąć. Czasy, kiedy pracownik ochrony witał w drzwiach sklepu, bezpowrotnie minęły. Przykładowo z naszego doświadczenia wynika, że w centrum handlowym potrzeba więcej pracowników ochrony w godzinach lunchu. Klienci przychodzący do centrum w tym czasie są roztargnieni, zostawiają w różnych miejscach zakupy, marynarki, portfele. Dlatego o tej porze zwiększamy skład osobowy ochrony, aby klienci czuli się bezpieczniej.

Ł.P.: Opisana mobilność jest obecnie elementem wyróżniającym ochronę w działaniach *loss prevention*. Dobrym przykładem są sklepy sezonowe w miejscach turystycznych, gdzie na ogół ochrony nie ma w ogóle, ale w sezonie musi być obecna od otwarcia do zamknięcia obiektu. Potrzeby są weryfikowane na bieżąco i na bieżąco dostosowujemy się do wymagań rynku.

Czy inwestorzy są świadomi ryzyka, czy to Waszą rolą jest ich uświadamianie?

A.K.: Inwestor jest świadomy ryzyka, naszą rolą jest opracowanie i przedstawienie rozwiązań do występujących zagrożeń. Zdarza się też, że otwarcie mówimy, iż ochrona nie jest potrzebna. Wiedzę tę uzyskujemy po audycie bezpieczeństwa, który przeprowadzamy zawsze przed podjęciem współpracy. Robimy go również cyklicznie u naszych stałych klientów. W takich przypadkach wykorzystujemy system VISION – autorski projekt Securitas – stanowiący nowatorskie narzędzie wsparcia systemów bezpieczeństwa oraz obsługi chronionych obiektów. Umożliwia zdalną koordynację ochrony w wielu obiektach jednocześnie.

Ł.P.: Dane z systemu VISION pomagają nam lepiej wyznaczać działania naszych pracowników, a dzięki dostępowi online widzimy m.in. jak rozkłada się w czasie ruch w sklepach. Te dane wiążemy z innymi informacjami, np. o akcjach promocyjnych, planowanych w okolicy demonstracjach lub koncertach.

Jakie jeszcze technologie mogłyby wspierać działania ochrony?

A.K.: Przydatne byłyby systemy wyposażone w funkcje wspomagające naszych pracowników w szybszym reagowaniu. Myślę o analizie zawartości obrazu, a głównie o rozwiązaniach integrujących systemy wspomagające zarządzanie bezpieczeństwem.

Ł.P.: Rewolucją będą działające systemy analizy twarzy zintegrowane z aktualizowaną centralną bazą sprawców kradzieży. Dzięki temu będzie możliwa natychmiastowa identyfikacja osób podejrzanych. Jestem pewny, że efekt skali zmieniłby zasądzane złodziejom kary. Obecnie pomimo zmian w prawie każdy przypadek kradzieży jest oceniany odrębnie. Wyspecjalizowani złodzieje kradną z kalkulatorem w ręku – do kwoty 499,99 zł, co traktowane jest jako wykroczenie* (art. 119 Kodeksu wykroczeń – przyp. red.). Działają już wyspecjalizowane szajki, posiadające wystarczające środki do opłacania mandatów i zakończenia sprawy w momencie złapania. Starając się temu przeciwdziałać, zbieramy informacje na temat wykroczeń w chronionych przez nas obiektach, tworząc ciągłość czynu i zmieniając tym samym klasyfikację z wykroczenia na przestępstwo.

Jakie najistotniejsze wyzwania stoją przed branżą ochrony?

A.K.: Rynek pracownika. Branża security ma z tym duży problem. Osoby z doświadczeniem odchodzą z branży. I nie chodzi o zmianę firmy, ale zwykły odpływ pracowników. Na to składają się m.in. rządowe programy socjalne. Drugim wyzwaniem jest pozyskanie pracownika, trzecim implementacja rozwiązań technologicznych i większy udział zabezpieczeń technicznych w stosunku do ochrony fizycznej.

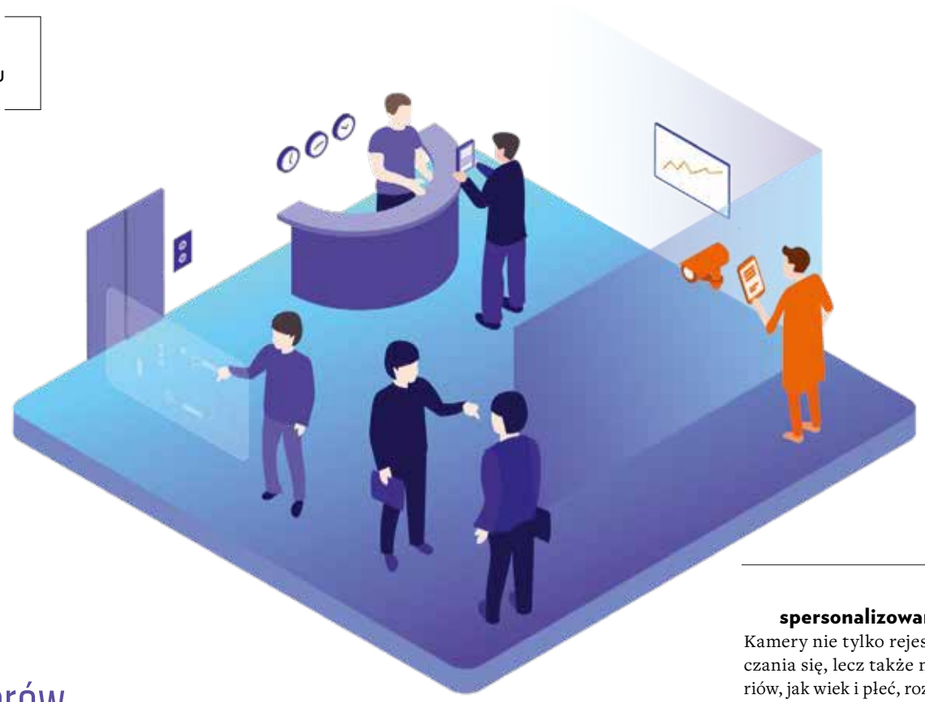
Ł.P.: Nasz rozwój wiążemy z Loss Prevention Group, czyli mobilnymi zespołami ochrony, które sukcesywnie wdrażamy u naszych klientów.

Dziękujemy za rozmowę

* Nowela KW z 2018 r. przewiduje utworzenie elektronicznego rejestru sprawców wykroczeń przeciwko mieniu, osób podejrzanych o popełnienie takich wykroczeń, obwinionych i ukaranych. „Rejestr będzie służył policji, prokuraturze i sądom do tego, by sprytni zawodowi złodzieje, popełniający drobne kradzieże w różnych miastach, nie odpowiadali za pojedyncze wykroczenia, lecz zsumowane przestępstwo" – uzasadniał projektodawca. W ustawie Kodeks karny dokonano nowelizacji art. 12 poprzez oznaczenie jego dotychczasowej treści jako par. 1 i dodanie par. 2 w brzmieniu: „odpowiada jak za jeden czyn zabroniony wyczerpujący znamiona przestępstwa ten, kto w krótkich odstępach czasu, przy wykorzystaniu tej samej albo takiej samej sposobności lub w podobny sposób popełnia dwa lub więcej umyślnych wykroczeń przeciwko mieniu, jeżeli łączna wartość mienia uzasadnia odpowiedzialność za przestępstwo". Ustawodawca chciał w ten sposób zaprzestać procederom kradzieży nieprzekraczających kwoty odpowiedzialności za przestępstwo, z których złodzieje zrobili sobie źródło utrzymania.

Perfekcyjnie wdrożony IoT w handlu detalicznym

Poradnik firmy SAST dla użytkowników i integratorów



STRATEGIA	CZYNNIKI SUKCESU			WYNIKI	SPRZEDAŻ
	Biznes	Technologia	Kultura		
	Model biznesowy	Urządzenia	Zwinność	Doświadczenie klienta	
	Organizacja, kompetencje	Platformy		Koszty operacyjne	
	Przykłady wykorzystania, funkcje	Aplikacje	Skupienie się na kliencie	Magazynowanie	
	Koncepcja danych	Bezpieczeństwo		Analityka biznesowa	

Rys. 1. Elementy Internetu Rzeczy pomocne w uzyskaniu ponadprzeciętnych wyników w sprzedaży [4], [5]

Rynek Internetu Rzeczy (Internet of Things – IoT) stale rośnie. Eksperci przewidują, że do 2020 r. ponad 20 mld urządzeń na całym świecie będzie połączonych w sieci [1]. Stają się one coraz bardziej inteligentne i wszechstronne. Kamera dozorowa, która dotychczas dostarczała dane wideo, teraz może je analizować.

Taki sposób działania może m.in. lepiej poznać zwyczaje zakupowe klientów i udostępniać oferowany asortyment w atrakcyjny sposób. Dane z systemu ochrony można też wykorzystać do optymalizacji zarządzania towarami w celu wsparcia sprzedaży. Sieciowe kamery dozorowe w IoT stają się więc czymś więcej niż tylko elementem ochrony.

Nic dziwnego, że 70 proc. detalistów planuje inwestycje w produkty IoT w ciągu najbliższych pięciu lat [2]. Badanie przeprowadzone przez Cisco wykazało jednak, że trzy na cztery takie projekty kończą się niepowodzeniem [3]. Może to być spowodowane zbyt jednowymiarowym podejściem do Internetu Rzeczy w sektorze handlu detalicznego – chociaż kamery są połączone w sieci, to z punktu widzenia wyników sprzedaży ich potencjał pozostaje niewykorzystany. Kluczem do sukcesu jest optymalna synergia między urządzeniami końcowymi, platformami i programowymi aplikacjami w IoT – określana jako „Perfekcyjny IoT".

Sklepy inwestują w Internet Rzeczy, aby [2]:
- poprawić doświadczenie klienta,
- zwiększyć sprzedaż,
- ograniczyć koszty operacyjne,
- dotrzymać kroku konkurencji,
- zoptymalizować magazynowanie.

Ukryty potencjał Internetu Rzeczy w obszarze ochrony

~~Wdrożone w ramach Internetu Rzeczy~~ kamery dozorowe mogą być pomocne w lepszym rozumieniu klientów. Taka wiedza otwiera nowe możliwości w dostosowania asortymentu do potrzeb klientów i zarządzania towarami. Zwiększa sprzedaż i pomaga obniżyć koszty. Prezentujemy tylko kilka przykładów, w jaki sposób Internet Rzeczy może nie tylko uczynić handel detaliczny bezpieczniejszym, ale także zwiększyć sprzedaż.

Poznajmy zachowania klientów

Do tej pory kamery monitoringu dostarczały przede wszystkim dane wizyjne z przestrzeni sklepu. Obecnie, dzięki analizie obrazu wideo, mogą ułatwiać rozpoznawanie najczęściej wybieranych tras przemieszczania się w sklepie, a w rezultacie umożliwiać lokowanie produktów tam, gdzie oczekują tego klienci. Można również uatrakcyjnić obszary odwiedzane rzadziej, by skierować do nich klientów.

Przykład odkrywania trendów przemieszczania się klientów w przestrzeni sklepowej

Zwróćmy uwagę kupujących i kierujmy nimi przy użyciu spersonalizowanych ofert

Kamery nie tylko rejestrują kierunki przemieszczania się, lecz także na podstawie takich kryteriów, jak wiek i płeć, rozpoznawać klientów w sklepach. Przykładowo, jeśli do sklepu wchodzi kobieta w średnim wieku, kamera może wywołać określoną akcję, np. ekran w pobliżu klientki pokaże ofertę dostosowaną do jej potrzeb. Umożliwia to personalizację interakcji z różnymi grupami klientów. Z technologicznego punktu widzenia jest to możliwe dzięki wydajnym procesorom i inteligentnym aplikacjom w kamerach, które rozszerzają ich funkcjonalność o analitykę obrazu.

Zoptymalizujmy zasoby w naszym sklepie i magazynie

Jeśli chcemy stworzyć idealną atmosferę zakupową, musimy w sklepie przez cały czas obserwować klientów, a jednocześnie mieć kontrolę nad oferowanymi produktami. Braki na półce lub źle odłożone towary ograniczają sprzedaż. Kamery dozorowe mogą stale monitorować stan zapasów w sklepie i w razie potrzeby powiadamiać personel oraz uruchamiać odpowiednie działania. Dane z naszych kamer uaktualniają informacje w systemie zarządzania towarami, zapewniając pełny wgląd w zasoby w czasie rzeczywistym.

> „Aplikacje IoT do optymalizacji sprzedaży zmieniają kamery w perfekcyjne narzędzia analityczne"
>
> Nikolas Mangold-Takao
> VP Product Management & Marketing w SAST

Wyzwaniem dla właściciela sklepu jest utworzenie środowiska niezbędnego do wykorzystania Internetu Rzeczy w firmie. Trzeba poznać aspekty technologiczne niezbędne do odniesienia sukcesu z IoT w handlu detalicznym.

Zalety IoT w handlu detalicznym

Żeby sieciowe kamery dozorowe mogły ułatwić osiągnięcie komercyjnego sukcesu, zaplanowany i wdrożony w firmie projekt powinien uwzględniać wiele czynników. Na *rys. 1* pokazano elementy umożliwiające wykorzystanie Internetu Rzeczy w celu uzyskania ponadprzeciętnych wyników w sprzedaży. Tworzą one razem model określany jako „Perfekcyjny IoT".

Celem modelu Perfekcyjnego IoT jest osiągnięcie jak najlepszego wykorzystania Internetu Rzeczy w sprzedaży. Odgrywające tu ważną rolę kryteria można podzielić na trzy obszary: biznesu, technologii i kultury. Każde kryterium musi być stale oceniane i optymalizowane, aby nieprzerwanie zwiększało swój udział w sukcesie. Kluczowe wskaźniki wydajności (*KPI – Key Performance Indicators*), służące do pomiaru skuteczności działań, powinny się opierać na celach, które chcemy – jako sprzedawcy detaliczni – osiągnąć. Są nimi: ulepszenie doświadczenia klienta, obniżenie kosztów operacyjnych, optymalizacja magazynowania, udoskonalona analiza biznesowa w firmie itp.

Wymagania technologiczne związane z IoT

Przedstawienie wszystkich kryteriów niezbędnych do osiągnięcia w firmie handlowej sukcesu dzięki IoT wykraczałoby poza ramy tego opracowania. Z tego względu skoncentrujmy się na obszarze technologicznym (przede wszystkim w sieciowych kamerach dozorowych) oraz na wskazówkach związanych z planowaniem i wdrażaniem systemów.

1 Urządzenia

Producenci kamer dozorowych coraz częściej wyposażają swoje urządzenia w funkcje sztucznej inteligencji (AI). Stało się to możliwe dzięki nowej generacji wydajnych mikroprocesorów – znanych jako neuronowe układy scalone – instalowanych w urządzeniach. W rezultacie kamery wysokiej jakości zapewniają już dzisiaj wystarczającą moc przetwarzania dla tak złożonych aplikacji, jak analiza wizyjna w urządzeniu. Nowe możliwości techniczne wiążą się z określonymi wymaganiami na sprzęt, którego mamy używać.

Wymagania dotyczące kamer IoT w handlu detalicznym
- Moc przetwarzania: wydajne mikroprocesory umożliwiające obsługę złożonych algorytmów do analizy wideo w kamerze.
- Funkcjonalność: aplikacje można instalować i aktualizować bez konieczności wymiany kamery.
- Ochrona danych: dane są analizowane i interpretowane w czasie rzeczywistym, co oznacza, że zamiast danych wideo mogą być przetwarzane wyłącznie anonimowe wyniki analityczne.

2 Platformy

Platformy IoT stanowią łącze między urządzeniami sieciowy-

Rys. 2. Uproszczona struktura platformy IoT

mi a systemami, które przechowują, przetwarzają i analizują dane. Ponadto platformy zapewniają podstawowe funkcje zarządzania aplikacjami IoT i raportowania. Wyzwaniem dla sprzedawcy jest znalezienie platformy odpowiadającej na jego potrzeby. Obecnie dostępnych jest ponad 450 platform IoT, ale nie każda spełnia wszystkie wymagania handlu detalicznego.

„W firmie SAST pracujemy na platformie, która zapewnia sprzedawcom detalicznym odpowiednią infrastrukturę dla ich wdrożeń IoT"

Michael Gürtner
CTO w SAST

gania dotyczące platformy IoT w handlu detalicznym

iza danych: platforma zapewnia narzędzia analityczne i aplikacje AI w celu uzyskania maksymalnych korzyści z danych dostarczanych przez IoT.

- Funkcje brzegowe: są ważnym elementem zdecentralizowanego przetwarzania danych, umożliwiającym urządzeniom sieciowym analizę danych na miejscu.
- Wymiana danych: dane można wymieniać z innymi systemami przy użyciu standardowych interfejsów.
- Środowisko programistyczne dla aplikacji: platforma zapewnia narzędzia programistyczne i standardy do prototypowania, raportowania oraz zarządzania dostępem.
- Rynek dla aplikacji IoT: aplikacje obejmujące szeroki zakres funkcjonalności zapewniają łatwe instalowanie i testowanie na urządzeniach sieciowych.
- Zarządzanie urządzeniami: funkcje i oprogramowanie na urządzeniach IoT pochodzących od różnych producentów mogą być centralnie zarządzane i utrzymywane przy użyciu standardowego systemu operacyjnego.
- Łączność: różne protokoły i formaty danych są scalane we wspólnym interfejsie oprogramowania, co umożliwia przepływ informacji między urządzeniami sieciowymi.

3 Aplikacje

Dostępnych jest już wiele aplikacji IoT do kamer dozorowych, większość z nich jest obsługiwana bezpośrednio w urządzeniach. Dotychczas wiązało się to z wysokimi kosztami instalacji i utrzymania, ale dziś oprogramowanie jest tak łatwe do zainstalowania i aktualizacji, jak aplikacje na smartfon pobierane ze sklepu z aplikacjami. Systemy operacyjne, na których działają aplikacje IoT, są również bardzo podobne do tych na smartfonach (niektóre nawet opierają się na systemie Android lub iOS).

Wymagania dotyczące aplikacji IoT z obszaru ochrony

- Standardy: standardy jakości dla rozwoju aplikacji i standardowy system operacyjny w sklepie z aplikacjami zapewniają wysoką jakość i kompatybilność aplikacji.
- Instalacja i aktualizacje: instalowanie i aktualizowanie za pośrednictwem sklepu z aplikacjami upraszcza proces testowania aplikacji, minimalizując ryzyko zagrożenia.
- Równoległa praca: w jednej kamerze dozorowej może być używanych jednocześnie wielu aplikacji.

4 Bezpieczeństwo

Aby chronić systemy IoT w firmie przed atakami i manipulacjami ze strony osób do tego niepowołanych, aplikacje muszą spełniać wysokie standardy bezpieczeństwa. Dlatego należy korzystać z aplikacji tylko od dostawców, którzy spełniają takie standardy. Ponadto wykorzystywana platforma IoT powinna gwarantować bezpieczny przepływ danych między urządzeniami a aplikacjami.

Wymagania dotyczące aplikacji IoT w zakresie bezpieczeństwa

- Ochrona danych: dane są analizowane i interpretowane w czasie rzeczywistym, co oznacza, że zamiast danych wideo mogą być przetwarzane wyłącznie anonimowe wyniki analityczne.
- Transfer danych: przepływ danych w ramach platformy IoT powinien być kompleksowo zabezpieczony przed dostępem i manipulacjami z zewnątrz.

Pierwsze kroki w stronę Perfekcyjnego IoT

Wiele projektów IoT kończy się niepowodzeniem, ponieważ sprzedawcy detaliczni starają się osiągnąć zbyt wiele rzeczy naraz. Najlepiej jest planować i realizować swoje projekty w małych, przewidywalnych etapach – zwłaszcza jeśli nie mamy doświadczenia w korzystaniu z IoT opartego na kamerach. Zacznijmy od projektów, które zapewniają sukces szybko i przy niewielkim ryzyku. Takie podejście umożliwi zebranie pierwszych doświadczeń i kontynuację rozwoju naszego Internetu Rzeczy. Strategia technologiczna, jaką zastosujemy dla swojego IoT, musi uwzględniać i dokumentować wszystkie wymagania i ograniczenia – biznesowe, techniczne i operacyjne. Ponadto powinna brać pod uwagę nie tylko bieżące, ale również przyszłe wymagania biznesu i dostosowywać się do zmian zarówno biznesowych, jak i technologicznych. Poniższy schemat przedstawia fazy, zadania i działania związane z wdrażaniem.

Uwagi końcowe

Internet Rzeczy stale się rozwija, a urządzenia sieciowe każdego dnia stają się coraz bardziej inteligentne i wszechstronne. Nowoczesne kamery dozorowe są w stanie dostarczyć więcej informacji niż tylko dane wizyjne. Procesory o większej mocy obliczeniowej, szybszy transfer danych i sztuczna inteligencja umożliwiły dzisiejszym kamerom tworzenie większej wartości na podstawie danych. Zapewniają sprzedawcom nie tylko większe bezpieczeństwo zakupów, ale także zoptymalizowanie sprzedaży. Wymagane do tego urządzenia i aplikacje są już dostępne. W firmie SAST dokładamy wszelkich starań, aby stosowanie tych rozwiązań było proste, opłacalne i elastyczne.

Bądźcie na bieżąco z aktualnymi wydarzeniami z obszaru Internetu Rzeczy dzięki naszemu blogowi:
https://www.sast.io/blog-home

PRZYGOTOWANIE

1	• Zdefiniuj cele biznesowe • Oceń luki w kompetencjach i stwórz zespół • Zdefiniuj kryteria sukcesu	• Stwórz CoE IoT • Zaangażuj architekta(ów) IoT • Zdefiniuj architekturę referencyjną

DEFINIOWANIE

2	• Zdefiniuj sposób podejścia • Zdefiniuj rozwiązanie ochrony • Rozwijaj prototyp • Oceniaj prototyp	• Doskonal architekturę • Oceń ryzyko i stwórz sposób jego minimalizowania

ROZWÓJ

3	• Specyfikacje i produkcja urządzeń • Ocena i zaangażowanie dostawcy	• Integracja platformy • Testowanie

WDRAŻANIE

4	• Dostarczanie urządzeń • Integrowanie danych i aplikacji	• Wdrożenie rozwiązania do zarządzania • Pomiary

DZIAŁANIE

5	• Utrzymanie • Automatyzacja • Monitoring • Ocena wyników	• Dostrajanie rozwiązania, architektury, procesów • Skalowanie

Rys. 3. Uproszczona struktura platformy IoT

SAST

www.sast.io
contact@sast.io

SAST (Security and Safety Things GmbH) jest należącym do firmy Bosch, ale niezależnym start-upem z siedzibą w Monachium. Wspomaga programistów w tworzeniu aplikacji dla urządzeń IoT z zakresu bezpieczeństwa i „operacji".
Jest projektantem globalnego ekosystemu aplikacji dla kamer dozorowych. Jego otwarta i bezpieczna platforma IoT, która zostanie uruchomiona w 2019 r., stworzy nowy standard przemysłowy oparty na otwartym systemie operacyjnym, interfejsach API, sklepie z aplikacjami i portalu integratora. To fundament, na który czeka nasza branża, chcąca wykorzystać potencjał IoT.

ŹRÓDŁA

[1] Gartner: Leading the IoT, https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf
[2] Zebra: 2017 Retail Vision Study, https://www.zebra.com/content/dam/zebra_new_ia/en-us/solutions-verticals/vertical-solutions/ retail/vision-study/retail-vision-study-2017-en-gb.pdf
[3] Cisco Survey Reveals Close to Three-Fourths of IoT Projects Are Failing, https://newsroom.cisco.com/press-release- content?articleId=1847422
[4] EFQM: www.efqm.de/efqm-modell.html
[5] Tresmo: https://www.tresmo.de/iot-industrie-4-0

Polityka *loss prevention* wyzwaniem dla przedsiębiorstw handlowych

ROZWAŻANIA NA TEMAT POLITYKI LOSS PREVENTION W PRZEDSIĘBIORSTWIE HANDLOWYM NALEŻY ROZPOCZĄĆ OD USTALENIA, CZYM WŁAŚCIWIE JEST LOSS PREVENTION, CZYLI ZAPOBIEGANIE STRATOM. ODPOWIEDŹ NA TO PYTANIE NIE JEST ANI PROSTA, ANI TYM BARDZIEJ OCZYWISTA. DEFINICJE TEGO POJĘCIA SĄ OPARTE NA TYM, CO W GRUNCIE RZECZY JEST NAJWAŻNIEJSZE W DZIAŁALNOŚCI HANDLOWEJ, CZYLI WSPARCIU DLA BIZNESU W OSIĄGANIU ZASADNICZEGO CELU, JAKIM JEST ZAMIERZONY ZYSK.

TEKST
Wincenty Ignatowski

W każdym elemencie bezpieczeństwa biznesu, jakim niewątpliwie jest polityka *loss prevention*, pojawiają się zagrożenia, które należy przewidzieć i oszacować, a następnie opracować metody i środki służące do ich minimalizacji. Przemyślana i dobrze przygotowana, a następnie wprowadzona w życie polityka zapobiegania stratom powinna opierać się na profesjonalnie przeprowadzonej analizie danych. Opracowywanie polityki *loss prevention* należy rozpocząć od nakreślenia koncepcji prewencji opartej na zdiagnozowanych źródłach powstawania strat.

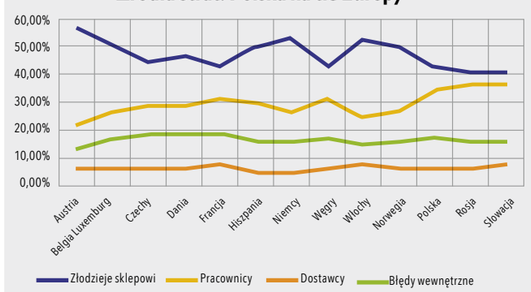
Podstawowym źródłem wiedzy na temat skali strat finansowych w przedsiębiorstwach handlowych są inwentaryzacje towarów, które muszą być rzetelnie i prawidłowo przeprowadzone. Wyniki inwentaryzacji towarów pozwalają na ustalanie strategicznych priorytetów w dążeniu do minimalizacji strat. Ich poziom pokaże tendencję, pod warunkiem że wcześniej zostanie określony poziom transferowanego ryzyka, czyli przeniesienia odpowiedzialności za skutki jego zmaterializowania się na inny podmiot (np. ubezpieczyciela). Należy również brać pod uwagę określenie ryzyka akceptowalnego, wynikającego z zagrożeń neutralizowanych skuteczną i wspieraną przez zarząd przedsiębiorstw handlowych polityką *loss prevention*.

Jedynie racjonalne podejście oparte na analizie wielu źródeł powstawania strat może przynieść zamierzone efekty w ich minimalizowaniu, co stanowi ważny element poprawy rentowności przedsiębiorstw handlowych

Wyniki inwentaryzacji uwidocznią skalę problemu, wykazując:
- jakich artykułów brakuje najwięcej,
- w jakich okresach,
- w jakich segmentach artykułów,
- realną wartość zaginionych artykułów,

ale niestety nie pokażą źródeł powstawania strat.

Źródła strat: Polska na tle Europy



(Na podstawie Global Theft Report 2014, Global Retail Theft Barometer, www.GlobalRetailTheftBarometer.com)

Źródeł powstawania strat może być wiele, każde z nich musi być brane pod uwagę i wszystkie rozpatrywane w sposób kompleksowy. Dopiero na tej podstawie podejmuje się odpowiednie metody walki z nieuczciwymi działaniami. Można wskazać cztery główne źródła powstawania strat, z których każde stanowi istotny element w rozumieniu wszystkich aspektów polityki *loss prevention*. Stawianie znaku równości pomiędzy stratą a kradzieżą jest bardzo dużym, w dodatku nieuprawnionym uproszczeniem, prowadzącym ekspertów od zapobiegania stratom do nietrafnych wniosków, mających często daleko idące konsekwencje. Skupianie się jedynie na kradzieżach powoduje, że znikają z pola widzenia inne przyczyny powstawania strat.

W wielu przedsiębiorstwach handlowych do dziś pokutuje jeszcze przeświadczenie, że praprzyczyną powstawania strat są złodzieje sklepowi lub pracownicy wewnętrzni. Takie podejście prowadzi jednak do radykalizacji działań wobec wszystkich klientów i pracowników. Tego rodzaju uogólnienia w polityce zapobiegania stratom są nieuzasadnione m.in. z kilku powodów:

1. skutkują powstawaniem syndromu oblężonego bastionu, co negatywnie wpływa na wizerunek przedsiębiorstwa;
2. powodują deficyt zaufania wobec wszystkich pracowników przedsiębiorstwa;
3. prowadzą decydentów (menedżerów) do przekonania, że jedynie wysoka restrykcyjność w polityce zapobiegania stratom jest niezbędna, co w konsekwencji może powodować nieuzasadnione wydatki na bezpieczeństwo.

Tymczasem przy bliższym poznaniu tematyki *loss prevention* okazuje się, że kradzieże stanowią „tylko" 20% wszystkich strat w przedsiębiorstwach handlowych. Jedynie racjonalne podejście oparte na analizie wielu źródeł powstawania strat może przynieść zamierzone efekty w ich minimalizowaniu, co stanowi ważny element poprawy rentowności przedsiębiorstw handlowych. Jako źródła powstawania strat, oprócz kradzieży, należy wskazać:

- błędy logistyczne,
- błędy informatyczne,
- ubytki w transporcie,
- ograniczoną wolę do walki ze stratami.

Pierwsze trzy źródła w polityce zapobiegania stratom stanowią przedmiot odrębnych obszernych rozważań. Skupię się na celowo przeze mnie użytym eufemizmie, jakim jest „ograniczona wola walki ze stratami". Tego rodzaju mechanizmy działania wśród kadry menedżerskiej przedsiębiorstw handlowych wypaczają rzeczywistość i polegają m.in. na transferze tzw. nierotujących towarów (stary stock) do strat znanych, które powinny być ewidencjonowane.
Doświadczenie uczy, że w wielu przedsiębiorstwach handlowych spotykamy się z niechęcią do tworzenia precyzyjnych planów działań naprawczych, wręcz z odstępowaniem od ich opracowywania i wdrażania. Taki stan rzeczy skutkuje bałaganem z jego nieobliczalnymi skutkami finansowymi, mającymi wpływ na ekonomikę przedsiębiorstwa. Jeszcze gorzej jest, gdy – jak głosi stare porzekadło– „za każdym bałaganem stoi czyjaś korzyść". Tak czy inaczej brak opracowanych, a co najważniejsze wdrożonych i konsekwentnie realizowanych planów działań naprawczych należy uznać za sabotowanie interesów przedsiębiorstwa, a tolerowanie takiego stanu wcześniej czy później doprowadzi do fatalnego końca.

Brak opracowanych, a co najważniejsze wdrożonych i konsekwentnie realizowanych planów działań naprawczych należy uznać za sabotowanie interesów przedsiębiorstwa

Tylko wtedy, kiedy w polityce *loss prevention* będą obowiązywały jasne reguły gry, a straty nie zostaną obarczone „bagażem" w postaci towarów, które się nie sprzedają, łatwiej będzie ekspertom czy nawet działom *loss prevention* prowadzić racjonalną politykę zapobiegania stratom. Upraszczanie polegające na skupianiu się w procesie zapobiegania stratom tylko na kradzieżach jest charakterystyczne dla wielu przedsiębiorstw handlowych przyzwalających na nieuczciwe praktyki lub promujące je wobec klientów, dostawców i innych interesariuszy przedsiębiorstw.
Informacje o wielu tego typu zjawiskach docierają zazwyczaj do prezesów firm handlowych, jednak często pojawia się w nich pokusa, by uznać, że wprawdzie „wiemy o tych mechanizmach, ale naszego przedsiębiorstwa to nie dotyczy". Każdy dyrektor odpowiedzialny za sprzedaż w przedsiębiorstwie handlowym, który tak pomyśli, właśnie ruszył ku przepaści...*) □

BIO

Wincenty Ignatowski

Absolwent UW (Wydział Socjologii) oraz studiów podyplomowych z zakresu Bezpieczeństwa Biznesu w Wyższej Szkole Finansów i Zarządzania w Warszawie. Od 2001 r. menedżer ds. bezpieczeństwa w międzynarodowych korporacjach z branży logistycznej, handlowych, usługowych i produkcyjnych w Polsce i Europie. Specjalizuje się w polityce zapobiegania stratom *(Loss Prevention Policy)*, Corporate Security, bezpieczeństwie procesów operacyjnych oraz kwestiach związanych z polityką *compliance*.

*) J. Konieczny, Wprowadzenie do bezpieczeństwa biznesu, Warszawa 2004, s. 27.

Nie daj szansy konkurencji

CASE STUDY

Standardem w centrach handlowych w Polsce stało się wyposażanie sklepów w inteligentne kamery i rejestratory. Za ich pomocą właściciel może uzyskać informacje o tym, ile osób przekroczyło próg sklepu. Zastosowane technologie pozwalają też określić profil klientów czy uzyskać informacje, które półki sklepowe cieszą się największym zainteresowaniem.

Uzyskane informacje umożliwiają zwiększenie efektywności pracowników i korzystnie wpływają na podejmowanie decyzji związanych ze stanem magazynowym. Mogą też stanowić źródło odniesienia do efektywnego zarządzania i podejmowania decyzji w celach marketingowych.

Jedną z firm, która zaufała naszym rozwiązaniom, jest Miniso – sieć sklepów detalicznych, która specjalizuje się w sprzedaży produktów użytku domowego i dóbr konsumpcyjnych. Marka ma ponad 2,6 tys. sklepów detalicznych na świecie, niedawno otworzyła placówki również w Polsce. Wyzwaniem dla handlu detalicznego jest nieustanne poszukiwanie nowych sposobów na podniesienie konkurencyjności. Marka Miniso zdecydowała się skorzystać z rozwiązań Hikvision, licząc na zyskanie przewagi, szczególnie w obliczu konkurencyjnego otoczenia (główne punkty handlowe), oraz popularność zakupów online. Aby uzyskać odpowiedź na pytania o skuteczności strategii marketingowej, Miniso sięgnęła po rozwiązanie AI z oferty Hikvision, obejmujące kamery zliczające osoby, kamery typu „rybie oko" z funkcją *heat map* oraz rejestratory NVR. Urządzenia te są skoordynowane za pośrednictwem oprogramowania HikCentral, dzięki czemu firma może zdalnie pozyskiwać wszelkie dane. Jedna z kamer zlicza potencjalnych klientów mijających sklep, natomiast druga – osoby wchodzące do niego i wychodzące. Na tej podstawie kadra zarządzająca może ustalić wskaźnik konwersji zakupowej. Znajomość liczby osób wchodzących do sklepu i zestawienie tego z wynikami sprzedażowymi daje pełny ogląd sytuacji, pozwalając badać, jakie czynniki zewnętrzne mają wpływ na liczbę osób odwiedzających sklep. Ponadto system montowanych na suficie kilku kamer typu „rybie oko" z funkcją *heat map* jest w stanie wygenerować jedną mapę ciepła dla całego obiektu handlowego. Kierownictwo może zidentyfikować „gorące strefy" oraz odpowiednio rozlokowywać produkty do celów promocji, a także sprawdzić, które z nich cieszyły się największą popularnością.
Ponieważ firma Miniso zastosowała tę samą konfigurację technologii we wszystkich swoich sklepach w Polsce, można porównać atrakcyjność poszczególnych lokalizacji. Jest to przydatne także podczas negocjacji kosztów wynajmu powierzchni w centrach handlowych.

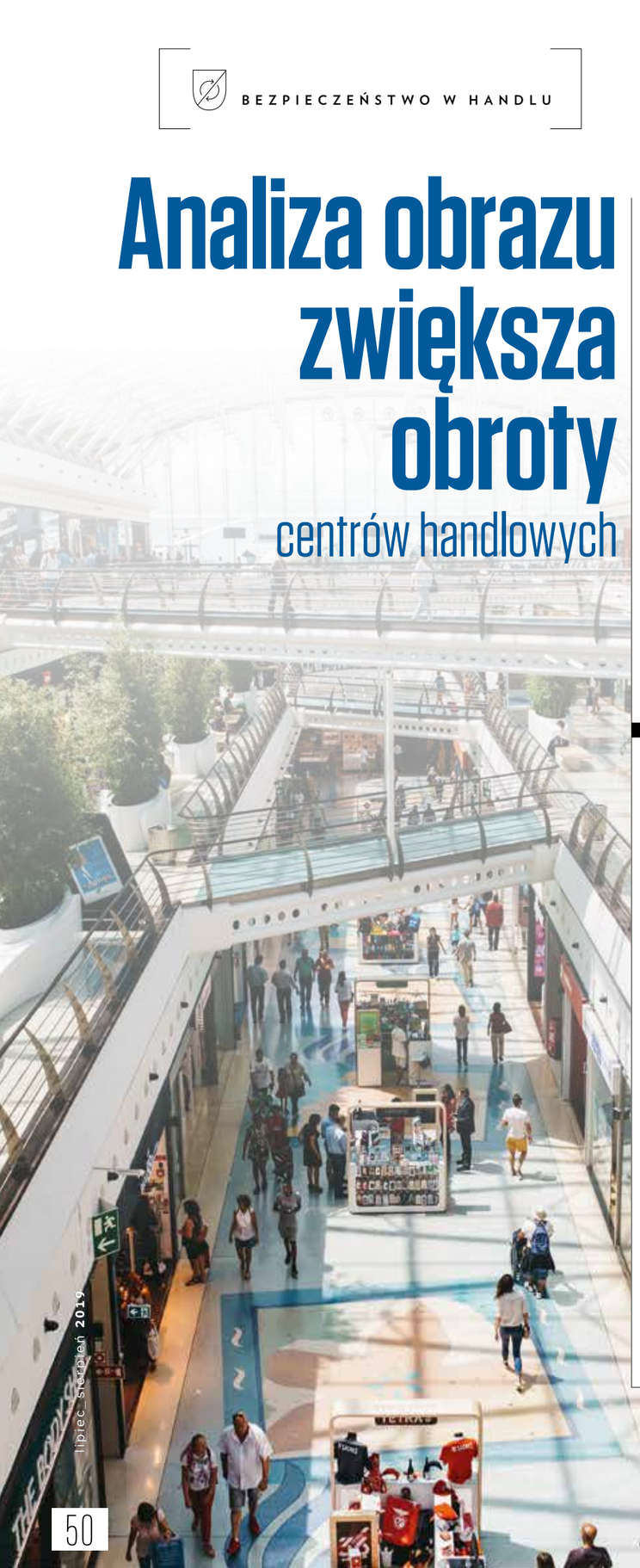
Wszystkie informacje dostarczane przez system są skoordynowane, a siedziba główna Miniso w Warszawie ma możliwość nałożenia danych biznesowych zarówno na plan sklepu, jak i na oryginalny obraz. Profesjonalna platforma do zarządzania materiałami wideo pozwala właścicielom uzyskiwać dostęp do informacji w różnych lokalizacjach oraz z dowolnego miejsca również dzięki aplikacjom mobilnym. Znacząco ułatwia to pracę zespołu operacyjnego, który musi monitorować sytuację we wszystkich placówkach jednocześnie. Oznacza to też, że wszystkie dane mogą być wyświetlane w tym samym momencie, dzięki czemu można identyfikować trendy w całej sieci.
To doskonały przykład na to, jak produkty do systemów monitoringu wizyjnego wsparte AI mogą zmienić perspektywę podejmowania decyzji biznesowych. Jest to szczególnie istotne w środowisku o wysokim stopniu konkurencyjności, takim jak centrum handlowe czy ulice handlowe. Dane na temat trendów zakupowych są bardzo pomocne sprzedawcy w osiągnięciu coraz lepszych wyników sprzedaży. Rozwiązanie to sprawdziło się tak dobrze, że firma Miniso postanowiła wykorzystać je w swoich sklepach w całej Europie – trafi ono do ok. 200 placówek już w przyszłym roku. □

Hikvision Poland

ul. Krakowiaków 50,
02-255 Warszawa
tel. 22 460 01 50
faks 22 464 32 11
e-mail:
info.pl@hikvision.com

Analiza obrazu zwiększa obroty centrów handlowych

Sposób, w jaki dokonujemy zakupów, zmienia się. Popularny od pewnego czasu handel przez Internet pozwala zamówić dowolny towar wraz z dostawą do domu. Powodem, dla którego ludzie wciąż odwiedzają centra handlowe, jest m.in. różnorodność oferty w miejscu, do którego się udają.



Współczesne centra handlowe są czymś więcej niż tylko miejscem robienia zakupów – zapewniają odwiedzającym dodatkowe rozrywki i korzyści. Tak będą funkcjonować zapewne również w przyszłości. Do centrów handlowych przychodzi się, by spotkać znajomych, wymienić doświadczenia z klientami o podobnych gustach lub samodzielnie porównać marki, w efekcie płynnie przechodząc od zakupów online do zakupów w realu. Naprzeciw rosnącemu zapotrzebowaniu klientów na bogatszą ofertę zakupowo-rozrywkową najszerzej wychodzą centra handlowe w Azji.

Zgodnie z wynikami raportu „Przyszłość centrów handlowych" przeprowadzonego przez AT Kearney, zarządcy będą musieli opanować dwie grupy technologii pomocnych w uzyskaniu pełnego zadowolenie klienta:

- technologie, z których na co dzień korzystają konsumenci do komunikowania się i realizowania działań handlowych, takie jak telefony komórkowe, tablety oraz ich aplikacje;
- technologie, których firmy używają i będą używać do identyfikacji poszczególnych kupujących, śledzenia zakupów, obliczania czasu przebywania w danym miejscu, analizy zachowania, komunikacji z klientami oraz kreowania akcji promocyjnych, marketingowych i reklamowych.

Uogólnienia są zawsze ryzykowne, jednak badania i doświadczenie wskazują, że wielu zarządców centrów handlowych nie dotrzymuje jeszcze kroku najemcom pod względem wykorzystania zaawansowanych analiz biznesowych.

Jak centra handlowe mogą zwiększyć swoje dochody dzięki możliwościom analizy obrazu

Najemcy lokali w centrach handlowych zwykle płacą czynsz na podstawie stałej kwoty ustalanej dla danej lokalizacji, wielkości i układu wynajmowanego lokalu, a także wynegocjowanego procentu od sprzedaży. W zamian oczekują od właścicieli obiektu zapewnienia odpowiedniego ruchu klientów.

Natężenie ruchu w centrum handlowym odzwierciedla atrakcyjność jego oferty. Z kolei natężenie ruchu w centrum w porównaniu z ruchem w danym sklepie pokazuje, w jakim stopniu najemcy potrafią przyciągnąć do siebie klientów (by ostatecznie osiągnąć większą sprzedaż). Zliczanie odwiedzających pozwala zobrazować aktywność w centrum handlowym, tendencję i okresy szczytowe, a nawet pomaga dokonać wysokopoziomowej oceny wpływu takich czynników dodatkowych, jak pogoda, wakacje czy promocje.

Na podstawie uzyskanych danych można również określić najlepsze okresy prowadzenia codziennych kampanii marketingowych mających na celu zachęcenie klientów do odwiedzenia sklepu.

Zarządcy centrów handlowych chcą budować kulturę podejmowania decyzji opartą na dobrze udokumentowanych faktach i wiarygodnych danych na potrzeby świadomej analizy decyzji biznesowych

Kamery firmy Axis z zaimplementowaną aplikacją *AXIS People Counter* **umożliwiają efektywne automatyczne zliczanie w czasie rzeczywistym osób przechodzących.** Aplikacja informuje również o kierunku, w którym te osoby się udały. Po zintegrowaniu z systemem PoS pozwala też gromadzić niezbędne dane dotyczące współczynników konwersji – na ich podstawie można podejmować kluczowe decyzje. Aplikacja gromadzi też informacje dotyczące przepływu klientów w sklepie. Na ich podstawie uzyskujemy wgląd w zachowania klientów i możemy podejmować właściwie działania.

Menedżerowie operacyjni centrów handlowych poświęcają sporo czasu na możliwie najlepsze rozmieszczenie poszczególnych sklepów w obiekcie. Pomocne mogą być dane pozyskane ze zliczania odwiedzających zestawione z innymi danymi, np. demograficznymi (wiek i płeć). Porównując popularność i wyniki sprzedażowe z różnych lokalizacji oraz częstość odwiedzin różnych sklepów przez te same osoby, można określić, jakie grupy konsumentów odwiedzają centrum handlowe i jak spędzają w nim czas. Aplikacja ***AXIS Demographic Identifier*** umożliwia właśnie porównanie statystyk dotyczących płci i wieku klientów w różnych sklepach i o różnych porach. Można dzięki niej ukierunkować działania marketingowe na konkretne grupy demograficzne, do których należą klienci sklepu w danym obszarze czy o danej porze dnia.

Innym obszarem istotnym z punktu widzenia zarządców centrów handlowych, również dotyczącym zachowania klientów, jest optymalizacja układu obiektu. Aplikacje analizy obrazu, np. zliczanie odwiedzających, obliczanie czasu przebywania w danym miejscu czy mapy pogody pomagają zobrazować całościowo ruch klientów. Pozwalają zidentyfikować miejsca szczególnie oblegane oraz tzw. wąskie gardła w sklepie i na ich podstawie określić pożądane zmiany aranżacji, a także pokazać wpływ przedsięwzięć o ograniczonym czasie trwania – np. sklepy typu pop-up (tymczasowe), na zainteresowanie klientów danym centrum handlowym. Tę wiedzę można następnie wykorzystać do oceny oddziaływania, jakie potencjalni najemcy będą mieć na centrum handlowe, a nawet do ustalania cen najmu.

Dla zarządców centrów handlowych, którzy we współpracy z najemcami chcą budować kulturę podejmowania decyzji opartą na dobrze udokumentowanych faktach, zbieranie wiarygodnych i cennych danych na potrzeby świadomej analizy decyzji biznesowych stanowi właściwy punkt wyjścia do uzyskania tego celu. □

E-sklepy nie mają dni wolnych

Jak wynika z raportu Gemius „E-commerce w Polsce 2018", 54% kobiet i 46% mężczyzn w Polsce dokonuje zakupów przez Internet. Kwoty, jakie wydajemy na produkty w sieci, stale rosną, a 30% respondentów planuje zwiększenie wydatków zakupowych. Wzrost popularności e-zakupów sprawia, że ta dziedzina staje się obiektem zainteresowania cyberprzestępców. Ich ataki są skierowane zarówno przeciwko e-sklepom, jak i kupującym.

Branża e-commerce jest konkurencyjna. Według danych firmy badawczej Bisnode w Polsce w 2010 r. było zarejestrowanych ponad 7,6 tys. sklepów internetowych, z tego na koniec stycznia 2018 r. mniej lub bardziej aktywnie funkcjonowało już tylko 2,3 tys. firm. Oznacza to, że tylko 30% polskich e-sklepów działa dłużej niż 8 lat. Posiadanie stabilnej, odpornej na cyberataki platformy zakupowej, która będzie zachęcała, a nie zniechęcała do zakupów, jest kluczowym warunkiem utrzymania się na tym trudnym rynku.

Klient nie będzie czekał, aż podniesiesz się po cyberataku

Zwrócenie uwagi klienta na ofertę e-sklepu nie gwarantuje jeszcze sukcesu. Z badania DPDgroup „Barometr E-shopper 2018" wynika, że 90% kupujących w sieci rozmyśla się i przerywa składanie zamówienia przed sfinalizowaniem transakcji. Jeżeli jeden z funkcjonujących na rynku sklepów internetowych przestanie działać na skutek cyberataku, kupujący natychmiast skorzystają z usług konkurencji. Dlatego niezwykle ważne jest stabilne działanie platformy zakupowej, która będzie stale dostępna.

Działając w branży e-commerce, nikt nie może czuć się w pełni bezpieczny i uważać, że problem cyberprzestępczości go nie dotyczy. Na wypadek cyberataku e-sklep musi posiadać odpowiednie procedury działania. Dobry system bezpieczeństwa ma budowę warstwową, dzięki czemu awaria jednego elementu infrastruktury nie paraliżuje pracy całej organizacji i pozwala zapewnić stały dostęp do usług.

Bezpieczeństwo dotyczy i dużych, i małych

Branża e-commerce jest bardzo zróżnicowana. Duże firmy mają rozbudowaną infrastrukturę IT i przechowują ogromną ilość danych. Te organizacje muszą zadbać o bezpieczeństwo wszystkich elementów – od centrum przechowywania i przetwarzania danych po urządzenia na brzegu sieci. Korzystają z pełnej palety rozwiązań zbudowanych na platformach pozwalających na wielochmurową integrację usług – *Cisco Application Centric Infrastructure* (*ACI*) wraz z elementami, takimi jak *Cisco Tetration* (zapewniającymi widoczność i segmentację, umożliwiającymi przeprowadzenie audytu) czy firewalle nowej generacji *Cisco Firepower*. W przypadku dużych e-sklepów niezwykle ważna jest segmentacja, czyli podział na mniejsze sieci, nie tylko ze względu na wzrost wydajności, ale również bezpieczeństwo. Separacja sieci zapewnia ograniczenie dostępu z jednego segmentu do drugiego w sposób automatyczny. W przypadku cyberataku na jeden element rozwiązania, możliwości „zarażania" czy eskalacji na inne wewnętrzne zasoby są ograniczone.

Tego typu mechanizmy mają duże znaczenie w kontekście uregulowań RODO. Nakładają one na firmy obowiązek właściwego zabezpieczenia danych osobowych, które duże e-sklepy codziennie przetwarzają w ogromnych ilościach. Chcąc mieć pewność, że organizacja działa zgodnie z unijnym rozporządzeniem, warto również skorzystać z mechanizmów klasy DLP (*data leaking protection*) służących zapobieganiu wyciekom danych. Są one wbudowane w rozwiązania informatyczne, takie jak Cisco ESA (proxy poczty elektronicznej), Cisco WSA (proxy www) czy Cisco CloudLock (broker usług chmurowych typu Dropbox, Box, Google Drive czy Office 365).

Na rynku jest też bardzo dużo małych e-sklepów, które działają na podstawie gotowych szablonów i korzystają z centrów danych zewnętrznych dostawców. Niekiedy posiadają dodatkowe aplikacje odpowiadające za programy lojalnościowe czy sieć dystrybucji. Dla nich właściwe będą prostsze rozwiązania, które chronią szczególnie wrażliwe na ataki elementy środowiska IT, np. Cisco Email Security (ESA) odpowiadające za bezpieczeństwo poczty e-mail. Warto zadbać o ten aspekt, gdyż wg danych grupy badaczy cyberbezpieczeństwa zrzeszonych w Cisco Talos w kwietniu tego roku spam stanowił aż 85% wszystkich wiadomości e-mail.

Niezależnie od tego, czy prowadzimy duży, czy mały e-sklep, musimy pamiętać, że nie uda się wygrać walki z cyberzagrożeniami w pojedynkę. Trzeba korzystać z doświadczeń innych, podobnych organizacji (tzw. *threat intelligence*) oraz wskazówek ekspertów, np. z grupy Cisco Talos. □

EKSPERCI CISCO WSKAZUJĄ TRZY ZASADY ZAPEWNIENIA BEZPIECZEŃSTWA E-SKLEPÓW

1 BIEŻĄCY MONITORING – monitoruj logi i system sieciowy twojego e-sklepu. Warto korzystać z dedykowanej konsoli bezpieczeństwa, np. Cisco StealthWatch. Dzięki temu dział IT e-sklepu może nie tylko mapować adresy IP, ale także powiązać potencjalne zagrożenia i wektory ataków z dodatkowymi informacjami, np. gdzie, kiedy i jak użytkownicy oraz urządzenia łączą się z systemem IT i żądają dostępu do jego zasobów. Analizując zdarzenie kontekstowo, StealthWatch zapewnia lepszą widoczność potencjalnych zagrożeń i przyspiesza identyfikację ich przyczyn.

2 GOTOWOŚĆ NA ATAK – upewnij się, że w sytuacji, gdy dojdzie do cyberataku, będziesz posiadać niezbędne informacje do tego, żeby móc ustalić, których elementów infrastruktury on dotyczył, które dane wyciekły (lub zostały zmodyfikowane). W prawidłowej ocenie skutków cyberataków pomagają takie rozwiązania, jak Cisco StealthWatch czy Cisco Advanced Malware Protection. Dzięki nim można zidentyfikować zarażone zasoby i „wyczyścić sieć", przywracając działanie usług.

3 BACKUP I BEZPIECZEŃSTWO CHMURY – backup danych zawsze powinien być zaszyfrowany. Jeżeli dane są przechowywane w chmurze, również należy je zabezpieczyć. O odpowiednią kontrolę usług chmurowych pochodzących od wiodących dostawców, takich jak Amazon AWS, Microsoft Azure, Google Drive, Dropbox czy Box Sync, może zadbać Cisco CloudLock. Rozwiązanie pozwala na identyfikację wykorzystywanych aplikacji SaaS (Security as a Service) i blokowanie tych, które stwarzają jakiekolwiek ryzyko zagrożenia.

Cisco Systems Poland

ul. Domaniewska 39B
02-672 Warszawa
www.cisco.com

Zarządzanie miejscami parkingowymi w centrach i galeriach handlowych

W 2018 r. na całym świecie sprzedano ok. 79 mln samochodów. Tegoroczne statystyki wskazują, że sprzedaż nadal będzie stabilna. Gdy na drogi wjeżdża coraz więcej pojazdów, rośnie zapotrzebowanie na miejsca parkingowe zarządzane z wykorzystaniem zaawansowanych technologii

a&s International

NAJWIĘKSZYM PROBLEMEM NA PARKINGACH W CENTRACH I GALERIACH HANDLOWYCH JEST PANUJĄCY NA NICH RUCH. ODWIEDZAJĄCY WJEŻDŻAJĄ I WYJEŻDŻAJĄ PRZEZ CAŁY DZIEŃ, NIERAZ TAKŻE W NOCY. POTRZEBUJĄ PRZY TYM WYGODNYCH, ŁATWYCH W OBSŁUDZE SYSTEMÓW PŁATNOŚCI.

Jak zauważa Międzynarodowy Instytut Parkingów i Mobilności (IPMI – *International Parking and Mobility Institute*), amerykańskie stowarzyszenie specjalistów z zakresu parkowania, transportu i mobilności, postęp techniczny i zmiany zachowania użytkowników doprowadziły do pojawienia się nowych trendów w branży. Najważniejszymi z nich są: korzystanie z technologii mobilnych, większe zastosowanie systemów nawigacji, wygodniejsza kontrola dostępu i możliwości w zakresie płatności.

Dochodzą do tego kwestie związane ze zmianami w przemyśle motoryzacyjnym. Ponieważ rośnie popularność samochodów elektrycznych, właściciele centrów handlowych mogą już tworzyć dla nich specjalne strefy. Wybiegając w przyszłość, można się spodziewać pojawienia się pojazdów autonomicznych, które stanowiłyby nowe wyzwanie.

Przedstawiamy najważniejsze wymagania w obszarze zarządzania parkingami w centrach i galeriach handlowych, potencjalne kryteria wyboru rozwiązań, a także kilka wyróżniających się i wartych uwagi rozwiązań.

Zagrożenia dotyczące bezpieczeństwa na parkingach w centrach handlowych

Centrów handlowych przybywa na całym świecie, podobnie jak prywatnych pojazdów, których ludzie używają, aby się do tych centrów dostać. W tej sytuacji niezbędne są doskonalsze rozwiązania do zarządzania parkingami, Takie, które zadbają o kwestie bezpieczeństwa, a także usprawnią procesy. Z punktu widzenia integratora systemów kluczowe jest zrozumienie zachodzącej tu ewolucji zagrożeń przekładającej się na ofertę rozwiązań, które zapewniają maksymalną ochronę. Specjaliści wymieniają najważniejsze, o których powinien wiedzieć integrator systemów.

Zagrożenie bombowe

Centra handlowe to miejsca, w których codziennie gromadzą się rzesze ludzi, stanowiąc potencjalny cel ataków terrorystycznych. W grudniu ub.r. zginęły dwie osoby, a blisko 30 zostało rannych, gdy bomba eksplodowała w centrum handlowym na Filipinach. Podobne zdarzenia miały miejsce również gdzie indziej. Bomby w samochodach, chociaż nie zawsze eksplodują na parkingach, stanowią poważne zagrożenie dla systemów zarządzania parkingami.

Złodzieje samochodów

Kradzieże samochodów lub rzeczy przechowywanych w pojazdach zaparkowanych w centrach handlowych to kolejne ryzyko. Zdarzające się incydenty, takie jak włamanie w centrum handlowym Stanford w kalifornijskim Palo Alto w ub.r., pokazują, że poziom bezpieczeństwem na parkingach wciąż nie jest najwyższy.

Kolizje i wypadki

Wypadki to ryzyko, z którym w miejscach, po których poruszają się samochody, zawsze należy się liczyć . W zamkniętych przestrzeniach parkingów, gdzie miejsce do manewrowania pojazdami jest ograniczone, staje się ono nawet większe. Według danych firmy ubezpieczeniowej Think Insure jeden na pięć wypadków zdarza się właśnie na parkingach. Chociaż większość z nich to niewielkie kolizje – zderzenia przy małej prędkości – zdarzają się również groźne wypadki.

Pożar

Niebezpieczeństwo zapalenia się pojazdu to kolejny poważny problem,z którym musi się liczyć dostawca rozwiązań dla parkingów. Eksperci zwracają przy tym uwagę, że producenci samochodów stosują obecnie w pojazdach więcej plastiku, co sprawia, że wypadki związane z ogniem stają się coraz groźniejsze.

Wandalizm i podobne incydenty

Problemem są także uszkodzenia samochodów przez wandali. Dochodzi do nich częściej w tych centrach handlowych, w których funkcjonują kluby nocne lub bary, a sprawcami nierzadko są osoby pod wpływem alkoholu. Wandalizmowi mogą towarzyszyć inne incydenty, np. kradzież. Obecnie centra handlowe stają się „nowymi głównymi ulicami". Tym samym należy się spodziewać podobnych problemów związanych z bezpieczeństwem w ruchu miejskim. Nie inaczej jest na parkingach – wszelkie zagrożenia dotyczące samochodu zaparkowanego na ulicy mogą pojawić się także tutaj. Jedyna różnica polega na skuteczności zastosowanego rozwiązania zarządzającego parkingami. Idealne powinno umożliwiać integrację z różnymi systemami zabezpieczeń (monitoringu wizyjnego, kontroli dostępu i sygnalizacji pożarowej), zapewniając działania adekwatne do danej sytuacji. Ale to tylko jedno z zadań rozwiązania do zarządzania parkingami. Jego efektywność operacyjna, zapewniane profity ekonomiczne i środowiskowe przekładają się na korzyści zarówno dla menedżerów centrów handlowych, jak i ich klientów. Kierowcy mogą poznać liczbę wolnych miejsc parkingowych jeszcze przed wjazdem na teren obiektu – niektóre rozwiązania oferują apli-

Konieczne staje się zastosowanie wysokiej jakości nadzoru wideo, który może dostarczyć wyraźny obraz stanu pojazdu w miejscu wjazdu

kacje mobilne, które za pomocą wiadomości SMS informują ich o stanie zajętości. Ogranicza to czas i wysiłek, który trzeba włożyć w poszukiwanie wolnego miejsca. Mniejsze jest także zanieczyszczenie środowiska.

Główne wyzwania w zarządzaniu parkingami

Zastosowanie najnowszych technik dostępnych na rynku może rozwiązać wiele problemów związanych z zarządzaniem miejscami parkingowymi.

W dobie szybko postępującej urbanizacji i mobilności człowieka preferowanym środkiem transportu w krajach rozwiniętych są pojazdy prywatne. Dla miasta wiąże się to z koniecznością tworzenia kolejnych miejsc parkingowych. Koncepcja parkingu ewoluowała przez lata – z miejsca, w którym można zostawić samochód, staje się dobrze chronionym obiektem zarządzanym przez zautomatyzowane rozwiązania ułatwiające obsługę. W miastach przybywa także centrów i galerii handlowych przyciągających coraz więcej osób, które muszą dojechać tam swoimi samochodami. Zapotrzebowanie na wydajne systemy zarządzania miejscami parkingowymi w centrach handlowych jest więc coraz większe. Nowym potrzebom i wyzwaniom muszą sprostać i zarządzający centrami, i dostawcy rozwiązań. Wprowadzanie systemów zautomatyzowanych eliminuje niektóre z tych problemów, inne wciąż czekają na rozwiązanie.

Ręczne wystawianie biletów jest czasochłonne

Rozwiązania elektroniczne warto stosować chociażby z tego powodu, że manualne systemy biletowe angażują więcej siły roboczej i pochłaniają czas, co zwiększa koszty i spowalnia przetwarzanie. Chociaż problem ten wydaje się oczywisty, na całym świecie nie brakuje centrów i galerii handlowych, które wciąż jeszcze korzystają z ręcznych systemów sprzedaży biletów.
Oparte na papierze systemy biletowe utrudniają zarządzanie informacją. W razie incydentu zarządzający parkingiem powinien móc natychmiast dostarczyć dane o każdym pojeździe zaparkowanym w ich obiekcie, a to umożliwiają zautomatyzowane systemy elektroniczne.

Awaria systemu kontroli dostępu i systemu biletowego

Jedną z największych niedogodności dla zarządcy parkingu jest nieprawidłowe działanie systemu kontroli dostępu. Ponieważ centra handlowe są zwykle otwarte przez długie godziny, często przez cały tydzień, parkingi są w użytkowaniu przez większość czasu. Jeśli system zarządzania wjazdami i wyjazdami zawiedzie w jakikolwiek sposób, może to prowadzić do opóźnień skutkujących niezadowoleniem klientów.

Fałszywe roszczenia odszkodowawcze

Zdarzają się klienci, którzy będą twierdzić, że ich samochód został uszkodzony na parkingu, podczas gdy w rzeczywistości miał już uszkodzenia przed wjazdem. Z tym problemem doskonale poradzi sobie wysokiej jakości system monitoringu wizyjnego, który dostarczy wyraźny obraz pojazdu w momencie wjazdu na parking. Aby zwiększyć skuteczność zainstalowanego systemu, wymagane będzie również zapewnienie odpowiedniego oświetlenia.

Integracja

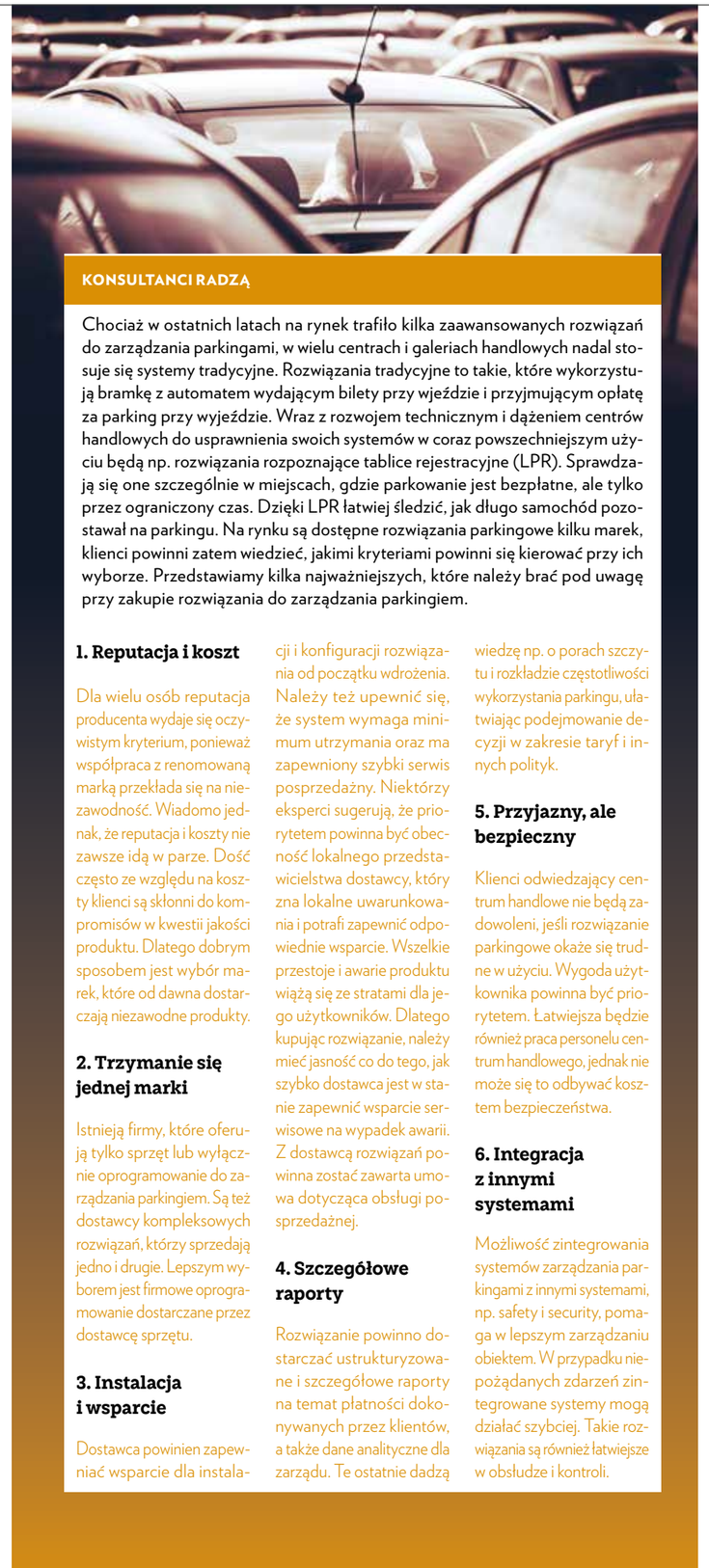
Zainstalowanie nowych rozwiązań parkingowych w już istniejących centrach i galeriach handlowych stanowi wyzwanie, które zwiększa konieczność ich integracji z systemami firm trzecich. Przykładowo, system monitoringu wizyjnego i system przeciwpożarowy mogą być zarządzane przez innego dostawcę. Jeśli wszystkie strony nie zaangażują się w proces integracji, operacje w takim środowisku stają się trudniejsze. W tym kontekście rośnie znaczenie otwartych standardów w wymianie danych o ruchu pojazdów, takich jak DATEX II. Na szczęście czołowi dostawcy wspierają takie standardy. Przykładowo, inteligentne rozwiązanie parkingowe firmy Siemens oferuje łącza do aplikacji innych producentów oparte na otwartych standardach. Interfejs pozwala na integrację danych z systemu z platformami operatorów płatności, egzekwowania przepisów oraz wbudowanymi w pojazdy – pobierają one informacje w celu świadczenia usług zwiększających wartość infrastruktury.

Podstawowe wymagania wobec rozwiązań parkingowych

Kluczem do zarządzania parkingami są bezpieczeństwo i wygoda. Ich zapewnienie nie jest jednak tak proste, jak się wydaje. Centra handlowe muszą dysponować parkingami zapewniającymi wygodę i bezpieczeństwo odwiedzającym. To warunek konieczny, ale nie wystarczający, gdyż wymagania klientów okazują się większe. Integratorzy, którzy dostarczają tego rodzaju rozwiązania, powinni poznać specyficzne potrzeby użytkowników końcowych.

Łatwość znalezienia miejsca parkingowego

Osoby przyjeżdżające do centrów handlowych powinny być informowane o liczbie i lokalizacji wolnych miejsc parkingowych jeszcze przed wjazdem do obiektu. Dostawcy rozwiązań zapewniają to na kilka sposobów. Czujniki umieszczo-



KONSULTANCI RADZĄ

Chociaż w ostatnich latach na rynek trafiło kilka zaawansowanych rozwiązań do zarządzania parkingami, w wielu centrach i galeriach handlowych nadal stosuje się systemy tradycyjne. Rozwiązania tradycyjne to takie, które wykorzystują bramkę z automatem wydającym bilety przy wjeździe i przyjmującym opłatę za parking przy wyjeździe. Wraz z rozwojem technicznym i dążeniem centrów handlowych do usprawnienia swoich systemów w coraz powszechniejszym użyciu będą np. rozwiązania rozpoznające tablice rejestracyjne (LPR). Sprawdzają się one szczególnie w miejscach, gdzie parkowanie jest bezpłatne, ale tylko przez ograniczony czas. Dzięki LPR łatwiej śledzić, jak długo samochód pozostawał na parkingu. Na rynku są dostępne rozwiązania parkingowe kilku marek, klienci powinni zatem wiedzieć, jakimi kryteriami powinni się kierować przy ich wyborze. Przedstawiamy kilka najważniejszych, które należy brać pod uwagę przy zakupie rozwiązania do zarządzania parkingiem.

1. Reputacja i koszt

Dla wielu osób reputacja producenta wydaje się oczywistym kryterium, ponieważ współpraca z renomowaną marką przekłada się na niezawodność. Wiadomo jednak, że reputacja i koszty nie zawsze idą w parze. Dość często ze względu na koszty klienci są skłonni do kompromisów w kwestii jakości produktu. Dlatego dobrym sposobem jest wybór marek, które od dawna dostarczają niezawodne produkty.

2. Trzymanie się jednej marki

Istnieją firmy, które oferują tylko sprzęt lub wyłącznie oprogramowanie do zarządzania parkingiem. Są też dostawcy kompleksowych rozwiązań, którzy sprzedają jedno i drugie. Lepszym wyborem jest firmowe oprogramowanie dostarczane przez dostawcę sprzętu.

3. Instalacja i wsparcie

Dostawca powinien zapewniać wsparcie dla instalacji i konfiguracji rozwiązania od początku wdrożenia. Należy też upewnić się, że system wymaga minimum utrzymania oraz ma zapewniony szybki serwis posprzedażny. Niektórzy eksperci sugerują, że priorytetem powinna być obecność lokalnego przedstawicielstwa dostawcy, który zna lokalne uwarunkowania i potrafi zapewnić odpowiednie wsparcie. Wszelkie przestoje i awarie produktu wiążą się ze stratami dla jego użytkowników. Dlatego kupując rozwiązanie, należy mieć jasność co do tego, jak szybko dostawca jest w stanie zapewnić wsparcie serwisowe na wypadek awarii. Z dostawcą rozwiązań powinna zostać zawarta umowa dotycząca obsługi posprzedażnej.

4. Szczegółowe raporty

Rozwiązanie powinno dostarczać ustrukturyzowane i szczegółowe raporty na temat płatności dokonywanych przez klientów, a także dane analityczne dla zarządu. Te ostatnie dadzą wiedzę np. o porach szczytu i rozkładzie częstotliwości wykorzystania parkingu, ułatwiając podejmowanie decyzji w zakresie taryf i innych polityk.

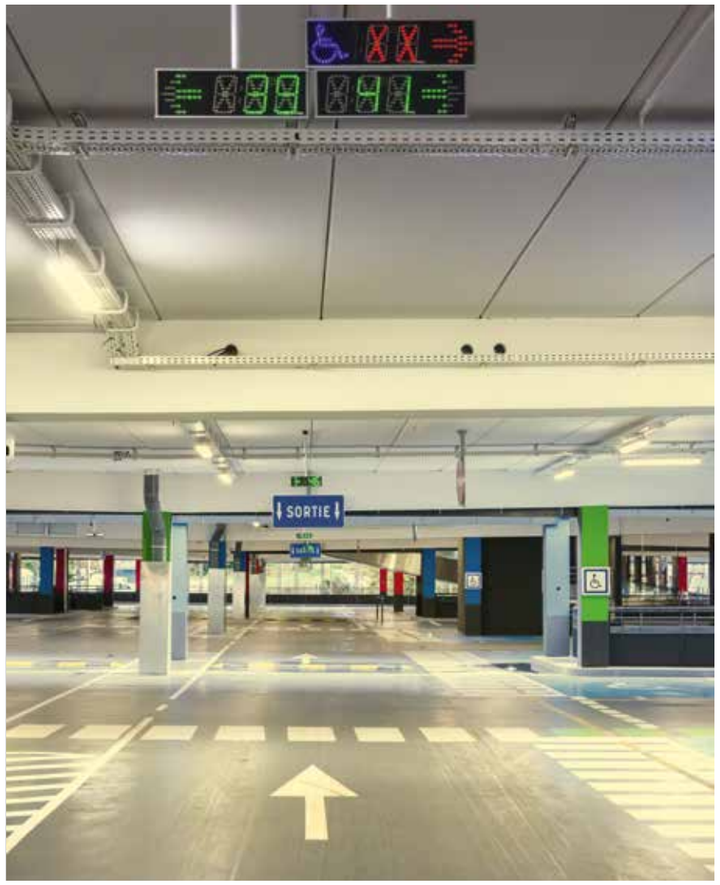
5. Przyjazny, ale bezpieczny

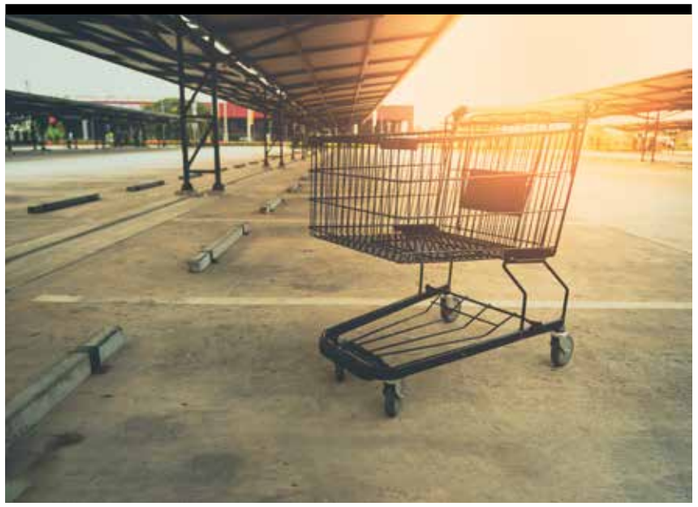
Klienci odwiedzający centrum handlowe nie będą zadowoleni, jeśli rozwiązanie parkingowe okaże się trudne w użyciu. Wygoda użytkownika powinna być priorytetem. Łatwiejsza będzie również praca personelu centrum handlowego, jednak nie może się to odbywać kosztem bezpieczeństwa.

6. Integracja z innymi systemami

Możliwość zintegrowania systemów zarządzania parkingami z innymi systemami, np. safety i security, pomaga w lepszym zarządzaniu obiektem. W przypadku niepożądanych zdarzeń zintegrowane systemy mogą działać szybciej. Takie rozwiązania są również łatwiejsze w obsłudze i kontroli.

Zainstalowanie nowych rozwiązań parkingowych w już istniejących centrach i galeriach handlowych stanowi wyzwanie, które zwiększa konieczność ich integracji z systemami firm trzecich





ne w każdym miejscu parkingowym informują system o stanie zajętości przestrzeni. Zebrane z nich dane mogą być wyświetlane na tablicach informacyjnych umieszczonych na zewnątrz parkingów. Niektóre rozwiązanie mogą również zapewniać usługi mobilne – kierowca po wysłaniu wiadomości do systemu uzyskuje aktualną informację o wolnych miejscach postojowych. Istnieją również takie rozwiązania oparte na aplikacjach, które informują kierowcę o tym, gdzie może zaparkować pojazd.

Bezpieczeństwo

Do zapewnienia bezpieczeństwa zaparkowanych samochodów niezbędne są systemy monitoringu wizyjnego. Nie tylko dostarczają dowody do celów dochodzeniowych, ale też – dzięki takim aplikacjom, jak system rozpoznawania tablic rejestracyjnych (LPR) – mogą pomóc w identyfikacji samochodów (np. wymagających specjalnej obsługi pojazdów VIP) . W wykrywaniu intruzów i natychmiastowym powiadamianiu pracowników ochrony przydatne są również rozwiązania analityczne. Kilku największych światowych dostawców zabezpieczeń oferuje rozwiązania przeznaczone do zarządzania parkingami, obejmujące kamery wyposażone w funkcje LPR zintegrowane z systemem kontroli dostępu.

Opłacalność

Wielu użytkowników końcowych obawia się wysokich kosztów inwestycji w rozwiązanie. Cena zakupu może stanowić barierę, zatem integratorzy systemów oraz dostawcy rozwiązań powinni starać się przekonać ich o długoterminowych korzyściach finansowych, takich jak zwiększenie wydajności operacyjnej.

Wiele opcji płatności

Klienci powinni mieć możliwość zapłaty za parking w preferowanej przez siebie formie. Może to być karta, gotówka lub mobilny system płatności, np. Apple Pay. Większy wybór może przyspieszyć wjazd i ograniczać tworzenie się długich kolejek. Oprogramowanie do zarządzania miejscami parkingowymi powinno

Odpowiedzią na wymagania klientów w obiektach handlowych jest połączenie rozwiązań, które zwiększają bezpieczeństwo i usprawniają działalność biznesową zarządzającym

być łatwe do skonfigurowania i ustawienia, mierzyć czas i obliczać koszt parkowania. W przypadku samochodów z przepustkami wydanymi przez zarząd system ma je wykluczać z płatności.

Integracja i modernizacja

W rozwiniętych krajach centra handlowe działają od lat i wiele obiektów, zwłaszcza starszych, wymaga rozwiązań, które można zintegrować z istniejącymi już systemami. Integratorzy systemów często będą musieli liczyć się z tego typu ograniczeniami.

Analityka

Rozwiązania analityczne, dające głębszy wgląd w zachowania klientów, umożliwiają zarządzającym lepszą ich obsługę oraz optymalizację operacji. Mogą również dostarczać informacji o stanie urządzeń i potrzebie konserwacji. Raportowanie można zautomatyzować i zaplanować wysyłanie informacji pocztą elektroniczną w regularnych odstępach czasu. Odpowiedzią na wymagania klientów w tym obszarze jest połączenie rozwiązań, które zwiększają bezpieczeństwo i usprawniają działalność biznesową zarządzającym. Integrator systemów, który dobiera sprzęt i oprogramowanie oraz integruje je z istniejącymi systemami, musi zapewnić ich bezproblemową współpracę.

Czego oczekują klienci parkingów?

Modernizacje w galeriach handlowych często są skoncentrowane na poszerzaniu sieci sklepów, oferty gastronomicznej i kulturalnej oraz wzbogacaniu zakresu usług. Parking jako pierwszy punkt styku z klientem jest często niedoceniany. A przecież zakupowe doświadczenie i opinia klienta zaczynają się i kończą właśnie tam. Jako eksperci od systemów parkingowych i systemów zabezpieczeń w Polsce pokazujemy, jak zwiększać przewagę konkurencyjną za pomocą rozwiązań parkingowych, aby współtworzone przez parking pierwsze i ostatnie wrażenie klienta z wizyty w centrum handlowym było jak najlepsze.

Przynależność do holenderskiego holdingu TKH Group daje C&C Partners możliwość wdrażania na polskim rynku rozwiązań zgodnych ze światowymi trendami technologicznymi. Jednym z nich jest system przeznaczony do parkingów wielopoziomowych, nadzorujący ponad 180 tys. miejsc parkingowych zlokalizowanych w 35 krajach. W Polsce możemy poszczycić się realizacjami systemów parkingowych w najbardziej prestiżowych galeriach, np. Galeria Północna, Arkadia, Wroclavia, Jurajska.

Nowoczesne parkingi w centrach handlowych

Z przeprowadzonych badań wynika, że dla 84% klientów centrów handlowych bezstresowe parkowanie ma znaczenie kluczowe, wśród rodzin z dziećmi – dla aż 88%[2]. Nie dziwi więc, że kierowcy chętniej wybierają parkingi z nowoczesnymi systemami wspomagającymi znalezienie wolnego miejsca postojowego. Park Assist jest pierwszym wprowadzonym na polski rynek systemem zajętości miejsc parkingowych opartym na sensorach z kamerami.

Wielkość parkingu nie ma znaczenia

Dopełnieniem naszej oferty rozwiązań parkingowych jest system ParkEyes przeznaczony do średnich i małych parkingów podziemnych. Podstawowym zadaniem takich systemów jest wskazanie wolnego miejsca poprzez sygnalizację optyczną specjalnych sensorów wyposażonych w kamery i diody LED. Kierowca ma także dostęp do aplikacji mobilnej wskazującej online stan zajętości parkingu. Ciekawą funkcją jest możliwość znalezienia zaparkowanego pojazdu w aplikacji czy infokioskach zlokalizowanych na piętrach galerii handlowej.

52% kierowców zapomina, gdzie zaparkowało swoje auto[2]

Komfort i bezpieczeństwo

Integracja z system poboru opłat pozwala na wyznaczanie i różnicowanie stawek za parkowanie na poszczególnych miejscach parkingowych, np. dla klientów VIP. Często zdarza się, że klienci parkują nieprawidłowo, zajmując więcej niż jedno miejsce. Odpowiednia konfiguracja systemu pozwala na dyscyplinowanie kierowców wg zasady: zajmujesz dwa miejsca – płacisz podwójnie.
Kamery zainstalowane w czujnikach pozwalają zwiększyć bezpieczeństwo użytkowe, w sposób ciągły monitorując każde miejsce parkingowego. Dlatego takie zdarzenia, jak stłuczki czy otarcia zostają zapisane w systemie, co umożliwia szybkie wskazanie sprawcy. Systemy zajętości bazujące na kamerach zapewniają także bogatą bazę danych marketingowych wykorzystywanych podczas planowana działań operacyjnych.
C&C Partners, pełniąc na polskim rynku funkcję pioniera w rozwiązaniach przeznaczonych do parkingów podziemnych, dba o bezpieczeństwo kierowców oraz interesy ich właścicieli. Oferuje kompleksowe rozwiązania zarówno z branży zabezpieczeń (np. systemy CCTV, KD), jak i komunikacji interkomowej. Rozwiązania te podnoszą komfort parkowania, poprawiają przepływ ruchu oraz wspomagają pracę właścicieli galerii handlowych.

25% klientów centrów handlowych jest skłonne zapłacić więcej za lepsze i wygodniejsze miejsca parkingowe[3]

C&C Partners

ul. 17 Stycznia 119, 121, 64-100 Leszno
www.ccpartners.pl

1) Raport: At Your Service. The Importance of Services in Shopping Centers. ECE Market Research no 2/2016
2) Badania Insurance.com
3) Badania Park Assist

Koniec z kuciem betonu

OVS – czujki parkingowe instalowane nad podłożem

Firma OPTEX w swoim nowym produkcie zastosowała dwie technologie: mikrofalową i ultradźwiękową, tworząc linię bardzo skutecznych detektorów pojazdów. Dzięki nim można uniknąć prac związanych z montażem pętli indukcyjnych, a także w znacznym stopniu usprawnić zarządzanie parkingiem.

Rys. 1. Czujkę OVS-01CC można wykorzystać w systemach zajętości miejsc parkingowych. Kierowca, wjeżdżając na teren parkingu, wie, w którym sektorze znajdzie wolne miejsce. Czujki są zamontowane przy pasach ruchu przeznaczonych do wjazdu i wyjazdu.

Pętle indukcyjne to sprawdzony od wielu lat sposób na automatyczne otwieranie bram i szlabanów. Nie zawsze jednak można je zastosować, np. gdy nawierzchnia drogi jest nieutwardzona, pod powierzchnią ziemi są rury czy został wykonany system odwodnienia. W takich sytuacjach dużo lepiej sprawdzą się skonstruowane przez firmę OPTEX czujki parkingowe OVS. Instaluje się je na słupku, co sprawia, że nie trzeba prowadzić prac ziemnych, a to oznacza koniec z kuciem betonu i niedogodnościami związanymi z zatrzymaniem ruchu na czas prac remontowych. Wystarczy w odpowiednim miejscu postawić słupek i zamontować na nim detektor, a na panelu sterowania ustawić czułość i zasięg detekcji. Proces kalibracji jest zautomatyzowany, wymaga naciśnięcia tylko jednego przycisku.

Czujki parkingowe OPTEX skutecznie rozpoznają pojazdy, ignorując jednocześnie ruch pieszych. Sprawdzą się we wszystkich obiektach, w których ważne jest odpowiednie zarządzanie ruchem pojazdów.

Seria OVS

W serii czujek parkingowych OVS wykorzystano technologię FMCW (*Frequency-Modulated Continuous-Wave* – radar o fali ciągłej zmodulowanej częstotliwościowo). To nowoczesna technologia, która mimo niewielkiej mocy promieniowania nadajnika (nieprzekraczającej 1 W) pozwoliła zachować zalety radaru impulsowego i dokładnie określać odległości do wszystkich obiektów w zasięgu wiązki. W odróżnieniu od systemów wykrywania i zliczania pojazdów opartych na wideoweryfikacji, czujki serii OVS są odporne na zmienne natężenie oświetlenia i oślepienie w strefie detekcji.

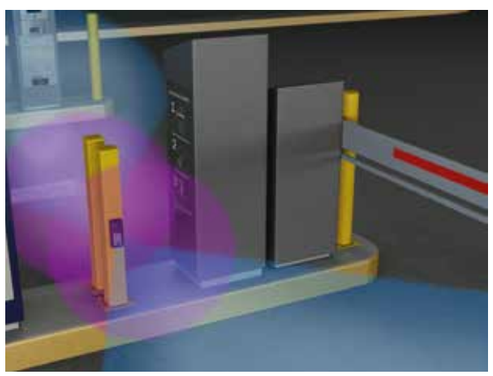
Seria OVS składa się z dwóch modeli: OVS-01GT oraz OVS-01CC.

Model OVS-01GT łączy dwie technologie – mikrofale i ultradźwięki. Z kolei model OVS-01CC wykorzystuje jedynie mikrofale, ale został wzbogacony o algorytm detekcji pojazdów, użyteczny w systemach zliczania. Można go również zastosować w systemach informujących o wolnych miejscach parkingowych (*rys. 1*).

Łatwość instalacji i integracji z systemami parkingowymi

Zainstalowana na słupku lub ścianie czujka OVS-01GT może być łatwo zintegrowana z istniejącymi systemami za pomocą wyjść przekaźnikowych o parametrach obciążalności 30 V, 300 mA. Zasięg działania mikrofali konfiguruje się w zakresie od 0,8 do 5,5 m (8 ustawień), a ultradźwięków w zakresie od 0,1 do 1 m (3 ustawienia). Detektor, który ma czas odpowiedzi 500 ms, wykrywa pojazdy poruszające się z prędkością od 2 do 20 km/h. Przy konfiguracji detektora dostępnych jest pięć poziomów czułości, a także pięć ustawień ignorowania ruchu pieszych. Obudowa o klasie szczelności IP65 pozwala instalować czujkę zarówno wewnątrz, jak i na zewnątrz. Szeroki zakres zasilania, w którym działa, to 12–24 V. Proces kalibracji jest zautomatyzowany, wymaga naciśnięcia tylko jednego przycisku. Z kolei OVS-01 CC to model zaprojektowany do współpracy z systemami liczenia pojazdów różnej wielkości. Pasy w przeciwnych kierunkach ruchu powinny być od siebie oddzielone. Wykrywane pojazdy mogą poruszać się z prędkością od 2 do 60 km/h. Czas reakcji detektora wynosi 300 ms. Czujkę OVS 01-CC montuje się na słupku albo ścianie, pod kątem 90 stopni do kierunku ruchu pojazdów. Strefa detekcji wynosi do 8 m, można wybrać odpowiednią czułość wykrywania (5 ustawień), by dostosować działanie detektora do konkretnych wymagań. Model OVS-01 CC to urządzenie do zastosowań zewnętrznych (odkryty teren) lub wewnętrznych (np. parking podziemny).

	 Model OVS-01CC	 Model OVS-01GT
Funkcjonalność	Detektor z algorytmem detekcji pojazdów użyteczny w systemach zliczania.	Detektor wykrywający obecność pojazdów przy bramach i szlabanach. Alternatywa dla pętli indukcyjnej.
Główne zastosowanie	Systemy parkingowe informujące o dostępności miejsc, systemy kontroli dostępu, systemy rozpoznawania tablic rejestracyjnych	Systemy parkingowe



Rys. 2. Czujka OVS-01GT kontroluje otwieranie i zamykanie szlabanu przy wjeździe na parking

Korzyści z zastosowania

Czujki serii OVS pozwalają wielu integratorom systemów i instalatorom otworzyć się na nowy rynek, jakim są systemy parkingowe, zapewniając klientom wartość dodaną w postaci kompleksowej usługi. Zaproponowanie systemu parkingowego i zarządzania ruchem opartego na pętli indukcyjnej wymagało specjalistycznej wiedzy w zakresie montażu pętli w trudnym środowisku lub generalnie powodowało potrzebę kompromisu pomiędzy poprawnym działaniem systemu a wymaganą przez klienta funkcjonalnością. Ze względu na wyeliminowanie głównej przyczyny tych uciążliwości czujka OVS znacznie ułatwia prace związane z instalacją systemów parkingowych. Instalator poświęci też znacznie mniej czasu na uruchomienie systemu. Styki alarmowe pozwalają w łatwy sposób integrować czujki z systemami parkingowymi, systemami kontroli dostępu czy systemami rozpoznawania tablic rejestracyjnych. Szczególnie ważnym zastosowaniem są parkingi piętrowe, gdzie nie można naruszyć konstrukcji podłogi. Urządzenie sprawdzi się też w zastosowaniach w *smart city*, informując o wolnych miejscach na parkingach miejskich czy autostradowych. □

Optex Security

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

Kamera – oczy i mózg w rozpoznawaniu numerów tablic rejestracyjnych

Automatyczne rozpoznawanie numerów tablic rejestracyjnych (ANPR – *Automatic Number Plate Recognition*) stało się popularną technologią stosowaną w wielu dziedzinach – od kontroli dostępu po egzekwowanie opłat.

TEKST
William Pao
a&s International

W systemie ANPR najważniejszym elementem jest kamera, która musi spełniać określone wymagania i być prawidłowo zainstalowana, by użytkownikom końcowym zapewnić optymalne korzyści. Jakiej kamery użyć, jakie wymagania musi spełniać, a także jak ją zainstalować?

Aplikacje ANPR

Rozpoznawanie numerów tablic rejestracyjnych (LPR – *License Plate Recognition*) – znane również jako automatyczne rozpoznawanie tablic rejestracyjnych (ALPR – *Automatic License Plate Recognition*) lub automatyczne rozpoznawanie numerycznych tablic rejestracyjnych (ANPR) – zyskuje coraz większą popularność. Według badania przeprowadzonego przez Research and Markets, globalny rynek ANPR w okresie 2017–2025 będzie charakteryzował się dużym wzrostem i w 2025 r. osiągnie 1,7 mld USD. ANPR jest przeważnie oparte na konwersji obrazu tablicy rejestracyjnej na ciąg znaków alfanumerycznych za pomocą technologii optycznego rozpoznawania znaków (OCR – *Optical Character Recognition*). Można je stosować w różnych obiektach i do różnych celów, np. na zamkniętych parkingach do wykrywania prób wjazdu nieuprawnionych pojazdów, w garażach do kontroli przepływu ruchu, w centrach handlowych do celów statystycznych. Władze lokalne mogą wykorzystać system do monitorowania przepływu pojazdów pod kątem przyszłych modernizacji drogowych.

Kontrola dostępu

Kontrola dostępu jest jedną z bardziej oczywistych aplikacji umożliwiających wjazd pojazdu na teren obiektu lub wyjazd z niego w sposób zautomatyzowany. Pojazd jest wpuszczany lub nie w zależności od tego, czy jego numer rejestracyjny znajduje się w bazie danych na liście uprawnionych.

Egzekwowanie prawa

Rozpoznanie numerów tablic rejestracyjnych pozwala zidentyfikować niezarejestrowane, a nawet skradzione pojazdy. Umożliwia również wykrywanie samochodów z nieopłaconymi mandatami. W skrajnych przypadkach system może pomóc organom ścigania w śledzeniu podejrzanych pojazdów.

Parking miejski

Zarządzanie parkowaniem w mieście – zwłaszcza szybko rozwijającym się – jest wyzwaniem. Ręczne sprawdzanie opłat za parkowanie zajmuje sporo czasu. Technologia ANPR upraszcza egzekwowanie opłat i poprawia ogólną wydajność.

> Oprócz sterowania przepływem pojazdów, dane dostarczane przez ANPR można wykorzystać do powiadamiania pracowników ochrony o wjeździe pojazdu z osobą niepełnosprawną, która może potrzebować pomocy

Skuteczność procesu rozpoznawania tablic rejestracyjnych zależy od prędkości migawki, głębi ostrości oraz właściwego oświetlenia

Zarządzanie ruchem

Analiza danych generowanych przez systemy ANPR, obrazujących natężenie ruchu pojazdów w obrębie miasta i na jego obrzeżach, dostarcza włodarzom miasta cennych informacji pozwalających usprawnić zarządzanie ruchem ulicznym. Mogą być pomocne w zrozumieniu wzorców tworzenia się korków i spowolnienia czasu przejazdu na konkretnym odcinku.

Inne aplikacje

Dane dostarczane przez ANPR można również wykorzystać do innych celów. Przykładowo operatorzy w supermarketach mogą informować pracowników o parkujących na miejscu dla inwalidów, którzy mogą potrzebować pomocy, np. o osobach niepełnosprawnych lub niedowidzących.

KAMERA: główny komponent ANPR

Na system ANPR składa się kilka komponentów: kamera, działający „silnik" odczytu tablic rejestracyjnych, nośnik pamięci, a także inne opcjonalne elementy, np. przełączniki sieciowe IP, urządzenia wejścia/wyjścia lub audio. Wśród nich najważniejsza jest kamera, której zadaniem jest odczyt numerów tablic rejestracyjnych, często w zmiennych warunkach otoczenia, nieprzerwanie przez 24 godziny na dobę, 7 dni w tygodniu.

Aplikacja ANPR w kamerze czy na serwerze?

Analiza ANPR może być wykonywana w kamerze, w rejestratorze znajdującym się blisko kamery lub na serwerze. Wzrost popularności i oferty kamer odczytujących tablice rejestracyjne wynika z dwóch powodów:

- przetwarzanie i analiza obrazu odbywają się w jednym urządzeniu. Dane z odczytu numerów nie muszą być przesyłane przez sieć, a kamera może być bardzo efektywnym jednoproduktowym systemem kontroli przejazdu, co oznacza mniejsze obciążenie sieci. Ponadto analiza może być wykonywana na nieskompresowanym obrazie;
- większa efektywność kamer ANPR – systemy oparte na platformie serwerowej mogą się nie sprawdzić w najbardziej wymagających scenariuszach. Często wymagają większej mocy obliczeniowej w porównaniu z kamerami z uruchomioną aplikacją ANPR. Jest to związane m.in. z niedociągnięciami programowymi. Struktura kodu aplikacji ANPR przeznaczonej na jednostki serwerowe nie jest optymalizowana pod kątem zużycia zasobów, tak jak jest to w przypadku ograniczonej mocy obliczeniowej kamer.

Jakość działania dostępnego oprogramowania ANPR różni się, w zależności od dostawcy, mocą obliczeniową czy nieefektywną konstrukcją silnika ANPR. Niektóre aplikacje mogą odczytywać tylko jedną tablicę w danej jednostce czasu (wtedy mowa o odczycie z jednego pasa ruchu o standardowej szerokości 3 m). Takie aplikacje nie są w stanie odczytywać tablic wielu pojazdów na drogach dwujezdniowych czy niestandardowych tablic z innych regionów.

Wymagania dotyczące kamery

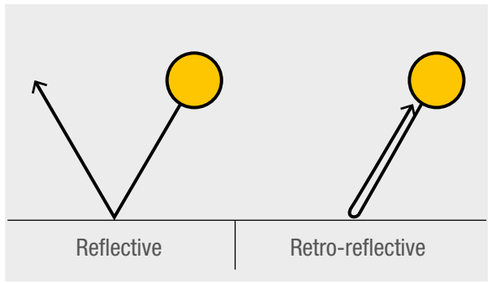
Kamery stosowane do aplikacji ANPR muszą spełniać specjalne wymagania. Kluczową kwestią jest to, że aby proces rozpoznawania działał skutecznie, obraz wygenerowany przez kamerę musi być wystarczająco ostry.

Przetwornik

Istotnym elementem każdej kamery jest właściwy przetwornik obrazu. Większość nowych modeli kamer radzi sobie dobrze w trudnych warunkach oświetleniowych. Obecnej technologii wytwarzania przetworników CMOS nie przeszkadza wzrost gęstości pikseli i najnowsze przetworniki 1/3" są znacznie lepsze niż niewiele starsze przetworniki 1/2". Kamery w warunkach dobrego oświetlenie mogą bez problemów pracować w tzw. trybie dziennym (tj. kolorowym) z włączonym filtrem odcinającym promieniowanie podczerwone. W warunkach niedostatecznego oświetlenia kamery przechodzą w tryb nocny, tj. czarno-biały, by umożliwić wprowadzenie promieniowania IR z promienników wbudowanych lub wewnętrznych. Najczęściej stosuje się oświetlacze IR o długości fali 850 nm. W przypadkach wykorzystania tego sposobu doświetlenia na trasach szybkiego ruchu lub w pobliżu portów lotniczych wymagane jest użycie oświetlaczy 940 nm.

Oświetlenie

Oświetlenie jest kluczowym parametrem kamery, ponieważ musi ona generować obraz tablic i w dzień, i w nocy, zwłaszcza że sugerowana szybkość migawki jest 10x większa od domyślnej, tj. 1/250 s. Wbudowane oświetlacze IR są użytecznym narzędziem umożliwiającym optymalny odczyt nawet w trudnych warunkach oświetleniowych. Diody LED muszą być wyposażone w odpowiednie soczewki i często także dyfuzory, aby równomiernie rozłożyć oświetlenie w kadrze, bez tzw. hot-spota, czyli bardzo jasno oświetlonego obszaru w środku kadru.
Niektóre tablice rejestracyjne nie są retro refleksyjne (np. w krajach Bliskiego Wschodu) i do prawidłowego odczytu wymagają użycia światła białego (*rys. 1*). Na Florydzie problem sprawiają metalowe pomarańczowo-zielone tablice. Do ich odczytu często używane jest oświetlenie IR o długości fali 750 nm, widziane przez kierowców jako czerwona poświata i czasami mylone z czerwonym światłem sygnalizacji świetlnej.



Rys. 1. Wyjaśnienie zasady zjawiska retro refleksyjności

Rozdzielczość i kompresja

Rozdzielczość obrazu to kolejny kluczowy parametr do rozważenia. Zaleca się, aby nie była niższa niż 1080p, ale nie powinna być zbyt duża bez wyraźnej potrzeby. Specjaliści uważają, że do odczytu standardowej tablicy w UE wystarczy ok. 256 pikseli na metr. Większa gęstość pikseli sprawi, że działanie systemu będzie wolniejsze, a to może spowodować pominięcie odczytu kolejnych tablic rejestracyjnych.
Większość nowoczesnych kamer IP może wysyłać obrazy zakodowane w standardzie MJPEG lub H.264. Warto pamiętać, żeby kompresja była ograniczona do minimum. Otrzymany obraz może wyglądać znakomicie dla człowieka, ale po powiększeniu jest rozmyty, co powoduje błędy w odczycie, zwłaszcza gdy tablica jest uszkodzona, brudna lub źle oświetlona.

Warunki środowiskowe

Instalacja kamery w pobliżu drogi stanowi nie lada wyzwanie. Pył, kurz i brud nanoszony spod kół przejeżdżających samochodów wymaga odpowiedniej obudowy kamery, by mogła skutecznie działać. Zdaniem ekspertów w większości scenariuszy wystarczy obudowa o klasie szczelności IP66 i dobrej jakości osłony przeciwsłoneczne chroniące obiektyw przed słońcem i pyłem.

Instalacja kamery

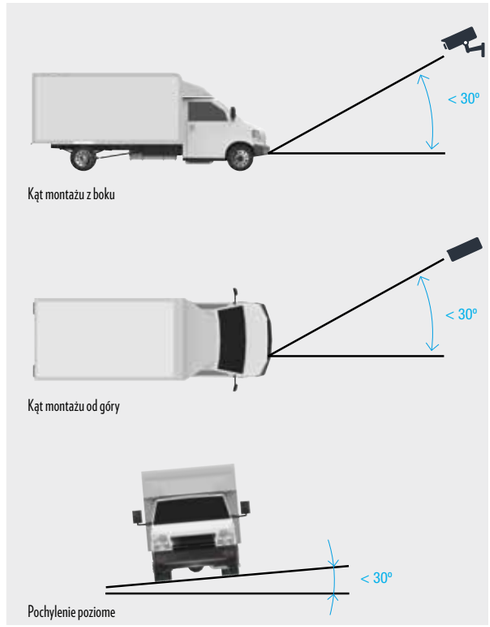
Właściwa instalacja odgrywa kluczową rolę w odczytywaniu numerów tablic rejestracyjnych, ponieważ poprawność montażu decyduje o wydajności i skuteczności systemu. Szczególnie ważne jest tu prawidłowe ustawienie kamery, wpływające na jakość generowanego obrazu, a tym samym na wydajność procesu rozpoznawania numerów rejestracyjnych.

Punkt montażu

Odległość między przejeżdżającym pojazdem a kamerą różni się w zależności od wymagań użytkownika. Kamera ANPR może odczytywać numery nawet z dużych odległości. Należy jednak pamiętać, że im pojazd jest bardziej oddalony, tym więcej zmiennych ma wpływ na pracę systemu, np. najeżdżanie pojazdów na siebie i w efekcie brak możliwości rozpoznania tablicy rejestracyjnej.

Kąt patrzenia

Ważny jest również kąt, pod jakim kamera jest skierowana w stronę pojazdu. Użytkownik powinien brać pod uwagę dwa: kąt pionowy między osią wzdłużną kamery a płaszczyzną, po której porusza się pojazd, oraz kąt poziomy między osią wzdłużną kamery a osią wzdłużną pojazdu. Im mniejszy kąt, tym lepiej. Najefektywniej funkcja rozpoznawania tablicy działa, gdy kąt mieści się w zakresie 30 stopni (*rys. 2*).



Rys. 2. Maksymalne kąty montażu kamery do właściwego odczytu tablic rejestracyjnych

Pozycja

Należy zwracać uwagę, aby kamera była odpowiednio ustawiona, np. za szlabanem, a nie przed nim, żeby ramię szlabanu nie zasłaniało pola widzenia kamery przechwytującej obraz tablicy rejestracyjnej. Jeśli z jakiegoś powodu tablica nie została poprawnie odczytana, to prawdopodobieństwo ponownego rozpoznania jest niewielkie. Gdy wjazd jest szeroki, a pojazdy poruszają się środkiem zamiast po wyznaczonym pasie ruchu lub wjazd jest pod kątem ostrym, warto zastosować więcej kamer. Techniczne rozwiązania drogowe wpływające na organizację ruchu, np. gumowe ograniczniki wyznaczają prawidłowe ustawienie pojazdów pod właściwym kątem do odczytu tablic.

Liczba pikseli

Wielkość obrazu tablicy rejestracyjnej jest bardzo ważna. Najlepszym sposobem jest podawanie wysokości w pikselach. Dobry silnik odczytuje numery rejestracyjne do 12 pikseli, ale optymalne rozpoznawanie uzyskuje się przy 20–30 pikselach. Dlatego ważne jest, aby stosować właściwy obiektyw. Według specjalistów najlepiej sprawdzą się kamery 1080p.

Inne wymagania

Czasami pojawiają się różne problemy, np. z zasilaniem czy komunikacją. Wybór właściwego miejsca montażu może stanowić najtrudniejszy etap wdrożenia. Należy uwzględnić specyfikę lokalizacji, w której kamerę ANPR można zainstalować. Głównym problemem jest uzyskanie pozwolenia na instalację w najlepszym miejscu dla kamery, trzeba pamiętać o zachowaniu odpowiedniej odległości, trajektorii czy kątów. Podsumowując, każda instalacja ma inne cele i wymagania. Projektując system ANPR, instalator musi je w pełni znać. Musi przewidzieć, czy tablica rejestracyjna zawsze będzie w polu widzenia kamery i w jakim zakresie prędkości pojazdów odczytają tablice. Może przydadzą się środki spowalniania ruchu lub pasy nakierowujące pojazd do pola widzenia kamery.

Mobilny LPR

W omówionym systemie ANPR kamera jest zamontowana na stałe, lecz może on być także w wersji mobilnej, z kamerą zainstalowaną na pojeździe ruchomym, np. na samochodach patrolowych, autobusach, robotach czy śmieciarkach. Wówczas jest skanowana tablica każdego pojazdu, który pojawia się w polu widzenia kamery. Pojazd z kamerą skanującą może poruszać się po mieście, prowadząc swoją regularną działalność. Każdy przechwycony numer jest przesyłany do serwera ANPR zlokalizowanego w chmurze lub w centralnej serwerowni. Rejestrowany jest czas, lokalizacja, obraz tablicy rejestracyjnej oraz obraz ogólny z tyłu lub przodu pojazdu. System ANPR, sprawdzając każdy tag w bazie danych, może wysyłać komunikaty np. do policji, gdy numer rejestracyjny figuruje na czarnej liście wykroczeń czy w bazie pojazdów skradzionych. □

Przegląd najpopularniejszych rozwiązań ANPR dostępnych na polskim rynku, stosowanych w rozwiązaniach parkingowych i kontroli wjazdu/wyjazdu

www.dahuasecurity.com/pl

Dahua: ITC215-PW4I – kamera ANPR AI

Wśród tegorocznych premier produktów w portoflio Dahua Technology pojawiła się nowa seria kamer ANPR automatycznie rozpoznających numery tablic rejestracyjnych. ITC215-PW4I-LZ to pierwsza kamera w ofercie dedykowana do rozwiązań parkingowych, której działanie opiera się na wykorzystaniu algorytmów sztucznej inteligencji.

Producent przyzwyczaił już użytkowników swoich kamer do doskonałej optyki. W najnowszym modelu ANPR za jakość obrazu odpowiedzialny jest znakomity przetwornik Sony Starvis 1/2.8" o rozdzielczości 2 Mpix oraz jasny obiektyw (F.13) moto-zoom 2,7 –13,5 mm. Dzięki wykorzystaniu technologii głębokiego uczenia *(deep learning)* skuteczność odczytu numerów tablic rejestracyjnych jest jeszcze wyższa. Ponadto, dzięki zaawansowanej analizie obrazu, kamera dostarcza dane na temat typu pojazdu oraz jego koloru. Daje to nowe możliwości przy przeglądaniu archiwum w poszukiwaniu konkretnego zdarzenia.

Najważniejsze parametry kamery	
Migawka	1/50-1/10 000
WDR	120 dB
Min. oświetlenie	0,005 lx/F1.3
Dokładność rozpoznania	99%

www.hikvision.com/pl

Hikvision: Kamera ANPR DS-2CD7A26G0/P-IZ(H)S

Firma Hikvision rozszerza swoje portfolio o nową kamerę ANPR DeepInView z technologią DarkFighter.

Kamera DS-2CD7A26G0/P-IZ(H)S została wyposażona w przetwornik obrazu *progressive scan* CMOS 1/2,8" generujący obraz 2 Mpix (1920 x 1080), z prędkością 50/60 kl./s. Dzięki zastosowanej technologii kamera ANPR z serii 7 potrafi rozpoznać pojazd i odczytać jego tablicę rejestracyjną, nie sczytując przy tym nadruku na plandekach pojazdów czy billboardach przy drogach. Dzięki zastosowanym w urządzeniu technologiom dokładność rozpoznania kierunku ruchu pojazdu jest większa niż 96%, a rozpoznawanie tablic rejestracyjnych nie mniej niż 98%.
Dużą zaletą oprogramowania ANPR jest możliwość tworzenia specjalnych białych i czarnych list pojazdów. W zależności od tego, na jakiej liście znajdzie się dany numer tablicy rejestracyjnej (maksymalnie można zdefiniować 10 tys. numerów), istnieje możliwość wywołania dostępnego zdarzenia alarmowego, m.in.: powiadomienie centrum monitoringu, wysłanie zdjęcia na FTP czy kartę pamięci. Dodatkową funkcjonalnością kamery jest rozpoznawanie motocykli, kierunku jazdy pojazdów, identyfikacja kraju czy wykrycie pojazdów bez tablicy rejestracyjnej.
Kamera z serii 7 ANPR wspiera kompresję obrazu H.265, ma klasę szczelności obudowy IP67 i odporności mechanicznej IK10. Ma 5 zdefiniowanych strumieni oraz wbudowany oświetlacz podczerwieni o zasięgu do 50 m (dla obiektywu 2.8-12 mm) lub 100 m (obiektyw 8-32 mm). Dodatkowo kamera może mieć interfejs Wiegand czy stopień ochrony NEMA4X.
DS-2CD7A26G0/P-IZ(H)S idealnie sprawdzi się m.in. na parkingach, dworcach, lotniskach, w miejskim systemie monitoringu wizyjnego czy też systemach kontroli wjazdu ze szlabanami lub bramami automatycznymi.

Najważniejsze parametry kamery	
Migawka	do 1/100 000
Min. oświetlenie	0,002 lx/F1.2 (AGC on), tryb kolor, filtr IR 0 lx (oświetlacz IR)
Dokładność rozpoznania	>98%

www.suma.com.pl

SUMA: VIVOTEK IB9387-LPR

VIVOTEK IB9387-LPR to kamera z automatycznym odczytywaniem tablic rejestracyjnych. Stanowi samodzielny system LPR z wbudowanym oprogramowaniem do rozpoznawania numerów tablic rejestracyjnych. Wyjątkowym atutem jest zabezpieczenie kamery licencją Trend Micro. Aplikacja LPR umożliwia tworzenie białych i czarnych list do zaawansowanej weryfikacji tablic rejestracyjnych. Kamera potrafi weryfikować tablice rejestracyjne z większości krajów na świecie jednocześnie. System ma możliwość konwertowania odczytanych numerów tablic rejestracyjnych na sygnały w standardzie Wiegand do systemu kontroli dostępu. Dzięki otwartemu API istnieje również możliwość integracji z innymi systemami, takimi jak zarządzanie parkingami, system poboru opłat czy wagowy. Rozwiązanie idealnie nadaje się do parkingów i systemów poboru opłat Stop & Go. Kamera IB9387-LPR może działać jako wbudowana niezależna aplikacja kontroli dostępu oparta na oprogramowaniu LPR.

Użytkownicy mogą zarządzać i tworzyć kilka białych i czarnych list, odpowiednio je nazywając. Dzięki temu pojazdy można przypisywać do kilku grup, np. pracownicy, dostawa, goście itp. W momencie odczytania tablicy rejestracyjnej z białej listy system m.in. automatycznie otworzy szlaban, uruchomi wiadomość powitalną i wiele więcej. Czarna lista pozwala na szybkie wykrycie niepożądanego pojazdu i uruchomienie alarmu oraz poinformowanie odpowiednich służb. Można uruchomić wiele list bez ograniczenia liczby obsługiwanych tablic rejestracyjnych. Kamera pozwala też na wyeksportowanie wyników rozpoznawania tablic rejestracyjnych i powiązanych zdarzeń. Kamera osiąga skuteczność do 98%. Najważniejsze technologie zastosowane w kamerze: WDR Pro, Smart Stream III, Smart IR II, Supreme Night Visibility, oprogramowanie zabezpieczające Trend Micro.

Najważniejsze parametry kamery	
Migawka	1/5 do 1/32 000
WDR	120 dB
Min. oświetlenie	0,06 lx/F1.4 (kolor), <0,01 lx/F1.4 (cz-b), 0 lx (z podświetleniem IR)
Dokładność rozpoznania	do 98%

www.vcn.pl / www.vnetlpr.vcn.pl

VCN: VnetLPR – tam, gdzie same kamery LPR nie wystarczą

VnetLPR

Tam, gdzie możliwości kamer z analityką LPR już nie wystarczają, zaczyna się prawdziwa przygoda z budowaniem funkcjonalności. System awizacji i przepustek VnetLPR to odpowiedź na większość potrzeb obiektów logistycznych, przemysłowych, biurowych, rekreacyjnych i handlowych. Został opracowany do współpracy z każdą kamerą LPR. Z kamerami największych producentów na rynku współpracuje już dzisiaj.

Cechy użytkowe VnetLPR: elektroniczna książka wjazdów, wyjazdów i ruchu pieszego, wielopoziomowy system nadawania uprawnień i/lub pobierania ich na bieżąco z systemów zewnętrznych, wymiana informacji z systemami klienta lub jego najemców, sterowanie szlabanami, tablicami informacyjnymi, drukarkami przepustek, czytnikami dokumentów tożsamości itp., dostęp do zasobów systemu za pomocą przeglądarki WWW, możliwość przechwytywania i archiwizacji wybranych strumieni kamer IP potrzebnych do dodatkowego dokumentowania procedur.
Korzyści: **łatwość wdrożenia, intuicyjność obsługi, podwyższenie bezpieczeństwa, obniżenie kosztów,** pełne i dynamiczne planowanie oraz kontrola ruchu kołowego i osobowego, przyspieszenie i jednocześnie standaryzacja procedur, natychmiastowy dostęp do zebranych danych, uprawnień i statystyk filtrowanych wg dowolnego parametru, usprawnienie obsługi i jednocześnie nadzór nad prawidłowością działań ochrony na bramach wjazdowych. Wielopoziomowy system uprawnień pozwala w tym samym czasie optymalnie korzystać z systemu przez wiele osób, często z różnych firm lub działów, przy zachowaniu poufności wybranych danych.

VnetLPR może przejąć „obowiązki" nawet kilku osób zaangażowanych w planowanie i weryfikację procedur na bramach wjazdowych i wewnątrz obiektu. Wciąż powstają kolejne funkcjonalności tworzone na zlecenia klientów końcowych, agencji ochrony lub integratorów.
Pamiętajmy, że kamery LPR to urządzenia generujące dane. Jednak dopiero podłączenie ich pod dobrze zaprojektowany system zapewnia zwielokrotnione korzyści. Zapytaj nas, w jaki sposób VnetLPR może pomóc w twoim biznesie.

Głos branży

BRANŻA SECURITY MA DO ZAOFEROWANIA SEKTOROWI HANDLU WIĘCEJ NIŻ TYLKO SYSTEMY ZABEZPIECZEŃ. SYSTEMY DOZOROWE DOSTARCZAJĄ CENNYCH DANYCH STATYSTYCZNYCH. A JAKIE OCZEKIWANIA MA BRANŻA RETAIL?

Adam Brzezicki

Axis Communications

Najnowsze technologie wspomagają handel

Kamery w systemach dozoru wizyjnego mają za zadanie rejestrować obrazy obserwowanego obszaru w celu ochrony ludzi i mienia. Wraz z rozwojem techniki mogą też spełniać dodatkowe funkcje, często niezwiązane z ochroną. Bardzo dobrym przykładem jest branża handlu detalicznego.

Prowadzenie biznesu nie jest łatwe. Każda podjęta przez nas decyzja jest tu na wagę złota. A im więcej posiadamy informacji na dany temat, tym lepiej możemy sytuację przeanalizować, by podjąć odpowiednie działania. Zarządzanie personelem jest jednym z kluczowych elementów mających wpływ na liczbę klientów oraz ich zadowolenie. Z pomocą przychodzą narzędzia dostarczające informacji o liczbie osób odwiedzających naszą placówkę, np. Axis People Counter oraz Axis Occupancy Estimator.

Nikt nie lubi stać długo w kolejkach. Dzięki implementacji w kamerze odpowiednich algorytmów analizy obrazu, takich jak Axis Queue Monitor, możemy wykryć, że tworzy się zbyt długa kolejka, i odpowiednio zareagować. Możemy również pójść krok dalej i zintegrować analizę obrazu z systemami audio. Takie rozwiązanie będzie automatycznie powiadamiało personel o wzmożonym ruchu przy kasach.

To tylko niektóre korzyści, jakie możemy uzyskać, implementując najnowsze technologie z zakresu analizy obrazu. Dzięki rozwiązaniom Axis Communications w segmencie handlu detalicznego możemy lepiej analizować różne czynniki, takie jak organizacja sklepu czy liczba personelu i ich wpływ na sprzedaż oraz zadowolenie klientów. Jesteśmy w stanie trafniej analizować wyniki czasowych promocji lub to, jakich klientów przyciągają poszczególne reklamy i akcje marketingowe. Mając więcej informacji, możemy szybko podjąć skuteczniejsze działania, które zapewnią stabilny rozwój naszego biznesu.

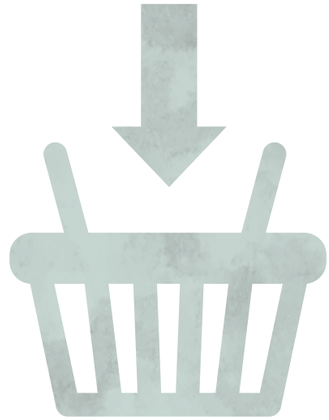
Marcin Walczuk

BCS

Bezpieczny handel, większe zyski

Zabezpieczenie obiektów handlowych, począwszy od małych sklepów po ogromne centra handlowe, już dawno przestało opierać się na prostym systemie alarmowym czy systemie telewizji dozorowej złożonym z kilku czy kilkunastu kamer.

Niejednokrotnie, a w przypadku dużych obiektów praktycznie zawsze są to skomplikowane centralnie zarządzane systemy zabezpieczenia, w których skład wchodzą, oprócz wspomnianych systemów SSWiN i CCTV, również systemy przeciwpożarowy oraz kontroli dostępu.



Priorytetem powinno być zapewnienie bezpieczeństwa osobom, które przybywają na terenie danego obiektu handlowego. Należy przede wszystkim przestrzegać przepisów budowlanych, norm przeciwpożarowych czy instrukcji BHP. Zastosowanie nowych rozwiązań technologicznych z zakresu monitoringu wizyjnego może zdecydowanie podnieść poziom bezpieczeństwa, ułatwić obsługę i odciążyć operatora, wykonując za niego coraz więcej zadań.

Wykorzystanie zaawansowanej analizy obrazu i algorytmów sztucznej inteligencji pozwala ograniczyć liczbę fałszywych alarmów i reagować na sytuacje, które faktycznie mogą stanowić zagrożenie. Funkcja detekcji pozostawionych obiektów pomoże szybko namierzyć taki przedmiot i podjąć odpowiednie kroki. Dzięki skróceniu czasu reakcji zwiększamy również szansę na odnalezienie osoby odpowiedzialnej za całe zdarzenie. Z kolei funkcja monitorowania zachowania tłumu czy poszczególnych osób ułatwi zlokalizować źródło paniki bądź wychwycić z otoczenia osoby zachowujące się podejrzanie.

Bezpieczeństwo jest najważniejsze, ale nowoczesny system CCTV może służyć już nie tylko do zabezpieczenia obiektu. Zaczyna stanowić coraz potężniejsze narzędzie analityczne, które szczególnie w handlu pomoże zwiększyć obroty placówek handlowych. Dane spływające z kamer w postaci map cieplnych obiektów, obrazujące miejsca o największym ruchu pozwolą lepiej pozycjonować (eksponować) produkty, na których sprzedaży zależy nam najbardziej. Raporty z kamer zliczających ludzi daje informacje, kiedy i ile osób weszło do sklepu, które można powiązać z innymi zmiennymi, takimi jak pora dnia, pogoda czy pora roku. Metadane, które pozyskujemy z kamer identyfikujących twarze czy z inteligentnych rejestratorów, określające płeć, przedział wiekowy czy nastrój, pozwolą lepiej ukierunkować działania marketingowe skierowane do docelowej grupy odbiorców.

Rozwój technologii zabezpieczeń jest ściśle powiązany z sektorem handlowym. Z jednej strony musimy zapewnić bezpieczeństwo, i to w dalszym ciągu powinien być cel nadrzędny każdego systemu zabezpieczeń, z drugiej zaś – nowoczesne rozwiązania pozwalają zwiększyć przychody. Dlatego tak ważna jest bliska współpraca producentów urządzeń służących do ochrony obiektu z jego odbiorcami, czyli w tym przypadku różnego rodzaju sieciami handlowymi.

Maciej Pietrzak

Technical Team Leader
Dahua Technology Poland

Nowe narzędzia branży security dla handlu

Pomimo stale rosnącej popularności sprzedaży internetowej fizyczne sklepy są nadal głównym kanałem dystrybucji. Klient ceni sobie bowiem możliwość obejrzenia produktu przed zakupem i skonfrontowania go ze swoimi oczekiwaniami. Sprzedaż internetowa niestety takiej możliwości nie daje. Jako przykład może posłużyć znany polski sklep internetowy z obuwiem, który doczekał się sklepu stacjonarnego, umożliwiającego przymierzenie na miejscu wielu modeli. Oprócz inwestowania w metody pozwalające na podniesienie atrakcyjności obiektu handlowego nieodzowne jest stałe dbanie o zapewnienie bezpieczeństwa.

Straty z tytułu kradzieży w sektorze retail w 11 krajach europejskich i Rosji sięgają 49 mld euro, a tylko w polskich sklepach wyniosły 1,7 mld euro. Przytoczone da-

ne pochodzą z raportu „Bezpieczeństwo w handlu detalicznym w Europie: wykraczając poza straty" *(Retail Security in Europe. Going beyond. Shrinkage, Crime&tech, 2019)*. Myśląc o kradzieżach, mamy przede wszystkim na myśli klientów sklepów, okazuje się jednak, że to zatrudniony personel generuje największe straty dla przedsiębiorstwa. Oczywistym narzędziem mającym zapewnić bezpieczeństwo sklepu jest system monitoringu wizyjnego, ale coraz częściej dozór to niejedyna funkcja kamer. Z pomocą przychodzi nowoczesna technologia. Internet Rzeczy czy algorytmy sztucznej inteligencji to już nie tylko hasła z filmów SF, ale także realne możliwości. Dzięki nim zyskujemy przede wszystkim świadomość sytuacyjną, jesteśmy również w stanie analizować sprzedaż towarów, zachowanie klientów, lepiej nadzorować personel. Wśród funkcjonalności, jakie dają dostępne na rynku systemy, mamy też m.in. możliwość kontrolowania długości kolejek, detekcję szwendania się czy tworzenie mapy ciepła pozwalającej na analizę drogi, po której poruszają się klienci. Nadal bardzo cenioną funkcją jest integracja systemów wizyjnych z terminalami POS, umożliwiająca nakładanie operacji fiskalnych na obraz z kamer. Dzięki temu mamy zapewnioną kontrolę poprawności transakcji czy choćby możliwość zauważenia fałszerstwa związanego ze zwrotem towaru.

Rynek handlu detalicznego stale podnosi swoje wymagania wobec dostawców systemów zabezpieczeń, co wymusza na nich opracowywanie nowych narzędzi. Dlatego z optymizmem i zaciekawieniem czekam na rozwój branży.

Anna Makowska

Hikvision

Bezpieczeństwo w handlu

Dla każdego człowieka niezwykle istotne jest zapewnienie sobie i bliskim bezpieczeństwa. Klienci, jako prawdopodobni posiadacze środków finansowych, są pożądani nie tylko przez sprzedających towary i usługi. Stanowią także potencjalne cele dla przestępców. Patrząc tylko na galerie handlowe, codziennie odwiedza je tysiące osób. Zabezpieczenie tak dużych i różnorodnych obiektów wymaga uwzględnienia wielu rodzajów zagrożeń. Stawia to ochronę takiego obiektu przed szeregiem wyzwań, problemów, nieprzewidzianych sytuacji wymagających natychmiastowej reakcji. Przede wszystkim wyzwanie stanowi ogromne natężenie ruchu oraz dostępność tej przestrzeni dla każdego. Co więcej, ma na to także wpływ położenie – często w centrum miasta, np. w bezpośrednim sąsiedztwie dworców. Rynek zabezpieczenia centrów handlowych stale rośnie, a jego potencjał widać w liczbach – w samym 2018 r. w Polsce otwarto 12 nowych centrów handlowych, 8 parków handlowych oraz 1 centrum wyprzedażowe. Doskonale wyposażone centrum bezpieczeństwa będzie stanowiło podstawę do sprawnego działania całego systemu. Monitoring obiektu to kilka obszarów wymagających nieco innego podejścia sprzętowego. Monitoring wejścia – są to miejsca, gdzie przewija się najwięcej osób, z tego względu wymagają możliwości dokładnego rejestrowania twarzy. Monitoring przestrzeni zakupowej – tutaj idealnie sprawdza się rozwiązanie panoramiczne. W obszarze magazynów – zabezpieczenie towaru to ochrona przed złodziejami, czy też nieuczciwymi praktykami pracowników. Monitoring przestrzeni parkingowej może być wyzwaniem głównie ze względu na słabe oświetlenie. Co więcej, warto przyjrzeć się poprawie wydajności systemu POS, by unikać strat. Coraz powszechniejsze staje się zastosowanie najnowszych technologii – sztucznej inteligencji – rozpoznawanie twarzy, zliczanie osób, czy wykrywanie kolejek znacząco wpływa na bezpieczeństwo oraz poprawę efektywności biznesu.

Jakub Sobek

Linc Polska

Technologia i szkolenia

Jeszcze kilka lat temu do zagadnienia bezpieczeństwa w tzw. branży retail podchodzono w dość prosty i schematyczny sposób. Skoro sklep jest okradany, trzeba zamontować w nim kamery – gdy już będą, to problem zniknie, a przynajmniej w bardzo znacznym stopniu zostanie ograniczony. Tymczasem każdego dnia policja przekazuje komunikaty, w których publikowane są twarze sprawców kradzieży w sklepach. Dowodzi to, że taki sposób myślenia nie do końca jest słuszny. Widok kamer nie odstrasza sprawców.

Na przestrzeni lat można jednak zaobserwować znaczący wzrost świadomości wśród osób zarządzających bezpieczeństwem w sklepach lub galeriach handlowych. Zmienia się dzięki temu podejście do wykorzystania kamer. Nadal są sklepy, w których pracownik ochrony przez cały czas obserwuje obraz z kamer. Skuteczność takiego rozwiązania oraz rosnące koszty pracy sprawiają jednak, że coraz częściej rezygnuje się z takiego sposobu monitorowania obiektów. Obecnie w wielu przypadkach kamery służą jedynie do dokumentowania zajść, a zgromadzony materiał jest pomocny na wypadek roszczeń którejkolwiek ze stron. Okazuje się, że kamery dają znacznie więcej możliwości. Wsparte algorytmami analizy wizyjnej działającymi lokalnie lub w chmurze pozwalają na automatyczną detekcję niepożądanych zdarzeń, np. zbyt długie kolejki przy kasach, detekcję pozostawionego bagażu, upadek osoby lub zbyt długie przebywanie w monitorowanej strefie. Coraz częściej wdrażane są także rozwiązania umożliwiające zliczanie klientów i monitorowanie ich aktywności w poszczególnych obszarach sklepu, a nawet sprawdzanie poziomu ich zainteresowania poszczególnymi produktami.

Kolejnym ważnym aspektem, który wpływa na podniesienie bezpieczeństwa w obiekcie handlowym, jest prawidłowe przeszkolenie pracowników. Skoro pracowników ochrony fizycznej jest coraz mniej lub nie ma ich wcale, część działań prewencyjnych muszą przejąć pracownicy sklepu. Szkolenia i treningi pozwalają rozpoznać typowe zachowania osób planujących np. kradzież. Takie szybkie typowanie może zapobiec przestępstwu. Szkolenia mogą także przyczynić się do podejmowania słusznych decyzji oraz szybkich reakcji, np. w przypadku agresji ze strony klientów. Wiedza zdobyta podczas szkolenia może być wykorzystana do łagodzenia powstających konfliktów. Wszystkie te elementy wpływają na poprawę bezpieczeństwa. Także w Polsce trwają już pierwsze testy sklepów w 100% samoobsługowych. Wszystkie wdrażane technologie w takich obiektach mają minimalizować ryzyko strat. Stosuje się m.in. technologie wizyjne, metki RFID oraz bramki antykradzieżowe. Odpowiednie połączenie tych elementów może być bardzo skutecznym rozwiązaniem mimo całkowitej rezygnacji z zatrudnienia pracowników w sklepie. Czy tak się właśnie stanie i czy rzeczywiście uda się wyeliminować straty lub zminimalizować je do akceptowalnego poziomu, pokażą już w najbliższych miesiącach pierwsze wdrożenia i zdobyte na ich podstawie doświadczenia i wnioski.

Krzysztof Kunecki

Schrack Sconet

Zapewnienie bezpieczeństwa pożarowego w obiektach handlowych

Dla zapewniania optymalnej ochrony przeciwpożarowej w obiektach handlowych należy zastosować urządzenia przeciwpożarowe, które charakteryzują się najwyższą niezawodnością działania oraz bardzo dużą elastycznością pozwalającą na ich dostosowanie do wymagań obiektu i realizację wszystkich założeń scenariusza pożarowego.

W przypadku wystąpienia pożaru w takim obiekcie, jak np. galera handlowa, uruchamiane są setki, a nawet tysiące urządzeń wykonawczych odpowiedzialnych przede wszystkim za wydzielenie strefy objętej pożarem w celu uniemożliwienia jego przedostania do bezpiecznych części obiektu oraz urządzeń zapewniających bezpieczną ewakuację osób z obiektu. Szczególnie zapewnienie bezpiecznej ewakuacji jest tu dużym wyzwaniem, ponieważ przebywają tu głównie osoby, które nie są jego stałymi użytkownikami. Nieznajomość układu obiektu utrudnia szybką ewakuację.

Dla podwyższenia poziomu bezpieczeństwa pożarowego coraz częściej stosuje się dedykowany system integrujący urządzenia przeciwpożarowe (SIUP). Zapewnia on kompleksowy nadzór, sterowanie i zarządzanie wszystkimi urządzeniami mającymi wpływ na bezpieczeństwo pożarowe. Dzięki przyjaznemu graficznemu interfejsowi użytkownika system pozwala na szybką ocenę sytuacji i wsparcie operatora poprzez wyświetlenie instrukcji postępowania. Instrukcje są przygotowywane na podstawie instrukcji bezpieczeństwa pożarowego obiektu i zawierają wytyczne postępowania pozwalające na sprawne i szybkie działanie personelu technicznego, co jest szczególnie ważne w sytuacjach stresowych.

Dla poprawy oceny zagrożenia istnieje możliwość integracji z innymi systemami bezpieczeństwa, takimi jak np. system dozoru wizyjnego (VSS) czy kontroli dostępu. Dzięki temu operator w momencie wykrycia pożaru, mając do dyspozycji obraz z kamery z zagrożonego miejsca, ma jeszcze lepszy przegląd sytuacji. Pozwala to na szybszą weryfikację zdarzenia, a kierujący akcją ratowniczo-gaśniczą może obserwować proces ewakuacji i aktywnie reagować na jego przebieg z wykorzystaniem zintegrowanych systemów, takich jak DSO.

System integrujący jest jedynym certyfikowanym urządzeniem uprawnionym do zarządzania ewakuacją, co pozwala na jego wykorzystanie również przy innych zdarzeniach kryzysowych w obiekcie i stanowi istotne wsparcie dla użytkownika/zarządcy obiektu oraz kierującego akcją ratowniczo-gaśniczą.

Mirosław Lukowski

krajowy senior menedżer, Dział Prewencji Ryzyka i Ochrony Carrefour

Najważniejsza jest prewencja wsparta technologią

Branża handlu detalicznego od kilku lat ewoluuje w stronę zautomatyzowanych procesów obsługi ułatwiających przepływ klientów i ich obsługę. Każdy taki proces jest związany z wdrożeniem nowych technologii i inwestycjami. Trudno nie zauważyć, iż wszystkie te procesy są ukierunkowane na działalność biznesową, natomiast marginalizuje się ofertę branży security. Uważam, że największym wyzwaniem dla całej branży retail jest przekonanie decydentów, iż ten proces powinien być równoległy, gdyż nowe technologie dają również nowe możliwości działania różnym grupom przestępczym, a przeciwdziałanie im wymaga zaawansowania technologicznego. Bazowanie jedynie na pracownikach ochrony powoduje, że może dojść do otwarcia nie tylko „furtek" umożliwiających działania na szkodę sieci handlowych, ale można zaryzykować twierdzenie, że nawet „bram". Przykładem są wszelkiego rodzaju kasy samoobsługowe, które kuszą mnogością możliwości, a jak wiadomo tylko wyobraźnia ogranicza człowieka.

W tym właśnie miejscu rynek retail i branża zabezpieczeń muszą się spotkać i wspólnie wypracować właściwe metody przeciwdziałania przypadkom, które już mają miejsce, oraz wszystkim nowym, które mogą zdarzyć się jutro. Mamy jako branża świadomość, że 100-procentowe zabezpieczenie nie istnieje i wykluczenie działań na szkodę sieci handlowych, zarówno zewnętrznych, jak i tych wewnętrznych, nie jest możliwe. Ale działając razem, mając uczciwe, rzetelne wsparcie ze strony branży zabezpieczeń, ukierunkowując wspólne wysiłki, utrudniamy działania grupom czerpiącym korzyści z luk w systemach zabezpieczeń. Tu każdy krok w stronę technologii uczenia maszynowego i analizy wizyjnej to krok we właściwym kierunku.

Pomijając aspekt handlowy, wszystkie wspólne działania na rzecz bezpieczeństwa klientów, rozwijanie systemów zarówno przeciwwłamaniowych, jak i telewizji dozorowej, dodawanie funkcji analizy obrazu i sztucznej inteligencji, a przede wszystkim podstawy, jaką jest integracja tych systemów, to są sekundy, które w przypadkach zagrożenia życia i zdrowia nie mają ceny. Każdy z nas w sytuacjach kryzysowych reaguje inaczej. Przy dużej rotacji personelu na jakże trudnym rynku pracy opieranie bezpieczeństwa tylko na czynniku ludzkim, bez profesjonalnego wsparcia ze strony technologii, to przejaw głębokiej wiary w to, że takie przypadki zdarzają się gdzie indziej, nie u nas.

Uważam, że największym wyzwaniem jest uświadomienie osobom decyzyjnym, iż tylko prewencja poparta zaawansowaną technologią oraz partnerstwo branży retail i specjalistów dostarczających rozwiązania ochronne pozwolą w sposób właściwy zoptymalizować koszty takiego procesu.

Krzysztof Moszyński

Seris Konsalnet Holding

Główne zadanie – spełnić oczekiwania klienta

Jakie – z perspektywy firmy ochrony – jest obecnie największe wyzwanie dotyczące zapewnienia bezpieczeństwa w obiektach handlowych? Z mojej zawodowej perspektywy wskazałbym dwa. Po pierwsze – klient i jego oczekiwania, po drugie – pracownicy ochrony. Dlaczego klient? Normą od kilku lat stały się w placówkach handlowych radykalnie wprowadzane oszczędności, w efekcie prowadzące do redukcji liczby posterunków (przy niezmienionych zakresach obowiązków, odpowiedzialności i wysokości kar umownych), oczekiwania związane z tzw. efektem WOW (wizerunek i wrażenie przede wszystkim), dociążanie pracowników ochrony zadaniami niemającymi nic (lub niewiele) wspólnego z zakresem twardego security (m.in. zastępowanie pracowników punktów info oraz recepcji, odprowadzanie wózków i koszyków, odbieranie przesyłek kurierskich, obowiązki administracyjne itp.).

Personel ochrony w coraz mniejszym stopniu zajmuje się usługami ochrony, stając się stopniowo działem obsługi obiektu i klienta (w tym również klienta swojego usługodawcy). I oczywiście wszystko jest możliwe do zrealizowania, ale wymaga odpowiedniego doboru pracowników, ich dobrego przeszkolenia i zmotywowania, a także zintegrowania systemów zabezpieczeń i wprowadzenia automatyzacji tych procesów klienta, które są powtarzalne, weryfikowalne i nie mają de facto wpływu na bezpieczeństwo. To z kolei generuje kolejne koszty, których obiekty handlowe (uogólniając) nie chcą w znacznej większości ponosić.

A dlaczego pracownicy ochrony? Odpowiedź jest prosta. Nasze państwo dorosło już do tego punktu w rozwoju, że oferuje swoim obywatelom coraz większe możliwości zarobkowe i dochodowe. Dziś wszystkie zawody niskopłatne (usługi ochrony, sprzątania itp.) zaczynają borykać się z dramatycznym niedoborem pracowników, zwłaszcza gdy wymaga się od tych pracowników coraz więcej, nie oferując im ani ścieżki rozwojowej, ani stabilizacji (w rozumieniu możliwości godnego utrzymania z „kodeksowych" godzin pracy), nie inwestuje się w nich i nie motywuje. Jedyne, co słyszą od swoich przełożonych, to: pracuj szybciej, lepiej, dokładniej częściej, uważniej! W takiej sytuacji rynkowej największym wyzwaniem dla firmy ochrony jest zapewnienie właściwej usługi o wysokiej jakości, przy dopuszczalnym poziomie kosztów własnych (czyli przy akceptowalnej marży) i minimalnej rotacji pracowników. Czyli de facto wyzwaniem jest spełnienie wszystkich oczekiwań klienta, ale w zaakceptowanej przez tego klienta cenie. I nie da się ukryć, że w efekcie tych dwóch wybranych, najważniejszych, choć nie jedynych składowych, za obecnie funkcjonujące na rynku ochrony wynagrodzenia nie można dostarczyć klientowi szeroko rozumianego bezpieczeństwa, a jedynie jego namiastkę. Namiastkę adekwatną do budżetu, jaki obecnie obiekt handlowy na to przeznacza.

Krzysztof Bartuszek

prezes Zarządu Securitas Polska

Bezpieczeństwo obiektów handlowych

Bezpieczeństwo obiektów handlowych jest procesem wielopłaszczyznowym, determinowanym przez różnorodność zagrożeń w miejscach użyteczności publicznej. Duże obiekty handlowe to restauracje, kina, miejsca rekreacji, place zabaw dla dzieci, a więc również miejsca spotkań towarzyskich. Bezpieczeństwo tego typu obiektów to szeroko rozumiany, dwutorowy proces skierowany w stronę najemców oraz klientów. Mimo że finalnie sprowadza się on do wspólnego mianownika, to rozwiązania i technologie rekomendowane przez branżę security mogą być różne.

Często zaniedbywanym, ale najważniejszym aspektem bezpieczeństwa są procedury ewakuacyjne i antyterrorystyczne. W dużym centrum handlowym w godzinach szczytu przebywa nawet kilkanaście tysięcy osób i setki samochodów. Sprawne przeprowadzenie ewakuacji takiej grupy to wyzwanie, któremu niełatwo sprostać. Tylko nieliczni najemcy decydują się na przeprowadzenie próbnej ewakuacji, a przecież procedury, współpraca wszystkich służb, zapewnienie sprawnej komunikacji i koordynacji czy umiejętność działania pracowników ochrony w dużym stresie muszą być dopracowane do perfekcji – a więc wielokrotnie przećwiczone. Panika i dezorientacja tak dużej grupy ludzi, brak odpowiednich systemów, które w chwili krytycznego zagrożenia zapewniłyby dobrą słyszalność komunikatów, brak lub złe rozmieszczenie oznaczeń i oświetlenia drogi ewakuacji mogą mieć tragiczne skutki. Kluczem są i będą szkolenia, próby, testy i treningi. Pomocne może być zastosowanie technologii, w tym systemów zliczania osób przebywających w obiekcie. W trakcie ewakuacji centrum handlowego człowiek nie będzie w stanie policzyć osób opuszczających obiekt – w takim momencie systemy spełnią swoją rolę i dadzą odpowiedź na pytanie, czy ktoś jeszcze pozostał w obiekcie, i jakie dalsze kroki należy podjąć podczas ewakuacji.

Panika tłumu niekoniecznie musi wiązać się z przeprowadzaną ewakuacją. Czynnikiem inicjującym może być szum komunikacyjny lub błędny przekaz informacji. Pamiętam, jak w jednej z galerii handlowych panikę wywołał klient, który zauważył pszczołę i zareagował histerycznym krzykiem.

Ochrona dużego obiektu handlowego nie może koncentrować się wyłącznie na ewakuacji obiektu jako takiego. Prewencyjne szkolenia poszczególnych najemców, budowanie ich świadomości w zakresie zagrożeń pożarowych powinny być stałą praktyką – lepiej zapobiegać, niż leczyć, a w tym przypadku świadomość pracowników i najemców może być kluczem do sukcesu. Natomiast ich brak świadomości i wiedzy na temat ryzyka jest najczęściej powodem zainicjowania sytuacji wymagających interwencji służb ratowniczych.

Obiekty handlowe to duże skupiska ludzi, a to wiąże się z takimi sytuacjami, jak wypadki, zasłabnięcia, a nawet porody. Bardzo cenna okazuje się w takich sytuacjach fachowa wiedza pracowników ochrony z zakresu ratownictwa medycznego, pierwszej pomocy przedmedycznej, obsługi defibrylatora. A zatem znowu – szkolenia, szkolenia, szkolenia i właściwy dobór pracowników.

Ostra rywalizacja handlowa, ale i sytuacja na rynku pracy sprzyjają poszukiwaniu optymalizacji kosztowych. Jedną z dróg jest przenoszenie sprzedaży do Internetu. Na poziomie fizycznych sklepów to m.in. samoobsługowe punkty kasowe, a docelowo w pełni samoobsługowe sklepy. Tutaj rola ochrony i systemów zabezpieczeń jest szczególnie istotna. Chcemy, aby każdy klient czuł się jak najbardziej swobodnie, mamy jednak świadomość, że dla niektórych swoboda i dostępność towarów nie idzie w parze z uczciwością. Pracownicy ochrony już teraz nadzorują bezobsługowe punkty kasowe, obserwując transakcje poprzez zintegrowane systemy elektronicznego paragonu połączone z kamerami. Być może w przyszłości będą to inteligentne systemy automatycznie weryfikujące zakupy poprzez sczytywanie w technologii RFID. Z ekonomicznego punktu widzenia ta technologia jest jeszcze za droga i wymaga zaangażowania już na etapie produkcji towarów, ale powinna zapewne tanieć i jej zastosowanie jest tylko kwestią czasu. Testy trwają i z punktu widzenia jakości zastosowanych rozwiązań zdają się potwierdzać słuszność tego kierunku. Jaka będzie wówczas rola ochrony? Otóż cały czas może istnieć konieczność podej-

mowania interwencji wobec nieuczciwego klienta. Można sobie wprawdzie wyobrazić zautomatyzowany sklep, który nie wypuści klienta, gdy ten nie ureguluje rachunku, ale byłoby to chyba zbyt nieludzkie.
Skoro jesteśmy przy interwencji i zadaniach pracowników ochrony, warto wspomnieć o wyzwaniu, przed jakim od lat staje branża ochrony, czyli właściwym doborze personelu. Pracownik ochrony, który ma podejmować działania wobec klientów, musi być miły, kulturalny i przeszkolony. O ile to ostatnie można (przynajmniej w teorii) zapewnić, o tyle pozostałe elementy to cechy, które wymagają selekcji kandydatów i ich profilowania. Pracownik ochrony może być w przyszłości jedyną osobą kontaktową dla klienta. Niektóre sieci handlowe już dzisiaj oczekują od nich podstawowej znajomości asortymentu produktów czy układu ekspozycji towarów, tak aby mogli się stać częścią systemu obsługi klienta. Wprowadza się zautomatyzowane punkty obsługi, a informacje o produkcie udostępnia elektroniczny stand reklamowy lub wręcz robot poruszający się w sklepie. Taki robot z zainstalowanymi kamerami i detektorami (np. wykrycia dymu) może stanowić wsparcie systemu bezpieczeństwa, będąc jednocześnie ciekawym elementem oddziaływającym marketingowo. Co prawda nie obcujemy jeszcze na co dzień z robotami, ale być może w przyszłości to one będą właśnie przyciągać klientów.

Adam Suliga

ekspert Polskiej Izby Handlu

Potrzebne są zmiany w polskim prawie

Rozważania dotyczące zapewnienia bezpieczeństwa w obiektach handlowych tak naprawdę będą bez znaczenia, dopóki nie dojdzie do istotnych zmian w polskim prawie. Digitalizacja, nowoczesne rozwiązania dotyczące monitoringu wizyjnego, sztuczna inteligencja, uczenie maszynowe, świetnie wyszkoleni security menedżerowie – nic nie poprawi sytuacji bez jasnych przepisów, które pozwoliłyby szybko i skutecznie ograniczać wciąż rosnącą skalę kradzieży sklepowych. Spójrzmy chociażby na nowelizację kodeksu karnego, która ma polegać na dodaniu do art. 115 § 9a (kradzież szczególnie zuchwała). Czy zaproponowana zmiana spowoduje, że kradzież w sklepie „mniejszych" kwot lub towarów o niskiej wartości nie będzie wykroczeniem? Czy zostanie uznana za kradzież szczególnie zuchwałą zagrożoną pozbawieniem wolności? A może po prostu będzie to kolejny martwy zapis, bo sędziowie będą mieli problemy z interpretacją? Obserwując działania polskiego wymiaru sprawiedliwości, można mieć pewność, że wynikną problemy z interpretacją tak skonstruowanego przepisu i będzie tak do chwili, aż kradzież zostanie uznana za przestępstwo niezależnie od wartości skradzionego mienia i dojdzie do wykreślenia art. 119 z kodeksu wykroczeń. W tym kontekście warto zwrócić uwagę na autorski projekt Polskiej Izby Handlu Ogólnopolski rejestr wykroczeń, który był już omawiany w 2013 r., tuż po wejściu w życie ustawy z 27 września 2013 r. Tak naprawdę to jedyne skuteczne narzędzie w walce z patologią, jaką są drobne kradzieże sklepowe. Co prawda rząd przyjął zmiany w kodeksie wykroczeń i jest tam też informacja, że zostanie utworzony rejestr sprawców wykroczeń (http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180002077 – art. 2 i art. 4 pkt 1 lit. b), ale termin jego utworzenia ustawodawca wyznaczył na 1 listopada 2019 r. Do tego czasu mają trwać prace nad ostatecznym kształtem rejestru. Jak będzie wyglądał, kto będzie nim zarządzał i na jakich zasadach, tego jeszcze nie wie nikt, a już na pewno nie osoby, które będą z niego korzystały.
Inny przykład – zmiana wysokości progu rozróżniającego wykroczenie od przestępstwa z 1/4 najniższego wynagrodzenia do stałego poziomu 500 zł. Czyżby kradzież w Polsce nie była problemem zasługującym na poważne traktowanie? Czy tak trudno dostrzec destrukcyjny charakter ustawy z 27 września 2013 r.? Kosmetyczne zmiany, jakie proponuje rząd, niczego nie zmienią. Magiczna kwota 500 zł w tym przypadku z pewnością nie „zaczaruje" rzeczywistości. Złodzieje sklepowi nadal będą kradli towary, dbając o to, by nie przekroczyć ustalonego progu. Ujęcie sprawcy kradzieży w sklepie samoobsługowym jest bardzo trudne. Gdy już do niego dojdzie, złodziej karany jest tylko za czyn, który mu udowodniono. W przypadku wykroczenia nie ponosi zbyt uciążliwych konsekwencji. Dlaczego nie można skończyć z fikcją i nazwać rzeczy po imieniu: kradzież to kradzież, bez względu na wartość skradzionego mienia. Zawsze powinna być traktowana jako przestępstwo.
Mam więcej pytań. Co np. z postulowanymi od kilku lat nowelizacjami ustaw o policji oraz o ochronie osób i mienia idącymi w takim kierunku, aby obie te formacje mogły ze sobą współpracować, zamiast wzajemnie sobie przeszkadzać? Gdzie podział się Program „Razem Bezpieczniej", który w wielu regionach Polski odnosił spektakularne sukcesy jeszcze do roku 2014, a potem nagle został zapomniany – głównie ze względu na brak sygnału ze strony MSWiA oraz KGP do jego kontynuacji? Kiedy wreszcie doczekamy się poważnego potraktowania zawodu pracownik ochrony i wymogu, by osoby zajmujące się tą profesją posiadały odpowiednie kwalifikacje, kompetencje, a nawet decyzyjność na wzór krajów Europy Zachodniej, aby móc zapewnić społeczeństwu realne, a nie fikcyjne poczucie bezpieczeństwa?
To są prawdziwe problemy, którymi należy się zająć. Reszta to tylko wydumane opowieści o utopijnym świecie, w którym roboty będą strzegły naszego bezpieczeństwa, a cyfrowa rzeczywistość będzie wolna od aktów agresji, kradzieży i innych niepożądanych zachowań, z którymi mimo istnienia dostępnych rozwiązań technologicznych nie potrafimy sobie poradzić.

Ewelina Zalewska

Loss Prevention
kierownik sekcji analitycznej
Super-Pharm Holding Sp. z o.o.

Najważniejszy jest dobrze wyszkolony zespół pracowników

Głównym wyzwaniem, przed którym stoimy, chcąc zapewnić bezpieczeństwo w obiektach handlu detalicznego, jest odpowiednio wyszkolony i zmotywowany zespół pracowników. Naszym zadaniem, jako Działu Loss Prevention, jest tworzenie w placówkach handlowych kultury zapobiegania stratom. Dbamy o to, ciągle szkoląc personel oraz podnosząc jego świadomość w zakresie *loss prevention*. Kluczowe jest, żeby kadra zarządzająca zdawała sobie sprawę z potencjalnych zagrożeń oraz umiała w odpowiedni sposób reagować, gdyby takowe się pojawiły. Takie podejście sprawia, że również szeregowi pracownicy podnoszą swoje umiejętności w zakresie zapobiegania stratom. Odpowiednio dopracowane procedury mają pomóc w zapobieganiu stratom i wymuszają na personelu w sklepie poprawne działania.
Wszystkie te elementy w połączeniu ze wsparciem ze strony Działu Loss Prevention sprawiają, że jesteśmy w stanie utrzymać straty na niskim poziomie. Dodatkowym wsparciem są odpowiedniej jakości urządzenia, które pomagają we właściwy sposób zabezpieczyć wszystkie zagrożone obszary w sklepie: salę sprzedaży, zaplecze i strefę kasową. Na pewno w najbliższym czasie duży nacisk będzie kładziony na możliwości analityczne kamer, co sprawi, że będziemy mogli szybciej i w dokładniejszy sposób wyłapywać nieprawidłowości i szybciej reagować na pojawiające się zagrożenia.

Andrzej Jankowski

ekspert

Sztuczna inteligencja w rozwiązaniach wideo

Technologie informatyczne rozwijają się bardzo szybko i równie szybko potrafią wywrócić do góry nogami mocno zakorzenione modele biznesowe. Dwa znane wszystkim przykłady to Uber, zmieniający rynek taksówek oraz AirBnB – start-up oferujący apartamenty do wynajęcia na całym świecie.
Uber dysponuje w tej chwili największą na świecie flotą „taksówek", a AirBnB jest największą siecią „hotelową". Obydwie firmy nie powstałyby, gdyby nie nowe technologie. Z dzisiejszej perspektywy ich sukces wydaje się oczywisty, ale kilka lat temu taki nie był. W obu przypadkach tradycyjne firmy nie były przygotowane na taką konkurencję.

Sztuczna inteligencja przyniesie zmiany na dużo większą skalę niż telefonia komórkowa czy nawet Internet. Pisze się o tym, że wpływ sztucznej inteligencji na nasze życie będzie taki, jak elektryczności. Z definicji sztuczna inteligencja to system, który jest w stanie wykonywać zadania wymagające ludzkich zdolności poznawczych. Jednym z takich zadań jest analiza obrazu. Od kiedy w 2012 roku system oparty na sieci neuronowej okazał się najlepszy w kontekście rozpoznawania obiektów na zdjęciach, prace nad tego typu rozwiązaniami znacząco przyspieszyły i w tej chwili komputery są już lepsze od człowieka w wielu zadaniach związanych z analizą wideo.
Monitoring wizyjny dzięki sztucznej inteligencji zmienia się bardzo szybko. Systemy SI są w stanie monitorować dowolną liczbę kamer w czasie rzeczywistym, nie męcząc się i zawsze z taką samą skutecznością. Bardzo łatwo jest skalować system, jeśli jest taka potrzeba. Co bardzo ważne, system jest w stanie się uczyć i cały czas poprawiać swoje działanie.
Dodatkowym atutem takich systemów jest możliwość wzbogacenia ich o możliwości analityczne, np. analiza zachowań konsumenckich w sieci handlowej, automatyczne rejestrowanie wejść i wyjść, rejestracja niebezpiecznych zdarzeń.
Klienci doceniają również fakt, że tego typu wdrożenia są nieskomplikowane. W wielu wypadkach wystarczy wpiąć kamery w istniejącą sieć komputerową. Dla firm świadczących usługi monitoringu sztuczna inteligencja jest idealnym pracownikiem. Zawsze zdrowa, zawsze na czas i potrafi również dostarczyć dodatkowego dochodu dzięki analizie danych.

Bezpieczeństwo pożarowe w galeriach handlowych

TEKST
Renata Trojanowska

Temat bezpieczeństwa w galeriach handlowych pojawia się w wielu jego aspektach, od spełnienia wymagań prawnych, poprzez zabezpieczenia techniczne, po bezpieczeństwo pożarowe. I to ostatnie jest najważniejsze, bo cóż po zabezpieczeniach przed kradzieżą, kiedy pożar strawi dorobek życia wraz z tym zabezpieczeniem?

W

Według raportu CBRE i Trei Real Estate Poland powierzchnia centrów handlowych w Polsce wynosiła 1,52 mln m² (dane na koniec I kwartału 2019 r.); szacuje się, że do końca roku może przybyć kolejne 170 tys. metrów kwadratowych. Wydawać by się mogło, że nasz rynek już się nasycił, jednak raport wykazał, iż parki handlowe rozwijają się w coraz szybszym tempie, stanowiąc kolejny krok w ewolucji formatów handlowych, z dużym potencjałem dynamicznego rozwoju.

Jeszcze nie tak dawno zakupy można było robić każdego dnia tygodnia. Ci, którzy dokonywali zakupów w niedziele, rezerwują na to czas w innym dniu tygodnia. Z punktu widzenia bezpieczeństwa w dni handlowe w obiekcie przebywa jednocześnie jeszcze więcej osób. Zakupowe godziny szczytu przypadają między 16.00 a 18.30, kiedy to klienci kończą pracę. Wyjątkiem jest czas wyprzedaży rządzący się swoimi prawami i można odnieść wrażenie, że tłumy są non stop.

W budynkach użyteczności publicznej szczególnie należy zadbać o ich bezpieczeństwo, głównie pożarowe. O ile w małych centrach handlowych sprawa nie jest zbyt skomplikowana, o tyle w wielkopowierzchniowych galeriach handlowych już tak. Może w nich przebywać jednocześnie nawet kilka tysięcy osób zwabionych różnorodnością usług dostępnych w jednym miejscu. Przy dużym zagęszczeniu ludzi trzeba się liczyć z mnóstwem potencjalnych zagrożeń, z których najgorsze skutki ma pożar – dla ludzi, ale i dla mienia.

O bezpieczeństwie pożarowym myśli się perspektywicznie już na etapie projektowania budynku, określając odpowiednie materiały, z których ma być wykonany, warunki ochrony przeciwpożarowej oraz system sygnalizacji pożarowej i instalacje ppoż. Mówią o tym ustawy i rozporządzenia dotyczące ochrony ppoż. i bezpieczeństwa pożarowego [1], [2], [3], [4]. Następnie na etapie wykonywania inwestycji powstaje scenariusz pożarowy, zawierający opis występujących po sobie możliwych zdarzeń w trakcie ewentualnego pożaru, funkcjonowania urządzeń ppoż. i ich współdziałania w momencie wybuchu pożaru. Z punktu widzenia bezpieczeństwa pożarowego to jeden z dwóch najważniejszych dokumentów. Drugim jest „Instrukcja bezpieczeństwa pożarowego" (IBP), będąca kompendium wiedzy na temat ochrony ppoż. danego budynku, zawierająca m.in. plany ewakuacyjne. Tylko właściwe zaprogramowanie wszystkich urządzeń ppoż. (co w którym momencie się załączy, co otworzy, co zamknie) oraz odpowiednie działania osób są w stanie uchronić budynek i przebywających w nim ludzi przed katastrofą.

Zadbanie o bezpieczeństwo pożarowe obiektu spoczywa na jego właścicielu. To on musi dostosować budynek centrum handlowego do wymagań technicznych, wyposażyć w sprzęt gaśniczy, oznaczyć drogi ewakuacyjne oraz zapewnić warunki do przeprowadzenia sprawnej i bezpiecznej ewakuacji. Zaniedbania skutkują nałożeniem kar, a nawet niedopuszczeniem budynku do użytku.

Od momentu otwarcia obiektu odpowiedzialność za bezpieczeństwo pożarowe i ewakuację ludzi spoczywa zwykle na przeszkolonych pracownikach ochrony (co powinno być zapisane w IBP). To oni najlepiej znają zakamarki chronionego obiektu, procedury na wypadek wystąpienia zagrożeń i potrafią powstrzymać spotęgowanie zagrożenia oraz uniknąć paniki, a przede wszystkim pomóc sprawnie przeprowadzić ewakuację. Te dwa ostatnie czynniki zbierają największe żniwo. Pożar z reguły wybucha niespodziewanie, a pierwszym odruchem człowieka jest brak jakiejkolwiek reakcji. W momencie, kiedy zagrożenie jest zbyt blisko, niewiele już można zrobić. Pojawia się strach, ludzie w panice próbują uciekać.

Ścisk, tłok, przypadkowe osoby nieznające obiektu to w momencie wybuchu pożaru idealne warunki prowadzące do tragedii.

I w tym momencie powinny wkroczyć osoby wyznaczone do koordynacji ewakuacji. Osoby za nią odpowiedzialne powinny być zdecydowane, energiczne i budzić autorytet, bo to od nich zależy przeprowadzenie sprawnej ewakuacji. Przypadkowi klienci kierują się w stronę wyjścia, które znają, natomiast w sytuacji zagrożenia powinni korzystać z wyjść ewakuacyjnych, na co dzień nieużywanych. Warto wiedzieć, gdzie one są.

Wymagania prawne

W ochronie ppoż. istnieje kilka pojęć, które definiują wymagania, jakim muszą sprostać budynki. Jednym z nich jest kategoria zagrożenia ludzi ZL. Galerie handlowe mogą się składać z kilku, a nawet kilkunastu stref pożarowych, a każda z nich może być zaliczona do jednej lub kilku kategorii zagrożenia ludzi [2]. Zwykle są to kategorie ZL I i ZL III. Dopuszczalna powierzchnia strefy pożarowej w galerii handlowej jednokondygnacyjnej wynosi 10 tys. m², natomiast w wielokondygnacyjnej zależy od wysokości budynku. I tak w budynku niskim (wysokość do 12 m włącznie) maks. strefa pożarowa wynosi 8 tys. m², w budynku średniowysokim (od 12 do 25 m włącznie) 5 tys. m². Wysokość mierzona jest nad poziomem terenu i nie wlicza się do niej kondygnacji podziemnych.

Dopuszczalne strefy pożarowe mogą zostać powiększone, gdy w obiekcie zostaną zastosowane:

- stałe urządzenia gaśnicze tryskaczowe,
- samoczynne urządzenia oddymiające uruchamiane za pomocą systemu wykrywania dymu.

Zastosowanie obu tych systemów pozwala powiększyć strefę o 200% i jest łakomym kąskiem dla inwestorów. Powierzchnia handlowo-usługowa jednej z warszawskich galerii wynosi 76 tys. m² i jest to budynek średnio wysoki. Gdyby inwestor nie skorzystał z możliwości powiększenia dopuszczalnej powierzchni strefy pożarowej, musiałby zamiast 8 stref pożarowych stworzyć 16, co wiąże się z kosztami wydzielenia tych stref. Elementy wydzielenia pożarowego zależą od klasy odporności pożarowej budynku – im jest wyższa, tym wymogi dla tych elementów są bardziej restrykcyjne, a koszty większe.

Historia niestety zna przypadki pożarów w galerii handlowych. W marcu ub.r. doszło do tragicznego pożaru w Kemerowie na Syberii. Wstępnie jako przyczynę podawano usterkę instalacji elektrycznej, podejrzewano również podpalenie w sali zabaw, gdzie znaleziono ognisko pożaru. Ogień błyskawicznie ogarnął cały trzypiętrowy budynek. Okazało się, że nie zadziałały systemy ppoż., niektórzy klienci zostali odcięci od wyjść ewakuacyjnych, zapanował chaos, zginęły aż 64 osoby.

Ewakuacja

Sprawna ewakuacja w sytuacji zagrożenia, jakim jest pożar, to najważniejszy proces. Aby była bezpieczna, muszą być spełnione wymagania techniczne wymienione w rozporządzeniach [2] i [3]. Przeprowadzenie ewakuacji w centrum handlowym jest priorytetem ze względu na liczbę osób tam znajdujących się, głównie przypadkowych klientów korzystających z oferty handlowo-usługowej obiektu. Im jest ich więcej, tym większa odpowiedzialność za ich bezpieczeństwo. Akcję ewakuacji podejmuje się w momencie, gdy zaistniałe zdarzenie stwarza realne zagrożenie dla ludzi. Bezpieczeństwo przeprowadzanej akcji jest zawsze zdeterminowane czasem, jaki upłynie od uświadomienia sobie faktu zagrożenia do momentu, gdy ucieczka jest już niemożliwa na skutek działania czynników pożarowych.

Do ewakuacji osób służą korytarze i klatki schodowe, z których bezwzględnie musi być zapewniona możliwość bezpiecznego wyjścia na zewnątrz. Innymi terminami określającymi ewakuację są przejścia i dojścia ewakuacyjne. Wszystkie te elemen-

ty, a właściwie ich wymiary (szerokość, wysokość i długość) mają ogromne znaczenie dla sprawnej ewakuacji.
W galeriach handlowych przestrzeń handlowo-usługowa jest zwykle podzielona na sklepy i butiki wynajmowane poszczególnym najemcom, punkty gastronomiczne zamknięte i otwarte, coraz częściej jest także siłownia i kino z kilkoma lub kilkunastoma salami projekcyjnymi oraz toalety. Na powierzchnię lokali usługowych składają się zwykle 2–3 pomieszczenia – główna przestrzeń handlowa lub usługowa, do której mają dostęp klienci, oraz zaplecze magazynowe lub kuchenne (zależnie od rodzaju prowadzonej działalności). W pomieszczeniach tych od najdalszego miejsca, w którym może przebywać człowiek, do wyjścia na drogę ewakuacyjną, do innej strefy pożarowej lub na zewnątrz budynku powinno być zapewnione przejście ewakuacyjne o odpowiedniej długości. W galeriach handlowych nie powinno ono przekraczać 40 m i przechodzić przez więcej niż trzy pomieszczenia.
Prawo dopuszcza powiększenie długości tych przejść, np. gdy wysokość pomieszczenia przekracza 5 m, można je wydłużyć o 25%, oraz pod warunkiem zastosowania:
- stałych samoczynnych urządzeń gaśniczych wodnych – o 50%,
- samoczynnych urządzeń oddymiających uruchamianych za pomocą systemu wykrywania dymu – o 50%.

Powiększenia podlegają sumowaniu, więc po spełnieniu wszystkich warunków przejścia ewakuacyjne mogą zostać wydłużone nawet o 125%. Natomiast szerokość przejść ewakuacyjnych oblicza się proporcjonalnie do liczby osób, do których ewakuacji ono służy: 0,6 m na 100 osób, ale nie może być mniejsza niż 0,9 m, chyba że służy do ewakuacji mniej niż trzech osób – wtedy 0,8 m. Podobne zasady obliczania szerokości obowiązują przy doborze szerokości drzwi ewakuacyjnych z pomieszczenia.

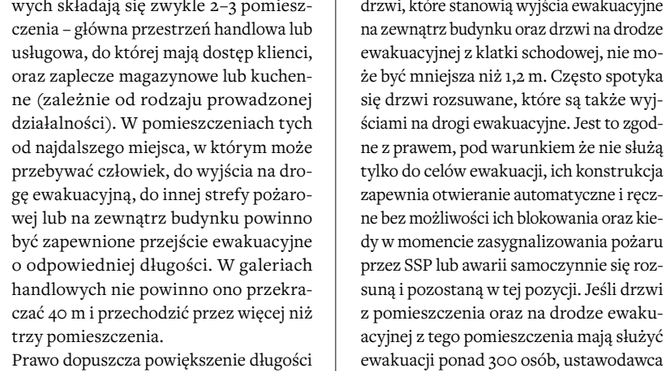
W centrach handlowych są też pomieszczenia, w których z założenia może przebywać więcej niż 50 osób, lub znajdują się w strefie pożarowej ZL, a ich powierzchnia przekracza 300 m² (restauracja, sala kinowa, supermarket). Wtedy należy zapewnić co najmniej dwa wyjścia ewakuacyjne oddalone od siebie o 5 m.
Drzwi będące wyjściami ewakuacyjnymi z pomieszczeń przeznaczonych do jednoczesnego przebywania ponad 50 osób powinny otwierać się na zewnątrz. Szerokość drzwi, które stanowią wyjścia ewakuacyjne na zewnątrz budynku oraz drzwi na drodze ewakuacyjnej z klatki schodowej, nie może być mniejsza niż 1,2 m. Często spotyka się drzwi rozsuwane, które są także wyjściami na drogi ewakuacyjne. Jest to zgodne z prawem, pod warunkiem że nie służą tylko do celów ewakuacji, ich konstrukcja zapewnia otwieranie automatyczne i ręczne bez możliwości ich blokowania oraz kiedy w momencie zasygnalizowania pożaru przez SSP lub awarii samoczynnie się rozsuną i pozostaną w tej pozycji. Jeśli drzwi z pomieszczenia oraz na drodze ewakuacyjnej z tego pomieszczenia mają służyć ewakuacji ponad 300 osób, ustawodawca nakłada obowiązek wyposażenia ich w zamknięcia przeciwpaniczne.
Kolejnym parametrem służącym sprawnej i bezpiecznej ewakuacji jest zapewnienie odpowiedniej szerokości poziomych dróg ewakuacyjnych. Oblicza się ją proporcjonalnie do liczby osób mogących przebywać na danej kondygnacji, zakładając 0,6 m na 100 osób, ale nie mniej niż 1,4 m.
Galeria zaliczona do grupy budynków średnio wysokich powinna być wyposażona w klatki schodowe obudowane i zamykane drzwiami oraz wyposażone w urządzenia zapobiegające zadymieniu lub służące do usuwania dymu. Zabezpiecza się przed zadymieniem również pasaże stanowiące ciągi pieszych, do których przylegają lokale handlowe i usługowe.
Co ważne, ruchomych schodów i pochylni nie zalicza się do dróg ewakuacyjnych, a korzystanie z wind w czasie pożaru jest zabronione! Z wyższych kondygnacji ewakuowanie się na zewnątrz budynku jest możliwe oddymianymi klatkami schodowymi.
W nomenklaturze pożarowej funkcjonuje wspomniane już pojęcie dojścia ewakuacyjnego. Jest to długość drogi ewakuacyjnej od wyjścia z pomieszczenia na tę drogę do wyjścia do innej strefy pożarowej lub na zewnątrz budynku. W *tabeli* zestawiono dopuszczalne długości dojść ewakuacyjnych:

Rodzaj strefy pożarowej	Długość dojścia [m]	
	przy jednym dojściu	przy co najmniej dwóch dojściach
ZL I, II i V	10	40
ZL III	30*	60

* w tym nie więcej niż 20 m na poziomej drodze ewakuacyjnej

Ustawodawca zezwala również na wydłużenie dojść ewakuacyjnych pod warunkiem zastosowania:
- stałych samoczynnych urządzeń gaśniczych wodnych – o 50% długości,
- samoczynnych urządzeń oddymiających uruchamianych za pomocą systemu wykrywania dymu – o 50%.

Powiększenia długości dojść (podobnie jak przejść) również można zsumować.
Zgodnie z rozporządzeniami [2] i [3] na drogach ewakuacyjnych należy zapewnić oświetlenie ewakuacyjne i zapasowe. Oświetlenie ewakuacyjne powinno działać przez co najmniej 2 godziny, natomiast awaryjne co najmniej 1 godzinę po zaniku oświetlenia podstawowego.
Właściciela lub zarządcę obiektu można uświadomić, jak przebiega proces ewakuacji, posługując się programami komputerowymi do symulacji albo organizując praktyczny sprawdzian organizacji i warunków ewakuacji, co zapewnia nieporównywalnie lepsze efekty. Programy do symulacji po zaimportowaniu planów budynku, np. z projektu budowlanego, przy zachowaniu rzeczywistych wymiarów pozwolą na przedstawienie warunków ewakuacji w sposób najkorzystniejszy i najlepiej odzwierciedlający warunki panujące w danym obiekcie.
Programy są wspomagane algorytmami z zakresu sztucznej inteligencji, dlatego każdej jednostce w obiekcie można przypisać szczególne cechy osobowości i fizyczne, a także korzystać z gotowych profili osobowych uwzględniających płeć, wiek, sprawność, budowę ciała, prędkość przemieszczania czy opóźnienie w podejmowaniu decyzji o ucieczce. Wyniki wskażą przybliżony czas ewakuacji i newralgiczne punkty, na które w realu szczególnie należy zwracać uwagę.
Rzeczywistość jest jednak nieprzewidywalna, dlatego warto co jakiś czas napisać scenariusz zdarzenia i przećwiczyć próbną ewakuację z zastosowaniem wszelkich procedur służących bezpieczeństwu. Jak mówią, trening czyni mistrza. Znacznie lepiej jest się przygotować i przećwiczyć zachowania w warunkach rzeczywistych, ale nadal próbnych, niż w sytuacjach prawdziwego zdarzenia.



• Instalacja wodociągowa przeciwpożarowa
W galeriach handlowych wymagane jest stosowanie hydrantów wewnętrznych z wężem półsztywnym o średnicy 25 mm. Muszą być one rozmieszczone przy wejściach do budynku i na klatki schodowe na każdej kondygnacji, a zasięg hydrantów wewnętrznych w poziomie musi objąć całą powierzchnię chronionego budynku, z uwzględnieniem długości odcinka węża oraz efektywnego zasięgu rzutu prądów gaśniczych, tj. 3 m.

• Instalacja tryskaczowa
Istnieje także wymóg stosowania stałych samoczynnych urządzeń gaśniczych wodnych w obiektach handlowych:
a) w budynkach jednokondygnacyjnych, w strefie pożarowej zakwalifikowanej do ZL I o powierzchni powyżej 8 tys. m²;
b) w budynkach wielokondygnacyjnych, w strefie pożarowej zakwalifikowanej do ZL I o powierzchni powyżej 5 tys. m².

• System sygnalizacji pożarowej (SSP)
SSP obejmuje urządzenia sygnalizacyjno-alarmowe służące do samoczynnego wykrywania i przekazywania informacji o pożarze, a także urządzenia odbiorcze alarmów pożarowych i urządzenia odbiorcze sygnałów uszkodzeniowych. SSP jest wymagany (podobnie jak przy instalacji tryskaczowej) w budynkach handlowych, tylko bez zaszeregowania do kategorii zagrożenia ludzi, i w tym przypadku ograniczono powierzchnię strefy do 5 tys. m² w budynkach jednokondygnacyjnych i 2,5 tys. m² w wielokondygnacyjnych.

• Dźwiękowy System Ostrzegawczy (DSO)
DSO umożliwia rozgłaszanie sygnałów ostrzegawczych i komunikatów głosowych na potrzeby bezpieczeństwa osób przebywających w obiekcie, nadawanych automatycznie po otrzymaniu sygnału z SSP, a także przez operatora. Tu również ustawodawca obliguje do wyposażenia obiektów handlowych w DSO:
a) w budynkach jednokondygnacyjnych, w strefie pożarowej zakwalifikowanej do ZL I o powierzchni powyżej 8 tys. m²;
b) w budynkach wielokondygnacyjnych, w strefie pożarowej zakwalifikowanej do ZL I o powierzchni powyżej 5 tys. m².

W galeriach handlowych z ofertą kinową należy przewidzieć systemy SSP i DSO, jeśli liczba miejsc przekracza 600.

• Gaśnice
Każde centrum handlowe musi być obligatoryjnie wyposażone w gaśnice (2 kg lub 3 dm³ środka gaśniczego na każde 100 m² powierzchni strefy pożarowej), a ich rodzaj powinien być dostosowany do gaszenia pożarów, z którymi należy się liczyć w obiekcie. Muszą być one rozmieszczone w łatwo dostępnych i widocznych miejscach, przy wejściach do budynków, na klatkach schodowych, korytarzach, przy wyjściach z pomieszczeń (sklepów) na pasaż. Rozmieszczając gaśnice, należy przewidzieć, by odległość z najdalszego miejsca w obiekcie, w którym może przebywać człowiek, nie była większa niż 30 m, a także zapewnić dostęp do gaśnicy o szerokości co najmniej 1 m.

• Droga pożarowa
Droga pożarowa o utwardzonej nawierzchni powinna być doprowadzona m.in. do budynku zawierającego strefę pożarową zakwalifikowaną do kategorii zagrożenia ludzi ZL I, a więc i do centrum handlowego. Musi ona umożliwiać dojazd pojazdów jednostek ochrony ppoż. o każdej porze. Powinna przebiegać wzdłuż dłuższego boku budynku galerii handlowej na całej jego długości, a gdy krótszy bok obiektu ma ponad 60 m – z jego dwóch stron. Bliższa krawędź drogi musi być oddalona od budynku o 5–15 m. Pomiędzy drogą pożarową a budynkiem nie mogą znajdować się stałe elementy zagospodarowania terenu lub drzewa i krzewy o wysokości przekraczającej 3 m.
Spełnienie opisanych wymogów prawnych oraz wyposażenie w zabezpieczenia techniczne i pożarowe leży po stronie inwestora, później – po otwarciu obiektu – użytkownika i zarządcy.
Bardzo ważnym elementem jest przeanalizowanie zdarzeń mogących wystąpić w galerii handlowej. Pomimo zastosowanych zabezpieczeń nie można zakładać, że nic się nie zdarzy, że klient nie stworzy zagrożenia, bo dla jednych wyjście do galerii handlowej to forma spędzenia wolnego czasu czy zrelaksowania się, dla innych natomiast może być okazją do spełnienia szalonych planów i np. podłożenia ognia czy ładunku wybuchowego. Ponieważ nie wszystko da się przewidzieć, należy przeprowadzać szkolenia personelu i odpowiednio przygotowywać się do różnych scenariuszy. W sytuacji zagrożenia to te osoby będą wskazywać zdezorientowanym klientom bezpieczne wyjście.
A co możemy zrobić my, zwykli klienci, żeby czuć się bezpiecznie w galerii handlowej? Powinniśmy stać się bardziej świadomi zagrożeń, zwracać większą uwagę na oznaczenia ewakuacyjne i znaki bezpieczeństwa, wiedzieć, gdzie jest miejsce zbiórki do ewakuacji, gdzie znajdują się pionowe drogi ewakuacyjne i wyjścia ewakuacyjne, znać numery alarmowe i zasady zgłaszania zagrożeń. To na co dzień, bez szukania górnolotnych powodów, natomiast w sytuacji prawdziwego zagrożenia należy zaufać osobom kierującym ewakuacją. □

Renata Trojanowska

Absolwentka Wydziału Inżynierii Bezpieczeństwa Pożarowego w Szkole Głównej Służby Pożarniczej w Warszawie, do niedawna zawodowo zajmowała się projektowaniem systemów gaszenia, dziś specjalistka ds. inwestycji budowlanych.

LITERATURA:

[1] Ustawa z 7 lipca 1994 r. – Prawo budowlane (tekst jedn. Dz.U z 2019 r., poz. 1186).
[2] Rozporządzenie Ministra Infrastruktury z 12 kwietnia 2009 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (tekst jedn. Dz. U. 2019 poz. 1065).
[3] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. 2010 nr 109 poz. 719).
[4] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 24 lipca 2009 r. w sprawie przeciwpożarowego zaopatrzenia w wodę oraz dróg pożarowych (Dz.U. nr 124 poz. 1030).
[5] Raport CBRE i Trei Real Estate Poland: Parki handlowe w Polsce.

Wykorzystanie systemu integrującego urządzenia przeciwpożarowe

na potrzeby zarządzania ewakuacją

T E K S T
Krzysztof Kunecki
Schrack Seconet Polska

Przy tworzeniu koncepcji bezpieczeństwa pożarowego, szczególnie w zakresie zapewnienia bezpiecznej ewakuacji osób w sytuacji zagrożenia dla obiektu handlowego, należy wziąć pod uwagę jego funkcjonowanie podczas codziennego użytkownika oraz fakt przebywania w nim osób, które nie są jego stałymi użytkownikami. Dobór urządzeń i rozwiązań powinien zapewnić pełny nadzór nad ewakuacją oraz umożliwiać aktywne wpływanie na procedurę ewakuacji w przypadku sytuacji specjalnych, wymagających np. przekierowania osób do innych wyjść ewakuacyjnych.

Zapewnienie bezpiecznej ewakuacji osób z budynku wymaga spełnienia niżej wymienionych warunków podstawowych:

1) wczesna i niezawodna detekcja i identyfikacja miejsca pożaru,
2) powiadomienie straży pożarnej w celu jak najszybszego rozpoczęcia akcji ratowniczo-gaśniczej,
3) zaalarmowanie osób przebywających w obiekcie o wykrytym zagrożeniu i skierowanie ich do najbliższych dostępnych wyjść ewakuacyjnych:
   - wysterowanie dźwiękowego systemu ostrzegawczego (DSO) lub sygnalizatorów akustycznych/optycznych w zależności od zastosowanego rozwiązania,
   - wysterowanie dynamicznego oświetlenia ewakuacyjnego (stosowanego opcjonalnie dla poprawy warunków ewakuacji),
4) uruchomienie urządzeń przeciwpożarowych odpowiedzialnych za wydzielenie strefy objętej pożarem od innych części obiektu, aby ograniczyć rozprzestrzenianie się pożaru, a w szczególności chronić drogi ewakuacyjne,
5) uruchomienie urządzeń oddymiających oraz zapobiegających zadymieniu, aby droga ewakuacyjna była wolna od dymu,
6) udrożnienie dróg ewakuacyjnych poprzez wysterowanie (zwolnienie) przejść systemu kontroli dostępu na drodze ewakuacji,
7) zapewnienie oświetlenia awaryjnego (ewakuacyjnego i zapasowego) w pomieszczeniach i na drogach ewakuacyjnych.

Opisane powyżej wytyczne powinny być zawarte w scenariuszu rozwoju zdarzeń w czasie pożaru, który powinien być przygotowany na etapie projektu budowlanego. Scenariusz pożarowy musi zawierać informacje o warunkach ochrony ppoż., analizę potencjalnych zagrożeń i wytyczne w zakresie doboru odpowiednich urządzeń. Za jego wykonanie odpowiadają projektant i rzeczoznawca ds. zabezpieczeń ppoż.

Na podstawie uzgodnionego scenariusza pożarowego należy dobrać wymagane urządzenia ppoż., stąd szczególnie istotna jest analiza warunków ewakuacji w celu wyboru optymalnego rozwiązania. Podstawowym warunkiem realizacji założeń scenariusza pożarowego jest automatyczne uruchomienie (zadziałanie) urządzeń przeciwpożarowych w przypadku wystąpienia pożaru w dowolnej części obiektu. Szczegółowe powiązania między ostrzegaczami pożarowymi a urządzeniami przeciwpożarowymi zabezpieczającymi wraz z dodatkowymi informacjami o warunkach ich wysterowania są zawarte w matrycy sterowań przygotowywanej na etapie projektu wykonawczego.

W zależności od wielkości zabezpieczanego obiektu, w momencie wystąpienia alarmu pożarowego konieczne jest wysterowanie często setek, a nawet tysięcy urządzeń wykonawczych. Dodatkowo należy też nadzorować stan poprawnego zadziałania uruchomionych urządzeń, a więc zarządca obiektu musi mieć narzędzie do sprawnego zrządzania urządzeniami i systemami dedykowanymi do ochrony ppoż.

W takim przypadku optymalnym rozwiązaniem jest zastosowanie dedykowanego certyfikowanego systemu integrującego urządzenia przeciwpożarowe (SIUP), który umożliwia nie tylko szczegółowe nadzorowanie (wizualizację) stanów pracy urządzeń, ale również ich pełną obsługę i sterowanie ręczne wieloma funkcjami. SIUP umożliwia też zmianę procedur automatycznego sterowania, co ma kluczowe znaczenie dla procedury ewakuacji i stanowi istotną różnicę w porównaniu z działającym automatycznie systemem sygnalizacji pożarowej, który inicjuje jednostadiowy tryb pracy urządzeń przeciwpożarowych zabezpieczających.

Podstawową zaletą SIUP jest jego elastyczność pozwalająca na optymalny – z perspektywy konkretnego typu obiektu – dobór elementów oraz funkcji, z zapewnieniem ścisłej współpracy i podziału kompetencji pomiędzy zintegrowanymi systemami. Istotną cechą systemu integrującego (w przeciwieństwie do standardowego systemu sygnalizacji pożarowej) jest możliwość spełnienia nieograniczonej liczby zadań i funkcji logicznych związanych z obsługą, sterowaniem i nadzorowaniem systemów w obiekcie, co ma szczególne znaczenie dla bezpiecznej ewakuacji obiektu.

W dalszej części artykułu zostaną omówione funkcje SIUP w zakresie zarządzania ewakuacją na poszczególnych etapach ewakuacji w odniesieniu do integrowanych systemów.

Wykrycie pożaru – weryfikacja alarmu i rozpoczęcie ewakuacji

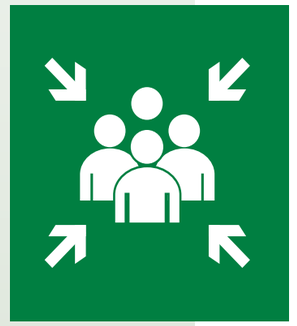
W momencie wyzwolenia alarmu przez czujkę pożarową lub ROP system SIUP automatycznie przełącza się na grafikę z alarmującym elementem, z jednoczesnym przedstawieniem operatorowi (personelowi uprawnionemu) instrukcji (kroków) postępowania dla danego zagrożenia. Dodatkowo dla ułatwienia lokalizacji pożaru w sytuacji zastosowania czujek specjalnych (np. czujki zasysające dymu) czy też zwizualizowania obszaru zadziałania urządzeń ppoż. (np. instalacji tryskaczowych) mogą zostać zaprogramowane aktywne graficzne obszary nadzorowania, które pokazują, jaki obszar jest objęty zagrożeniem pożarowym i/lub oddziaływaniem urządzeń zabezpieczających. Ma to szczególne znaczenie dla dokonania szybkiej oceny konkretnego zdarzenia.

Instrukcja postępowania jest przygotowywana na podstawie instrukcji bezpieczeństwa pożarowego (wymaganej dla każdego obiektu). Powinna zawierać szczegółowe wytyczne postępowania, z czytelnymi informacjami w zakresie działania zintegrowanych urządzeń ppoż. w następujących obszarach: ewakuacja osób, ograniczenie rozprzestrzeniania się pożaru i zapewnienie bezpieczeństwa ekipom ratowniczym.

W przypadku integrowania SIUP z systemem dozoru wizyjnego (VSS) wyświetlany obraz z kamery powiązanej z alarmującym elementem z zagrożonego obszaru pozwala na szybszą weryfikację zagrożenia. Operator może potwierdzić zdarzenie pożarowe bezpośrednio z poziomu platformy informatycznej SIUP, a tym samym bezzwłocznie uruchomić procedury sterowania urządzeniami ppoż. zgodnie ze scenariuszem pożarowym. Integracja z VSS pozwala w szczególnych przypadkach także na uruchomienie procedury alarmowej, zanim zdarzenie zostanie wykryte przez czujki pożarowe. W przypadku wykrycia pożaru podczas rutynowej obserwacji obiektu operator systemu VSS może wysłać specjalny sygnał alarmowy do systemu integrującego, aby z poziomu systemu certyfikowanego na potrzeby zarządzania ewakuacją uruchomić procedurę sterowania urządzeniami ppoż. Za pomocą tego interfejsu może być przesłana także informacja o innym zdarzeniu niebezpiecznym (kryzysowym) w obiekcie, które wymaga odpowiedniej reakcji służb ochrony obiektu i ukierunkowanej ewakuacji. W tym zakresie niezbędne jest jednak osobne opracowanie procedury ochrony osób i ich ewakuacji z obiektu z wykorzystaniem SIUP.

Ewakuacja osób – zarządzanie ewakuacją

Po uruchomieniu urządzeń odpowiedzialnych za ewakuację, SIUP realizuje funkcję nadzoru nad skutecznością realizowanych funkcji podstawowych i dodatkowych dzięki integracji z innymi systemami. W przypadku integracji SIUP z systemem kontroli dostępu (SKD) nadzorowane jest – oprócz samego wysterowania przez wyjścia systemu sygnalizacji pożarowej aktywatorów przejść także potwierdzenie „zdjęcia" napięcia z samych elektrorygli dla potwierdzenia skuteczności wysterowania, a nadzorowanie systemu wentylacji pożarowej pozwala na weryfikację skuteczności oddymiania dróg ewakuacyjnych. W przypadku sytuacji specjalnych SIUP może być stosowany do sterowania ręcznego ewakuacją, np. za pośrednictwem DSO. W przypadku integracji cyfrowej DSO z SIUP istnieje możliwość uruchomienia lub zatrzymania zaprogramowanych komunikatów alarmowych i ostrzegawczych bezpośrednio z poziomu platformy informatycznej SIUP.



Zastosowany w obiekcie system dynamicznego oświetlenia ewakuacyjnego i jego integracja z SIUP pozwala na dynamiczną ewakuację osób w zależności od miejsca pożaru, jego rozprzestrzeniania, dostępności (drożności) dróg i przejść ewakuacyjnych. Na podstawie informacji z nadzorowanych urządzeń jak np. obraz z VSS operator może monitorować stan przejść ewakuacyjnych i w sytuacji ich zablokowania przekierować osoby do bezpiecznych wyjść ewakuacyjnych.

W artykule przedstawiono wybrane funkcje SIUP, który umożliwia realizację dowolnych funkcji nadzoru i ręcznego sterowania, zależnie od typu zintegrowanych systemów. Zastosowanie certyfikowanego systemu integrującego urządzenia ppoż. oraz inne urządzenia techniczne mające wpływ na bezpieczeństwo pożarowe obiektu, znacznie podwyższa poziom bezpieczeństwa obiektu i pozwala na aktywne reagowanie w sytuacjach, gdy procedury automatycznego działania są niewystarczające. ▫

Schrack Seconet Polska
ul. A. Branickiego 15,
02-972 Warszawa
www.schrack-seconet.pl

Sklep z bezpieczeństwem

czyli jak kupujemy rozwiązania i usługi

TEKST
Rafał Łupkowski

Zakup usług z zakresu bezpieczeństwa na polskim rynku często sprowadza się do wypełnienia tabelki ograniczonej do dwóch okienek, np. liczba roboczogodzin i stawka za roboczogodzinę. Taki schemat zakupowy wpływa bezpośrednio na postępującą degradację niektórych usług.

Upraszczanie i sprowadzanie całego rynku do wspólnego mianownika nie jest najlepszym podejściem, nie wszystkie bowiem czynności związane z zakupami wyglądają podobnie. Dlaczego jednak wiele z nich nie zawiera podstawowych wartości parametrów produktu czy usługi?
Pamiętam sprzed lat jedną z pierwszych moich analiz oferty dotyczącej systemów zabezpieczeń. Ofertę na system sygnalizacji włamania i napadu (SSWiN) otwierała pozycja w tabeli: *Centrala alarmowa szt. 1 – Cena (taka a taka)*.
Zdziwiłem się i uznałem to za błąd, po czym skontaktowałem się z rzeczonym dostawcą, aby doprecyzować materiał. W odpowiedzi usłyszałem, że oferta jest kompletna! Postanowiłem odwrócić role. Wcieliłem się w rolę sprzedawcy i powiedziałem, że mam do sprzedania samochód w bardzo dobrej cenie i czy jest zainteresowany jego zakupem. Usłyszałem zdziwiony głos rozmówcy, o co właściwie mi chodzi. *Zastanawiałem się, czy zapytałby pan, stojąc przed decyzją zakupu, np. o markę, model, rodzaj silnika czy wyposażenie auta* – wyjaśniłem. Mój rozmówca poprawił zestawienie zgodnie z naszymi oczekiwaniami...
W rezultacie tego i kilku podobnych ćwiczeń powstało coś na kształt standardu zapytania ofertowego, a ujęta w nim tabela uniemożliwiała dowolność interpretacji przedmiotu zapytania, jasno określała warunki dla wszystkich potencjalnych dostawców i pozwalała na precyzyjne oddzielenie urządzeń od materiałów instalacyjnych i robocizny. Do dziś spotykam (podobne jak opisane wyżej) przypadki zapytania i ofertowania.

Podstawowym wyzwaniem dla wielu działów zakupów, a także jednostek merytorycznych jest określenie warunków brzegowych dotyczących rozwiązania bądź usługi. Zleceniodawcy często nie mają świadomości, że jest możliwe, a wręcz pożądane określenie warunków (tzw. parametryzacja) usługi jeszcze na etapie zapytania o jej koszt. To właśnie te warunki – np. rodzaj wyposażenia, kompetencje językowe, a także warunki *Service Level Agreement* (SLA) – określają konieczny potencjał, a także ewentualne ryzyka po stronie wykonawcy. Dlaczego więc tak rzadko korzystamy z tej możliwości? Przyznam, że i ja miewam trudność z jednoznaczną odpowiedzią na to pytanie.

Dość często spotykam się z podejściem do zakupu rozwiązań z zakresu bezpieczeństwa biznesu bez wyraźnej koncepcji co do jego działania, tzn. bez odpowiedzi na podstawowe pytanie, co to rozwiązanie ma w rezultacie dostarczyć.
Jeden z potencjalnych klientów postanowił, że ochronę osobową w sieci obiektów użyteczności publicznej zastąpi rozwiązaniami technicznymi. Pomysł ten ze względu na szybujące stawki godzinowe wydawał się zasadny. Nie można jednak tak po prostu zastąpić człowieka kamerą dozorową, jeśli nie ma się wiedzy, jakie wykonuje on zadania i jakie ew. procesy operacyjne jego działalność implikuje. Jeśli zadania ochrony ograniczają się do podnoszenia szlabanu, sytuacja jest relatywnie prosta, pod warunkiem że ów pracownik nie odbiera np. nocnych dostaw części do produkcji. A znacząco komplikuje się, gdy jednocześnie np. administruje uprawnieniami kontroli dostępu dla pracowników kompleksu, o czym mógł nie wiedzieć nawet zarząd spółki, podejmując decyzje zakupowe.

Czy przed rozpoczęciem procesów zakupowych warto tworzyć koncepcję bezpieczeństwa? Czy w procesie zakupowym Security Concept odgrywa ważną rolę i jaką wartość dodaną zapewnia?
Odpowiedź na te pytania brzmi: zdecydowanie TAK, ponieważ zakupy – bez względu na to, czy dotyczą usług, czy rozwiązań bezpieczeństwa – warto poprzedzić analizą wpływu na działalność operacyjną oraz upewnić się, że wnoszą wartość dodaną. Ważne, by podobnie postrzegali to zleceniodawcy. Jak zatem zadbać o prawidłowy przebieg postępowania zakupowego już na etapie jego przygotowania?

- Powinno się inwentaryzować obszar zakupowy. Analiza stanu faktycznego, często sprowadzająca się do audytu usługi lub zwykłej inwentaryzacji systemu, pozwala określić dokładnie stan faktyczny i rzeczywiste potrzeby. Często rozwiązania kupowane przed kilkoma laty są już nieadekwatne do skali prowadzonych operacji i nie wspierają ich.
- Należy określić, czego oczekujemy od systemu na podstawie konkretnych przesłanek – czyli jakie ryzyka chcemy ograniczyć lub jakie procesy powinniśmy wspierać? Nie ulegajmy nadmiernym pokusom wyszukanych rozwiązań, jeśli docelowo nie mamy zamiaru lub możliwości z nich korzystać. To kosztuje. Po co wprowadzać rolls-royce'a, kiedy po dokładnym określeniu potrzeb VW golf wykona zadanie.
- Trzeba określić parametry zamówienia na tyle precyzyjnie, aby nie pozostawić dowolności interpretacyjnej. Unikniemy wówczas sytuacji, w której porównujemy „jabłko do śliwki" i nawet najstarsi handlowcy i security managerowie mają problemy z opracowaniem rekomendacji dla decydentów.
- Warto korzystać z dostępnej wiedzy rynkowej. Mając na względzie postęp i szybkość zachodzących zmian, nie bójmy się korzystać z wiedzy innych, zwłaszcza że nasze doświadczenia często są ukierunkowane tylko na jeden sektor. Może to powodować, że umkną nam rzeczy ciekawe, użyteczne i skuteczne, które np. inne branże wprowadziły z racji swojej specyfiki znacznie wcześniej i nie musimy wymyślać koła, które już się kręci, albo prochu.
- Traktujmy częściej proces zakupowy tak, jakbyśmy wydawali własne pieniądze. To pozwala zmienić optykę i ograniczyć potencjalne zakupy, dostosowawszy je do rzeczywistych potrzeb, a co za tym idzie precyzyjnie argumentować dostarczoną wartość dodaną.

Nie można pominąć bardzo ważnego aspektu, jakim jest kupowanie rozwiązania lub usługi, a nie np. roboczogodziny – sprowadzenie procesu zakupowego w systemach bezpieczeństwa do tzw. ślepego kosztorysu z reguły bowiem kończy się posiadaniem karykatury rolls-royce'a czy VW golfa (bez możliwości komfortowego i sprawnego podróżowania) oraz nieuchronną wymianą floty. Wielu decydentów wydaje w ten sposób pieniądze przedsiębiorstwa, czemu mógłby skutecznie zapobiec dobrze opracowany i zastosowany przez strony transakcji Security Concept.
Łatwo powiedzieć, trudniej wykonać – w często skomplikowanych procesach zakupowych świat idealny jest trudny do osiągnięcia. Należy jednak próbować zmieniać nieskuteczną rzeczywistość, ucząc się od lepszych, gdyż takie podejście działa i z pewnością ma przyszłość. □

Nie można tak po prostu zastąpić człowieka kamerą dozorową, jeśli nie ma się wiedzy, jakie wykonuje on zadania i jakie ewentualnie procesy operacyjne jego działalność implikuje

BIO
Rafał Łupkowski

Niezależny doradca w obszarze bezpieczeństwa biznesu, właściciel firmy SecurityBroker.
Pasjonat i wieloletni praktyk zarządzania bezpieczeństwem biznesu w korporacjach międzynarodowych, współtwórca Kongresu Security.

Ekonomiczny wymiar cyberprzestrzeni

SZYBKIE PRZEMIANY CYWILIZACYJNE OSTATNICH LAT I ROZWÓJ NOWOCZESNYCH TECHNOLOGII SPOWODOWAŁY, ŻE ZIEMIĘ OGARNĘŁO PRAWDZIWE CYFROWE TSUNAMI. CYBERINTEGRACJA STAŁA SIĘ TAK POWSZECHNYM ZJAWISKIEM, ŻE NAWET NIE ZDAJEMY SOBIE SPRAWY Z TEGO, JAK BARDZO JESTEŚMY UZALEŻNIENI OD CYFROWYCH ZER I JEDYNEK. GŁĘBOKIE PODPORZĄDKOWANIE ŻYCIA CZŁOWIEKA I OTACZAJĄCYCH GO PROCESÓW GOSPODARCZYCH WSZECHOBECNEJ INNOWACYJNOŚCI NIESIE ZARÓWNO KORZYŚCI, JAK I ZAGROŻENIA.

Gospodarka nasycana kolejnymi innowacjami technologicznymi ustawicznie się zmienia. Wraz z postępem technologicznym maszyny coraz częściej zaczynają zastępować człowieka, a ludzie są świadkami szybkich zmian, z czym wcześniej nie mieli do czynienia. Technologia i jej nieustanny rozwój pozwalają zintegrować współczesne społeczeństwo i działalność biznesową, sprawiając, iż staje się ono cyfrową wspólnotą. Przyspiesza także proces globalizacji, a to z kolei napędza kolejne fazy rozwoju technologicznego. Elastycznym procesom rozwoju gospodarczego powinno jednak towarzyszyć myślenie o konsekwencjach szybkiego postępu i dbałość o poczucie bezpieczeństwa jednostki i całego społeczeństwa.
Miarą zmian, jakie zachodzą w funkcjonowaniu zarówno jednostki, niewielkich firm, jak i transnarodowych korporacji, jest idea społeczeństwa informacyjnego oparta na rozwoju technologicznym. Nowe technologie pozwalają przetwarzać, gromadzić, odzyskiwać i przekazywać informacje w dowolnej formie – mówionej, pisanej i wizualnej – bez względu na odległość, czas i wielkość. Wraz z rozwojem technologicznym i jego wpływem na przemiany gospodarki typologia różnych obszarów zaangażowanych w tworzenie potencjału ekonomicznego jest w większym stopniu uzależniona od innowacji.

T E K S T
Krzysztof Gawkowski

Systemy gospodarcze na całym świecie zmieniały się i ewoluowały w minionych wiekach wielokrotnie. W XXI w. tradycyjny, a zarazem historyczny podział świata zmienia się gwałtownie. Z chwilą pojawienia się i upowszechnienia pojęcia społeczeństwa informacyjnego prym wiedzie podział cyfrowy – na mających bądź niemających dostępu do nowoczesnych technologii. Skok technologiczny ostatnich dekad spowodował, że gospodarka przyjęła zupełnie nowy wymiar, który ma podstawę w cyberprzestrzeni. Obszar ten obejmuje wiele poziomów i klasyfikacji, ale bez wątpienia rozpoczyna się od obywateli, a kończy na rządzących. Technologie informacyjno-komunikacyjne stanowią obecnie jeden z najważniejszych elementów rozwoju gospodarczego, a globalna sieć komunikacyjna pozwala na interakcję oraz wymianę informacji i pomysłów na całym świecie.

Pozytywnego wpływu nowoczesnych technologii na gospodarkę nie sposób kwestionować. Chodzi tu nie tylko o rozszerzającą się błyskawicznie ofertę nowych produktów i usług, lecz także o umiejętność posługiwania się technologiami IT w obszarze biznesu. Tegoroczne badania Polskiego Instytutu Cyberbezpieczeństwa wskazują, że w grupie firm osiągających najlepsze wyniki finansowe ponad 70 proc. zdolnych jest tworzyć i wdrażać nowe rozwiązania technologiczne w ciągu trzech miesięcy lub krótszym czasie. Do najnowocześniejszych rozwiązań należą obecnie różnego rodzaju aplikacje mobilne, gromadzenie i przetwarzanie dużych zasobów danych (*big data*), korzystanie z możliwości chmury obliczeniowej, a także uczenie maszynowe, sztuczna inteligencja, robotyka (zwłaszcza w zakresie robotów mobilnych) i Internet Rzeczy.
Gospodarka i biznes zmieniają się dynamicznie również dzięki niewyobrażalnemu komunikacyjnemu przyspieszeniu. Dzisiaj mało kto pamięta czasy telegrafów, przewodowych telefonów i faksów. Nawet korespondencja listowa bardziej kojarzy się z wysyłką e-maila niż kopertą ze znaczkiem. W Polsce w 1985 r. nadano ok. 20 mln telegramów, w 1990 r. było to 12 mln, w 2002 r. – 2,5 mln, a po roku 2010 ich liczba spadła do ok. 0,4 mln. Dziś usługa telegramu jest już niedostępna, a liczba SMS-ów, jaką dziennie wysyłają Polacy, przekracza 250 mln.
Duża część przedsiębiorstw także rozwija się dzięki narzędziom technologicznym, pozwalającym na prowadzenie e-biznesu lub stosowaniu jego elementów w działalności, a więc dającym np. szansę sprzedaży towarów i usług z wykorzystaniem sieci teleinformatycznych (zarówno w kraju, jak i poza jego granicami). Podstawowe segmenty e-biznesu to: serwisy internetowe i e-usługi (np. portale, strony ogłoszeniowe, media społecznościowe, wortale), e-marketing (np. agencje interaktywne, agencje SEO/SEM), e-commerce (np. e-sklepy, serwisy aukcyjne, serwisy zakupów grupowych) oraz serwisy dla e-biznesu (np. hosting, płatności itp.). Obecnie wartość rynku e-commerce na świecie wycenia się na prawie 2 bln dolarów, a kupuje w nim już ponad 2 mld osób.

Dochody z e-commerce rosną także w Polsce. W tym roku rynek będzie wart 50 mld zł. Z raportu Statista Digital Market Outlook wynika, że Polska znajduje się na trzynastym miejscu w zestawieniu najszybciej rosnących rynków e-commerce na świecie. W najbliższych czterech latach jego wartość ma się powiększyć o ponad 20 mld zł. E-handel stał się dla Polaków codziennością i ponad 15 mln obywateli decyduje się za zakupy w Internecie, dzięki czemu rosną branże firm kurierskich, logistycznych czy agencji interaktywnych.
Jednym z najbardziej cennych obszarów, wpływających na ekonomiczne wyniki zarówno państw, jak i firm z sektora prywatnego, są dane osobowe. W 2018 r. jego wartość wyniosła ponad 21 mld dolarów, w roku 2019 wzrośnie o kolejne 25–30 proc. Najwięcej cyfrowych informacji o internautach kupuje się w Stanach Zjednoczonych, a cały północnoamerykański rynek danych osiągnie w 2019 r. wartość 12,3 mld dolarów. Na drugim miejscu znajduje się Wielka Brytania – tu wydatki sięgają niemal 1,9 mld dolarów, a w 2019 r. wzrosną o 25% do 2,4 mld dolarów. Intensywnie rozwija się także rynek chiński, który charakteryzuje się największą dynamiką wzrostu, a jego wartość szacuje się na 1,5 mld dolarów. Podobnie jest w Polsce, gdzie sprzedaje się dane o wartości 21 mln dolarów, w przyszłym roku ma to być blisko 40 mln dolarów.

Technologią, która całkowicie zmieni ekonomiczne ramy świata, jest najprawdopodobniej *blockchain*. Jego olbrzymie możliwości wynikają z tego, że systemy w ten sposób budowane opierają się na łańcuchu rozproszonych bloków, bez jednostki centralnej. Taka konstrukcja procesu komunikacyjnego umożliwia łączenie niezależnych od siebie komputerów. Dane między nimi są przesyłane w formie zaszyfrowanej, co pozwala na identyfikację tylko nadawców i odbiorców. Ponadto, jeśli użytkownik chce dodać do zbioru jakąkolwiek informację, musi ona zostać zaakceptowana przez pozostałych. To jedna z głównych zalet systemu, ponieważ dane są chronione na wielu płaszczyznach. Nawet włamanie do jednego z ogniw systemu nie spowoduje utraty danych, bo jednocześnie są one zapisane w wielu miejscach. Na razie gospodarka uczy się *blockchain* kojarzonego przede wszystkim z kryptowalutami, tym niemniej globalny rynek zastosowań tego typu rozwiązań rozwija się w błyskawicznym tempie. Szacuje się, że wpływy związane z użytkowaniem tej technologii mogą być liczone w bilionach dolarów, a rozwiązania wdrożone w wielu sektorach. Giełda na Wall Street rozważa nawet powołanie specjalnego rynku dla takich spółek, a Bank Światowy zlecił narodowemu bankowi Australii przeprowadzenie pierwszej emisji dwuletnich obligacji w systemie rejestrów rozproszonych.

Trudno jednak wskazać cele, które mają stanowić fundament bezpiecznego kształtowania gospodarki i ekonomii. Niepodważalne jest to, że rozwój technologii pozostaje nieodłącznym elementem rozwoju społeczno-gospodarczego, a w momencie zestawienia go z konkretną kwestią pojęcie to nabiera nowego kontekstu – można powiedzieć nawet, że specjalnego znaczenia. Wysoki poziom bezpieczeństwa ekonomicznego w cyfrowym świecie zależy od wielu czynników. Najważniejszymi są odpowiednia koordynacja działań mająca na celu zachowanie oraz umiejętność dostrzegania zagrożeń i właściwe reagowanie na nie. Rynki finansowe związane z szybkim rozwojem technologicznym nigdy jednak nie osiągną pożądanego stanu, jeśli nie będzie istniał odpowiedni system organizacyjno-prawny w tym zakresie.

Nowoczesne technologie i cyberprzestrzeń stały się jednymi z najważniejszych obszarów funkcjonowania innowacyjnej gospodarki. Mimo że duża grupa użytkowników Internetu wciąż pamięta czasy, gdy technologie te jeszcze nie funkcjonowały, przyzwyczajenia sprawiają, iż obecnie nie wyobrażają sobie bez nich życia. W celu zapewnienia odpowiednich norm mających organizować ochronę technologiczną państwa i rządy muszą konsekwentnie angażować się w procesy mające na celu poznanie ekonomicznego wymiaru cyberprzestrzeni. Brak granic komunikacyjnych w zglobalizowanym świecie musi iść również w parze z tworzeniem prawa i przepisów o zasięgu ogólnoświatowym. Dalszy rozwój gospodarczy jest bowiem możliwy tylko wtedy, gdy korzystanie z nowoczesnych technologii będzie otwarte i bezpieczne.

Rozwój technologii nie będzie zwalniał, a wszystko wskazuje, że przyspieszy. Członkowie Rady Rozwoju Biznesu „Forbesa" wskazali kilka technologii, które ich zdaniem będą w ciągu najbliższych lat rewolucjonizowały gospodarkę. Do kluczowych innowacji zaliczyli m.in. rzeczywistość wirtualną i rozszerzoną, która do roku 2020 będzie przemysłem wartym 140 mld dolarów. Zmieni ona na pewno sposób interakcji między ludźmi i zamiast rozmów telefonicznych i wideokonferencji spotkania biznesowe będą się odbywać w świecie wirtualnym. Ważnym elementem mają być też boty mające być pomostem między gromadzeniem ważnych informacji a wstępną oceną możliwości handlowych. Uwagę zwraca się także na technologie głosowe, czyli możliwość rozmowy z maszyną, która odpowiada na pytania złożone, a następnie przeprowadzania transakcji – bez dotknięcia klawisza klawiatury i sięgania po telefon.

Pomimo szybkiego rozwoju technologicznego cyberbezpieczeństwo ekonomiczne nie jest elementem integralnym w procesie wdrażania technologii. W Polsce przedsiębiorstwa przeznaczają zaledwie 4–5 proc. swojego budżetu na cyberochronę, a to zdecydowanie za mało, aby zbudować skuteczną obronę przed atakami. Pocieszający może być jednak fakt, że z roku na roku świadomość konieczności inwestycji w tym obszarze rośnie. Firmy i ich właściciele coraz częściej interesują się, jak nie stracić przewagi konkurencyjnej. Decydują się na udział w audytach, badaniach czy testach potwierdzających przygotowanie do ochrony przed atakiem w cyberprzestrzeni i wykazują chęć przeciwdziałania czyhającym zagrożeniom.

Ekonomiczny krwiobieg świata tworzy dziś otwarta i złożona z wielu obszarów cyberprzestrzeń. Nowoczesne technologie codziennie ewoluują i tylko od człowieka zależy, w jaki sposób będzie je wykorzystywał. Żyjemy w czasach, które mogą zaskoczyć nas postępem nawet z dnia na dzień. Warto przy tym pamiętać, że większość społeczeństwa na co dzień nie zastanawia się, jaki wpływ na ich życie mają nowoczesne technologie i czy są one bezpieczne. Ekonomia to dla jednostki zazwyczaj zasobność konta w banku, które powinno być bezpieczne. Brak granic komunikacyjnych w zglobalizowanym świecie sprawił, że pomysł na zrównoważony balans społeczny pomiędzy nową technologią a bezpieczeństwem ekonomicznym musi iść w parze z zapobieganiem zagrożeniom, których możemy nawet nie znać. □

Nowoczesne technologie i cyberprzestrzeń stały się jednymi z najważniejszych obszarów funkcjonowania innowacyjnej gospodarki

BIO

Krzysztof Gawkowski

społecznik i wykładowca akademicki. Doktor nauk humanistycznych specjalizujący się w zakresie bezpieczeństwa państwa. Dyrektor Polskiego Instytutu Cyberbezpieczeństwa oraz kierownik Katedry Bezpieczeństwa Wewnętrznego Uczelni Techniczno-Handlowej im. Heleny Chodkowskiej w Warszawie. Członek Komitetu Technicznego PKN oraz przewodniczący Rady Programowej Instytutu Bezpieczeństwa Inteligentnych Miast. Autor książek: ***Obudzić państwo*** oraz ***Administracja samorządowa w teorii i praktyce***, a także powieści kryminalnych ***Piętno prawdy*** oraz ***Cień przeszłości.***

PRZESTĘPSTWA białych kołnierzyków

TEKST
Michał Czuma

W lipcowo-sierpniowym wydaniu amerykańskiego „Harvard Business Review" ukazał się artykuł analizujący ostatnie największe skandale w handlu pod kątem nieetycznych, oszukańczych praktyk biznesowych i czy przyniosły korzyści biznesowi i sprawcom naruszeń. W Polsce też mamy skandale, np. GetBack czy afera mięsna, która nadszarpnęła opinię o naszych produktach, utrudniając handel w kilku krajach. Tych, którzy biorą w nich udział, można podzielić na kilka grup: pierwsza to sprawcy – część już odbywa kary pozbawienia wolności, część ma do czynienia z organami ścigania, inni mają nadzieję, że nikt do nich nie dotrze. Zdecydowana większość czuje się pokrzywdzona.

Tego typu skandali na całym świecie jest bardzo dużo. Trzy lata temu, latem 2016 r. pojawiły się doniesienia, że pracownicy Wells Fargo – jednostki bankowości detalicznej prywatnego banku o 160-letniej historii – otworzyli ponad milion nieautoryzowanych kont i sprzedali tysiące niepotrzebnych produktów swoim klientom, wykorzystując ich zaufanie. Skandal drogo kosztował Wells Fargo. Biuro Ochrony Finansowej Konsumentów (wraz z Urzędem Controller of the Currency and the City and County of Los Angeles) 8 września ukarało firmę grzywną w wysokości 185 mln dolarów. Po ujawnieniu kolejnych nadużyć konsumenckich bank ukarano dodatkową grzywną w wysokości 1 mld dolarów; musiał też wysupłać kolejne 575 mln na zaspokojenie roszczeń prawnych poszkodowanych klientów. Kurs jego akcji spadł natychmiast o 13%, obniżając kapitalizację o ok. 20 mld dolarów, do dziś pozostawiając bank w zastoju.

John Stumpf, który w październiku 2016 r. zrezygnował z funkcji prezesa zarządu, oraz Carrie Tolstedt, szefowa banku detalicznego, która w lipcu 2016 r. ogłosiła przejście na emeryturę, zostali zmuszeni przez zarząd do zwrotu dziesiątek milionów dolarów wypłaconych im jako premie. Czterech starszych menedżerów odeszło z pracy z własnej woli. Reputacja firmy została splamiona – dla szczycącej się długą historią instytucji upokorzenie było szczególnie bolesne. Pracownicy Wells Fargo, kiedyś przekonani, że naciąganie klientów na nic niewarte produkty przyniesie im kosmiczne zyski, już wiedzą, że oszustwo nie popłaca.

Jak mogło dojść do takiego biznesowego kolapsu, tym bardziej że naganne praktyki były szeroko rozpowszechnione w jednostkach detalicznych banku, chociaż Wells Fargo posiadał systemy kontroli i zarządzania ryzykiem nadzorowane przez zarząd? Co nie zadziałało? Dochodzenie zlecone przez zarząd wykazało, że zawiniły wypaczona kultura korporacyjna, zdecentralizowana struktura organizacyjna i słabe przywództwo. Śledztwo wewnętrzne ujawniło, że nielegalne zachowania były podyktowane presją osiągania zbyt agresywnych celów sprzedażowych, co wiązało się z premiami i promocjami. Kierownictwo firmy otrzymywało wiele sygnałów ostrzegawczych: od 2000 do 2004 r. liczba przypadków realizacji takich celów przez pracowników wzrosła 10-krotnie, a krytyczne artykuły budzące wątpliwości co do nowych kont, presji na sprzedaż i rosnącej rotacji pracowników pojawiły się w „Wall Street Journal" w 2011 r. i w „Los Angeles Times" w 2013 r. Liderzy banku detalicznego obarczyli jednak tymi problemami kilku – ich zdaniem – złych pracowników, natomiast prezes banku bez głębszej refleksji to akceptował.

Niestety historia Wells Fargo nie jest jedyna. Przestępstwa popełnione przez ludzi w białych kołnierzykach – oszustwa, malwersacje, łapownictwo czy pranie brudnych pieniędzy – zniszczyły lub nadszarpnęły reputację wielu wartościowych dla akcjonariuszy firm, np. Alstom, Odebrecht, Petrobras, Rolls-Royce, Siemens, Telia, Teva Pharmaceutical, VimpelCom, Volkswagen i wielu innych. Ich łączne straty są szacowane na miliardy dolarów. Kary prawne, jakie ponoszą przedsiębiorstwa, mogą być znaczne: Siemens otrzymał 1,6 mld dolarów grzywny, Odebrecht – 3,5 mld dolarów, a Volkswagen – ok. 20 mld dolarów. Są też koszty biznesowe: czas i energia, jakie kierownictwo musiało poświęcić na sprzątanie bałaganu i negocjowanie ugody, a nie na pokonywanie rywali; szkody dla reputacji; wpływ na sprzedaż, zyski i cenę akcji; spadek zaangażowania i wydajności pracowników; zwiększenie rotacji pracowników. Badania przeprowadzone m.in. przez Jonathana Karpoffa z Uniwersytetu Waszyngtońskiego wskazują, że dochodzą do tego dodatkowe kary nakładane przez sądy w innych, będących skutkiem skandali, procesach.

Dlaczego zatem ludziom wciąż się wydaje, że nieuczciwość może się opłacać? W odpowiedzi na głośne przypadki i rosnące zaniepokojenie opinii publicznej organy regulacyjne w USA i innych krajach zażądały od przedsiębiorstw zwiększenia wysiłków na rzecz zapobiegania nadużyciom. W rezultacie prawie każda firma międzynarodowa inwestuje znaczne środki w przestrzeganie przepisów i popiera zasadę zerowej tolerancji dla nielegalnego zachowania pracowników. Mimo zaostrzonych regulacji i zwiększonych kontroli przestępstwa popełniane przez pracowników i menedżerów niestety nie zmalały, wręcz przeciwnie – wciąż rosną. W badaniu PwC z 2018 r. aż 49% spośród 7228 organizacji stwierdziło, że w poprzednim roku doświadczyło przestępstw gospodarczych i nadużyć finansowych (w porównaniu z 30% w badaniu z 2009 r.), a ponad połowa to „sprawcy wewnętrzni". Opowieści o przestępstwach na stanowiskach kierowniczych zapełniają ostatnio szpalty gazet. Niektóre zarzuty są coraz poważniejsze, np. pracownicy Goldman Sachs byli zamieszani w wielomiliardowe oszustwa w Malezji, Deutsche Bank pomagał klientom w przekazywaniu pieniędzy z działalności przestępczej do rajów podatkowych, Dunske Bank był zamieszany w pranie rosyjskich pieniędzy, a Airbus angażował się w korupcyjne praktyki zawierania umów.

Jest tego coraz więcej, ale dlaczego?

Po setkach rozmów z wieloma klientami, po przeczytaniu wielu analiz z pełną odpowiedzialnością mogę stwierdzić, iż główną przyczyną problemu nie są nieefektywne regulacje i systemy zgodności. Za taki stan rzeczy odpowiada przede wszystkim słabe przywództwo i wadliwa kultura korporacyjna. Człowiek, zwłaszcza gdy decyduje o kierunkach działania, skuszony wizją potężnych zysków i osobistych korzyści, potrafi „umotywować" działania, które finansowo mogą pogrążyć udziałowców i czasami nieświadomych właścicieli firm.

Firmy dotknięte poważnymi skandalami miały podobne mechanizmy kontroli jak konkurencja i podobnie jak Wells Fargo otrzymywały sygnały wczesnego ostrzegania o zbliżających się problemach. W każdej z nich kultura tworzenia statystyk i wyników, dążenie do zysku za wszelką cenę przewyższało obawy o metody osiągania wyznaczonych celów, a dla menedżerów oznaczało zadanie, które za wszelką cenę trzeba zrealizować.

Badając w ostatnich 10 latach przestępczość na stanowiskach kierowniczych i analizując, czy firmy mogłyby stworzyć środowisko, które je do nieetycznego zachowania zniechęca, wykorzystano dane pochodzące z poszczególnych firm oraz badań przeprowadzonych przez PwC, EY czy Transparency International (organizację pozarządową założoną w 1993 r. do zwalczania korupcji), Bank Światowy, firmy rekrutacyjne i inne. Dziennikarze „Harvard Business Review" przeanalizowali dane dotyczące tysięcy organizacji i osób fizycznych. Przeprowadzili wywiady z ponad 50 mene-

> Kultura tworzenia statystyk i realizacji wyników przeważyła nad wszelkimi obawami dotyczącymi sposobu osiągnięcia celów

dżerami wyższego i średniego szczebla w 10 organizacjach, które doświadczyły skandali. W trakcie badań wielokrotnie przekonali się, że chociaż systemy zgodności odgrywają ważną rolę, przywództwo jest kluczowe w kształtowaniu postaw organizacji wobec zapobiegania przestępczości i jej reakcji w przypadku wykrycia nadużyć. Zbyt często kadra kierownicza ucieka od odpowiedzialności, zwalnia się z ponoszenia konsekwencji różnych zaniechań albo wprost nie chce ich dostrzegać. Okazało się, że kadra kierownicza wyższego szczebla w większości firm, które ucierpiały na skutek nagłośnionych afer, nie postrzegała tych incydentów jako osobistej odpowiedzialności za zajęcie się problemem. Nie uznała ich także za dowód na to, że coś było nie w porządku w ich organizacjach.

Postrzegała je raczej jako niezwykle rzadkie zdarzenia spowodowane przez „kilka zatrutych owoców", którym nie można było zapobiec. Akceptując konieczność inwestowania w systemy zgodności i oczekując od pracowników uczciwości, zazwyczaj za priorytety uważała osiąganie lepszych niż konkurencja wyników i zaspokajanie oczekiwań inwestorów, nieegzekwujących wysokich standardów prawnych i etycznych. Co gorsza, zbyt wielu właścicieli i nadzorców przeoczyło wątpliwe praktyki biznesowe lub wykazało się pobłażliwością wobec członków ich przestarzałych struktur, których przyłapano na przestępstwach.

Zarządzający biznesem muszą też poważnie traktować wszelkie obawy zgłaszane przez pracowników o możliwości nadużyć i presji związanej z wynikami. Niedopełnienie tego obowiązku zwiększa prawdopodobieństwo, że nawet ci uczciwi będą niejako zmuszeni do tolerowania wykroczeń lub uczestniczenia w nich. Zlecony przez zarząd audyt po skandalu w Wells Fargo wykazał, że Carrie Tolstedt, która kierowała jednostką detaliczną od 2007 r., nie lubiła, gdy kwestionowano jej decyzje. Stosowała mobbing nawet wobec starszych menedżerów. John Stumpf, dyrektor generalny banku macierzystego, zignorował obawy związane z niewłaściwym postępowaniem w bankowości detalicznej, zgłoszone już w 2002 r. i ponownie w 2004 r. oraz w latach 2012–2014. Kiedy w 2013 r. ukazały się krytyczne artykuły w „Los Angeles Times", J. Stumpf (i zarząd) nie zbadali zarzutów. I chociaż doniesienia o niewłaściwym postępowaniu pod rządami C. Tolstedt były uporczywe, Stumpf nadal ją wspierał, nawet wtedy, gdy główny niezależny dyrektor Wells Fargo i przewodniczący komisji ds. ryzyka zarządu zasugerowali jej zwolnienie pod koniec 2015 r.

Kluczowe znaczenie ma zapewnienie skutecznego działania programów informujących o nieprawidłowościach (*whistleblowing*). Badania przeprowadzone przez Eugene'a Soltesa wykazały, że 20% infolinii dla zgłaszających nieprawidłowości nie funkcjonuje prawidłowo, a organizacje mające słabą kontrolę wewnętrzną nie pozwalają zgłaszającym na zachowanie anonimowości. Powinno się ich hojnie wynagradzać lub przynajmniej chronić, ponieważ mają odwagę przerwać zmowę milczenia nt. nadużyć, a przecież to oni ponoszą wysokie koszty: utratę relacji, stres, trudności w znalezieniu pracy.

Zaczyna się od tego: przekaż wszystkim komunikat, że przestępstwo się nie opłaca

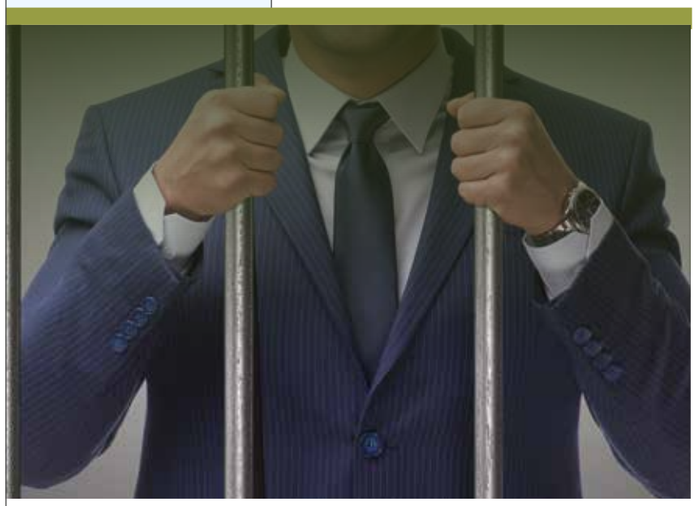
Każdy cierpi

Liderzy, którzy skutecznie zwalczają nieetyczne zachowania pracowników, są głęboko zaangażowani w ustalanie norm społecznych w swoich firmach i zarządzanie ryzykiem niewłaściwego postępowania. Czynią to, przekazując jasny komunikat, że przestępczość szkodzi wszystkim w organizacji. Nie robią wyjątków, kiedy karzą sprawców. Rekrutują i promują menedżerów ceniących sobie uczciwość, a także tworzą procesy decyzyjne, które ograniczają możliwość popełnienia czynów nielegalnych lub nieetycznych. Dokładają wszelkich starań, aby ich transakcje w skorumpowanych krajach były przejrzyste, są proaktywni, gdy chodzi o zwalczanie nieetycznych praktyk, wspierają instytucje społeczne, które wzmacniają odpowiedzialność korporacyjną i uczciwe zachowanie biznesowe.

Może zabrzmi to jak odkrycie, ale doświadczenia i praktyka w zderzeniu z licznymi badaniami i analizami mówią jasno: biznes prowadzony w sposób nielegalny wnosi niewiele lub nic do wyniku finansowego, a ludzie w firmie – nie tylko sprawcy, ale także ich przełożeni i prezes cierpią, gdy przestępstwo zostaje ujawnione. Funkcjonowanie z obciążeniem, że robiliśmy coś nie tak i to może wyjść na jaw, powoduje rosnący paraliż obaw, rodzi kolejne patologie i straty. Osoby odpowiedzialne za biznes powinny to wiedzieć!

Przywódcy międzynarodowych koncernów twierdzą publicznie, że ich firmy nie tolerują korupcji.

Ale fakty tego nie potwierdzają. Siemens i SNC-Lavalin, firmy inżynieryjne i budowlane, które w ostatnich 12 latach zostały oskarżone o przekupstwo w krajach



rozwijających się, gdzie przepisy antykorupcyjne nie są właściwie egzekwowane. Ich kierownictwo ujawniło, że audyty pokazały, iż zyski z transakcji związanych z nielegalnymi płatnościami były nieoczekiwanie niskie, w dużej mierze z powodu znacznych kosztów łapówek (aż 10% wartości kontraktu). Doświadczenia tych firm wydają się regułą, nie zaś wyjątkiem. Przyjrzano się finansom 480 przedsiębiorstw międzynarodowych, które w 2006 r. zostały ocenione przez Transparency International pod kątem stosowanych systemów antykorupcyjnych i działań ujawnionych w ich rocznych raportach i na ich stronach internetowych. Porównując wyniki z okresu 2007–2010, firmy w regionach słabo uregulowanych odnotowały o 5% wyższy roczny wzrost sprzedaży niż te o dobrym ratingu. Firmy międzynarodowe o słabej ocenie wiarygodności kredytowej odnotowały też niższą rentowność wzrostu sprzedaży w regionach słabo regulowanych niż ich wysoko oceniani odpowiednicy. Różnice w rentowności były porównywalne pod względem wartości do łapówek wypłacanych zazwyczaj w tych regionach.

Dodatkowy wzrost sprzedaży generowany przez nielegalnie pozyskany biznes nie zwiększa wartości również dla akcjonariuszy nawet, gdy łapówki nie zostaną ujawnione, co odkryli dziennikarze z „Harvard Business Review". W przypadku ujawnienia praktyk korupcyjnych cierpi reputacja firmy, a kurs jej akcji spada. To nie jest małe ryzyko: analizując dane z lat 2007–2010, stwierdzono, że prawdopodobieństwo medialnego skandalu jest o 28% większe w przypadku firm o słabych ocenach antykorupcyjnych. Jak pokazuje historia, utrata reputacji zdecydowanie obniża wiarygodność firmy i powoduje, że klienci zaczynają jej unikać. Sprawcy przestępstw, którzy są karani, płacą cenę i finansowo, i zawodowo. Ale szkody ponoszą też pracownicy, którzy nie mieli nic wspólnego z przestępstwem. Przebadano ponad 2000 menedżerów wyższego szczebla (dyrektorów i liderów jednostek biznesowych), którzy zmienili pracodawców oskarżanych o skandale kryminalne. Okazało się, że u nowych otrzymywali wynagrodzenie prawie o 4% niższe niż inni. Różnice w zarobkach nawet tych, którzy opuścili firmę przed skandalem i byli z aferami niezwiązani, utrzymywały się przez lata. Koszty tego piętna były większe dla kadry kierowniczej wyższego szczebla (różnica 6,5% w płacy rocznej), dla kobiet (7%) oraz w krajach o silnych systemach regulacji i zarządzania (6%). Wiele osób w swoich CV nie wpisuje nawet kilkuletniego zatrudnienia w firmach, które straciły reputację w wyniku afer. Przykładem w Polsce są zatrudnieni w Amber Gold – próżno szukać informacji o tym w ich CV.

Dane te powinny wiele osób skłonić do przemyślenia, czy tolerowanie nagannych działań w firmie jest opłacalne. Kluczowe znaczenie ma zapewnienie skutecznego działania programów informujących o nieprawidłowościach.

Nie chroń swoich

Pracownikom trzeba dawać jasny przekaz, że pewnych zachowań nie będzie się tolerowało. Kierownictwo firm, w których zostały wykryte poważne afery, nie ustaliło wyraźnych granic między akceptowalnymi a niedopuszczalnymi praktykami handlowców i partnerów biznesowych działających w skorumpowanych krajach. Według jednego z dyrektorów Siemensa pracownicy otrzymali od swoich menedżerów następujące przesłanie: „Załatw interes – nie muszę wiedzieć, jak to zrobisz".

Inne kroki podjął duży producent farmaceutyków, który doświadczył oszustwa wewnętrznego, aby przedstawić swoje stanowisko w sprawie takiego zachowania. Zlecił dziennikarzom Harvard Business School napisanie pracy dotyczącej tego incydentu i korzystał z niej podczas własnych sesji szkoleniowych, pomagając menedżerom w zdiagnozowaniu przyczyn problemu i sposobów zapobiegania incydentom.

Brak tolerancji dla fraudów wymaga poświęcenia. Należy zdecydowanie reagować na przestępstwa, zwalniając sprawców i podejmując działania prawne przeciwko każdemu na jednakowych zasadach. Jak pokazuje życie i historie przytoczonych afer, z tym bywa różnie. I to powstrzymuje decydentów w firmach przed działaniem – o ile łatwiej podejmować restrykcyjne działania wobec nieznanych szerzej pracowników czy menedżerów, o wiele trudniej, gdy jest to ktoś bliski i zaufany. Siemens menedżerom przyłapanym na płaceniu łapówek we Włoszech zezwolił przejść na emeryturę i wypłacił 1,6 mln dolarów odszkodowania odchodzącemu dyrektorowi finansowemu odpowiedzialnemu za nadzorowanie kontraktu. Taka pobłażliwość w traktowaniu sprawców nie jest rzadka – dziś w prasie jest głośno o ujawnianych przez ruch Me Too skandalach związanych z molestowaniem seksualnym czy skandalach pedofilskich w Kościele katolickim. Osoby nadzorujące daną instytucję usiłują chronić sprawców, a nie pomagać ofiarom.

Chcąc zrozumieć, dlaczego w biznesie taka pobłażliwość jest wszechobecna, przeanalizowano kary, jakie firmy wymierzały sprawcom przestępstw „białych kołnierzyków". Oparto się na danych z badania PwC, w którym pytano firmy o ich doświadczenia z przestępczością w 2011 r., m.in. o dane dotyczące charakteru przestępstw, kar i demografii głównych sprawców. Spośród 3877 firm, które udzieliły odpowiedzi, 608 zgłosiło wykrycie przestępstw popełnionych przez pracowników w tym samym roku. Stwierdzono, że 42% głównych sprawców zostało zwolnionych lub opuściło organizację i stanęło przed sądem, 46% zwolniono bez postępowania sądowego, a 13% pozostało w organizacji (z przeniesieniem albo ukaraniem lub bez takich działań). Niski wskaźnik działań prawnych przeciwko sprawcom najprawdopodobniej odzwierciedla praktyczne wyzwania związane ze ściganiem przestępstw „białych kołnierzyków". Dowody na to, że dana osoba dopuściła się czynu, nie są wystarczające; muszą być również dowody, że zamierzała go popełnić lub wiedziała o popełnieniu czynu niedozwolonego. Biorąc pod uwagę potencjalne kary i ryzyko utraty reputacji przez firmę, prawnicy korporacyjni często doradzają kadrze zarządzającej, by sprawców zwalniać po cichu, bez podejmowania jakichkolwiek działań prawnych.

Łagodne traktowanie sprawia, że do potencjalnych sprawców wysyłany jest komunikat, że przestępstwo może się opłacać lub nie jest zbyt ryzykowne. Obniża tym samym morale uczciwych pracowników, którzy w firmach nękanych taką przestępczością wyrażają swoją frustrację z tego powodu. Było też powodem fermentu w firmach lub doprowadzało do odejścia z pracy.

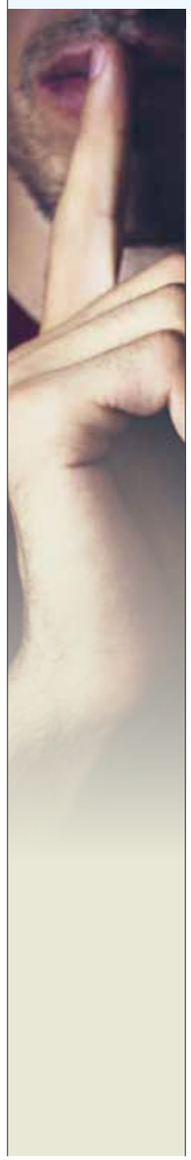
Innym niepokojącym faktem jest to, że sprawcy, którzy byli młodszymi menedżerami lub pracownikami, byli o 24% częściej narażeni na działania prawne i zwolnienia niż kierownicy wyższego szczebla, którzy częściej otrzymywali kary lub wewnętrzne przeniesienia bez zwolnienia z pracy. Kierownicy wyższego szczebla są niechętnie zwalniani ze względu na ich relacje z klientami lub obawy, że trudno będzie zastąpić ich wiedzę specjalistyczną. To błędne podejście, gdyż uruchomiony proces sprawia, że zły przykład i ferment tworzą kolejne patologie, ogarniając powoli całą firmę. Tylko kwestią czasu będzie kolejna afera, która nadszarpnie reputację firmy. Praktyka pokazuje, że brak podejmowania działań uzdrawiających i naprawczych szkodzi i generuje kolejne straty.

Oczywistym środkiem zaradczym jest stworzenie i wymuszenie na drodze uświadamiania polityki równego karania wszystkich. Tak właśnie zrobił Erik Osmundsen w Norsk Gjenvinning (NG), norweskiej firmie zajmującej się gospodarką odpadami. Wkrótce po mianowaniu go na stanowisko prezesa zarządu rozpoczął działania mające na celu ukrócenie i wyeliminowanie powszechnych oszustw, kradzieży i korupcji w firmie. Opracował zestaw wartości i zachowania odpowiedzialnego przedsiębiorcy, który nie idzie na skróty i gra zespołowo zarówno w firmie, jak i w społeczeństwie. Wartości te zostały przełożone na konkretne kodeksy postępowania w odniesieniu do każdego stanowiska w firmie – na ich przestrzeganie każdy pracownik musiał wyrazić zgodę. Następnie firma wdrożyła 4-tygodniowy okres amnestii, podczas którego pracownicy mogli wyznać wykroczenia, które popełnili lub których byli świadkami. W ciągu 18 miesięcy blisko 170 dyrektorów (blisko połowa wszystkich menedżerów) opuściło firmę – zdecydowana większość kadry postanowiła sama odejść, niewielka część została zwolniona.

Aby zmienić kulturę firmy nękanej przestępczością systemową, należy wprowadzić nowych, uczciwych liderów. Jeśli w branży panuje korupcja, konieczne może się okazać zatrudnienie kadry kierowniczej z innej branży, która będzie miała inną perspektywę i prawdopodobnie zachwieje status quo. Przykładem może być Siemens. Klausa Kleinfelda, który ustąpił ze stanowiska dyrektora generalnego podczas dochodzenia w sprawie przekupstwa, zastąpił Peter Löscher, dyrektor wykonawczy z branży farmaceutycznej. Jednym z kluczowych argumentów za nominacją Löschera, cytowanym w komunikacie prasowym (co jest rzadko praktykowane) był „jego uczciwy charakter". Dostrzegając wyzwania związane ze zmianą kultury w firmie Siemens, P. Löscher zatrudnił kilku starszych menedżerów, z którymi wcześniej pracował i których znał jako ludzi o wysokiej uczciwości. Wśród nich byli Andreas Pohlmann, dyrektor ds. zgodności, oraz Peter Solmssen, główny radca prawny i członek zarządu. Obaj mężczyźni oraz Barbara Kux, która zasiadła w zarządzie jako dyrektor ds. zrównoważonego rozwoju, odegrali kluczową rolę w opracowaniu planu rozwiązania problemów w firmie i zreformowania jej kultury. Dzisiaj Siemens to firma, której reputacja i zaufanie klientów rośnie, osiągając coraz wyższe zyski.

Ponieważ problemy norweskiej NG były endemiczne (charakterystyczne) dla branży gospodarki odpadami, jej nowy prezes E. Osmundsen również zdecydował się na pozyskiwanie świeżej krwi spoza niej (z branż budowlanej, handlu aluminium, handlu detalicznego, ropy

> Biznes prowadzony w sposób nielegalny wnosi niewiele lub nic do wyniku finansowego, a ludzie w firmie – nie tylko sprawcy, ale także ich przełożeni i prezes cierpią, gdy przestępstwo zostaje ujawnione



naftowej i gazu oraz firm produkujących napoje bezalkoholowe). Przekonał ludzi, aby przyłączyli się do jego wizji uczynienia z NG modelowej firmy ekologicznej – takiej, która dzięki innowacyjnemu podejściu do gospodarki odpadami mogłaby odegrać znaczącą rolę w promowaniu zrównoważonego rozwoju środowiska naturalnego. W pierwszym, krótkim okresie fluktuacja pracowników miała negatywny wpływ na wyniki finansowe, jednak w ciągu trzech lat firma odzyskała równowagę finansową. Obecnie to już zupełnie inna firma.

Wymóg podejmowania trudnych decyzji przez grupy pracowników

Jak opisuje HBR, kiedy Statoil – norweska spółka energetyczna (niedawno przemianowana na Equinor) – rozpoczęła intensywną działalność na rynku w Angoli, kierownictwo i zarząd uznały, że jej pracownicy będą zmuszeni płacić tam łapówki. (Transparency International sklasyfikowała Angolę jako jeden z najbardziej skorumpowanych krajów). Aby zmniejszyć prawdopodobieństwo poddania się tej presji, liderzy firmy nakazali pracownikom, by podejmowali decyzje zespołowo. Było to bezpośrednim wynikiem doświadczeń Statoil w Iranie – w 2004 i 2006 r. firma zgodziła się zapłacić kary finansowe w Norwegii i USA za przekupienie urzędnika państwowego w celu zabezpieczenia kontraktu w Iranie (chociaż Statoil nie przyznał się ani nie zaprzeczył swojej winie). Z tego skandalu wyciągnięto wniosek, że pracownicy są bardziej skłonni iść na skróty i postępować nieetycznie, gdy sami podejmują działania.

Podejmowanie trudnych decyzji w grupie wymaga otwartej i uczciwej dyskusji, a to nie dzieje się automatycznie. Pracownicy muszą ufać, że inni członkowie grupy z zaangażowaniem wysłuchają ich opinii i docenią je, a liderzy firmy będą wspierać decyzje grupy, nawet gdyby miały mieć negatywne konsekwencje finansowe. Jeśli liderzy nie wzbudzają takiego zaufania, jest mało prawdopodobne, że przekazanie decyzji grupom rozwiąże problem. Badania przeprowadzone na Harvardzie przez Amy Edmondson wykazały, że aby stworzyć klimat bezpieczeństwa psychicznego, potrzebne jest silne przywództwo. Liderzy muszą aktywnie promować zachowania, jakich oczekują w całej organizacji – pokazując, że można np. zadawać trudne pytania i wyrażać odmienne poglądy, czy upoważniając pracowników z pierwszej linii do szczerego mówienia swoim przełożonym o oznakach potencjalnych problemów lub błędach popełnionych przez organizację i otwartego omawiania ich, a także szanując brak wiedzy na dany temat.

Lider transparentności

Po ujawnieniu przekupstwa przez firmę Statoil Helge Lund, ówczesny nowy dyrektor generalny, zdecydował, że spółka jako jedna z pierwszych w branży wydobywczej ujawni publicznie płatności dokonane na rzecz zagranicznych rządów w celu uzyskania tam dostępu do zasobów naturalnych. Za taką praktyką od dawna opowiadały się organy regulacyjne i grupy interesu publicznego. Pracownikom wysłano wyraźny sygnał, że stare sposoby prowadzenia działalności gospodarczej nie będą już w firmie tolerowane.

Wspieranie instytucji badających i raportujących korupcję to kolejny sposób, w jaki kierownictwo może pokazać pracownikom, że poważnie podchodzi do prowadzenia działalności gospodarczej w sposób etyczny. Organizacje te promują uczciwą konkurencję i przekonują opinię publiczną, że przestępstwa biznesowe są wykrywane i karane. A ograniczając korupcję, stymulują rozwój gospodarczy.
Statoil jest jednym z pierwszych członków Inicjatywy Przejrzystości w Branżach Wydobywczych (EITI), skupiających

> Pracownicy są mniej skłonni do nieetycznego postępowania, gdy decyzje podejmują zespołowo

firmy, rządy i organizacje pozarządowe w celu ograniczenia korupcji w krajach bogatych w zasoby oraz zwiększenia przejrzystości w zakresie płatności dokonywanych przez przedsiębiorstwa naftowe, gazowe i górnicze w tych krajach. Wczesne sprawozdania EITI dostarczały zbiorczych informacji o płatnościach przedsiębiorstw i dochodach krajowych, najnowsze często zawierają już informacje szczegółowe. Badania empiryczne, analizujące dane ze 186 krajów w ciągu ponad 10 lat sugerują, że w krajach, które przekazują raporty EITI, nastąpił znaczny spadek korupcji, zwłaszcza tych, gdzie jej poziom był wysoki.

P. Löscher i P. Solmssen z Siemensa zwrócili się do konkurentów, rządów, organizacji pozarządowych i innych grup interesariuszy, aby przedstawić argumenty przemawiające za szerszą reformą. W 2009 r. w ramach ugody z Bankiem Światowym za swoje wcześniejsze przewinienia firma zgodziła się wydać 100 mln dolarów w ciągu 15 lat na wsparcie organizacji i projektów zwalczających korupcję poprzez działania zbiorowe, edukację i szkolenia. Do końca 2017 r. Siemens zarobił 73 mln dolarów w postaci dotacji na 55 projektów. Został też członkiem Partnering Against Corruption Initiative (PACI) – Światowego Forum Ekonomicznego, w którego skład wchodzi 87 dużych firm.
Na całym świecie powstają kolejne programy zwalczające nieuczciwość w biznesie, które uzdrawiając środowisko biznesowe, eliminują z niego tych, którzy swoimi działaniami psują rynek i branżę.
Trzeba mieć świadomość, że w dużych organizacjach i firmach błędy będą popełniane. Ale tworząc kulturę zachęcającą pracowników do działania w sposób etyczny i zgodny z prawem, liderzy mogą zminimalizować prawdopodobieństwo, że skandal uderzy w ich firmę. Mogą też zwiększyć jej zdolność do niedopuszczania do nielegalnych działań. Aby nadać właściwy ton, muszą modelować wysokie standardy w życiu zarówno zawodowym, jak i osobistym.
Wielu pracowników, którzy zdecydowali się pracować w firmach o wysokim poziomie integracji w krajach i branżach wysokiego ryzyka, postąpiło tak ze względu na renomę tych firm. Niektórzy akceptują niższe płace, chwaląc dobrą atmosferę w pracy. Takie firmy i ich liderzy cieszą się szacunkiem klientów, organów regulacyjnych i społeczności. Bardziej prawdopodobne jest, że będą dobrze prosperować i przetrwają na często agresywnych rynkach. □

BIO

Michał Czuma

Niezależny ekspert, prowadzący obecnie własną działalność doradczą. Stworzył i zarządzał pierwszymi w kraju Biurami Antyfraudowymi w spółkach grupy PKO Banku Polskiego. Były wieloletni z-ca dyrektora Departamentu Bezpieczeństwa PKO Banku Polskiego.

TO PIĄTY Z SERII ARTYKUŁÓW O BEZPIECZEŃSTWIE. INSPIRACJI DO POWSTANIA CYKLU DOSTARCZYŁ PORADNIK JACKA PAŁKIEWICZA „DŻUNGLA MIASTA. KLUCZ DO BEZPIECZEŃSTWA". NA ŁAMACH „A&S POLSKA" PARTNERUJE MU WIELOLETNI PRAKTYK ZARZĄDZANIA BEZPIECZEŃSTWEM JACEK TYBUREK. WSPÓLNIE PRZEDSTAWIAJĄ SWÓJ PUNKT WIDZENIA NA BEZPIECZEŃSTWO W RÓŻNYCH JEGO ASPEKTACH.

Postęp postępem, ale architektura musi być nasza

czyli dlaczego architektura jest niezmiennie strażnikiem bezpieczeństwa mieszczan

Kolejną część serii „Dżungli Miasta wg Jacka & Jacka" rozpocznie opowieść o skrajnie niedżunglowym temacie. Chodzi o rolę architektury nie tyle tej rozumianej jako bryły budynków czy urbanistyka nadająca kształt życiu publicznemu w mieście, ile o znaczenie i przydatność elementów tzw. małej architektury miejskiej. Inspiracją cyklu „Dżungla miasta wg Jacka & Jacka" jest książka Jacka Pałkiewicza. W tym odcinku opieram się również na książce Artura Jasińskiego „Architektura w czasach terroryzmu. Miasto – przestrzeń publiczna – budynek".

Główną funkcją miasta, a wcześniej domów była ochrona – przed zimnem, upałem, wodą, najeźdźcami, przestępcami. Bezpieczeństwo zapewniała wspólnota jej mieszkańców. Do tego celu dawni budowniczowie wykorzystywali naturalne ukształtowanie terenu: rzeki, skały, wzniesienia i inne naturalne bariery, a także sypali obwałowania, kopali fosy i wznosili mury. To właśnie mury stały się funkcjonalnym i symbolicznym wyznacznikiem miasta – pojęcie *intra muros* było synonimem wspólnoty miejskiej. Fortyfikacje miały za zadanie powstrzymanie napastnika, utrudnienie mu ataku, wystawienie go na skuteczny odwet broniących się.
W klasycznej już definicji miasta autorstwa Maxa Webera fortyfikacje były jednym z jego pięciu podstawowych atrybutów. Pozostałe to rynek, własny sąd, stowarzyszenia, częściowa autonomia. W czasach nam bliskich najnowszą koncepcją wykorzystania planowania urbanistycznego i architektury w celu poprawy bezpieczeństwa było CPTED, czyli *Crime Prevention through Environmental Design* (prewencja kryminalna przez kształtowanie przestrzeni).
Amerykański kryminolog C. Ray Jeffrey przedstawił psychologiczne i środowiskowe uwarunkowania przestępczości, wskazując na związki pomiędzy zachowaniem przestępcy a stanem środowiska, w jakim on przebywa, może ono bowiem stymulować lub ograniczać jego wolę popełnienia przestępstwa. Zauważył on, że być może łatwiej niż resocjalizować i zmieniać przestępcę jest oddziaływać na jego zachowania, tworząc środowisko o określonych cechach, które będzie zniechęcać go do popełnienia przestępstwa, utrudniać je i wzmacniać jego przekonanie o wysokim ryzyku i możliwej karze. Pisał, że właściwy projekt i efektywne wykorzystanie środowiska zbudowanego może prowadzić nie tylko do ograniczenia strachu i redukcji zagrożenia przestępczością, ale wręcz podnieść jakości życia.
Początkowo głównym założeniem programu było takie kształtowanie układu urbanistycznego, aby obserwacja miejsc „trudnych" z punktu widzenia zagrożeń kryminalnych była maksymalnie ułatwiona. Pamiętajmy, że przypominamy sobie XX wiek, jego drugą połowę, lata 70. i 80. Ale to jednak poprzedni wiek! Systemy CCTV dopiero raczkują, kosztują majątek i są raczej ciekawostką technologiczną niż realnym narzędziem.

7 GŁÓWNYCH ZASAD KONCEPCJI CPTED

1. Wspieranie kontaktów międzyludzkich, zwiększanie wzajemnej czujności oraz wspieranie działań służących delimitacji terytorialnej i kontroli sąsiedzkiej (terytorialność).
2. Maksymalizacja zdolności lokalizowania podejrzanych osób lub działań (punkty obserwacyjne).
3. Wspieranie przemyślanych sposobów wykorzystania przestrzeni przez mieszkańców (wspieranie aktywności).
4. Identyfikacja właścicieli przestrzeni prywatnych i publicznych oraz realne lub symboliczne rozgraniczenie tych przestrzeni (hierarchia przestrzeni).
5. Wykorzystanie barier, zabezpieczeń i innych sposobów ograniczających swobodę dostępu (kontrola dostępu).
6. Minimalizowanie możliwości powstawania konfliktów przez projektowanie odpowiedniej lokalizacji grup użytkowników (środowisko).
7. Dbałość o czystość i stan środowiska, budynków i obszarów (konserwacja).

Betonowe zapory drogowe (*Jersey barriers*)

Cele strategiczne programu koncentrowały się natomiast wokół czterech zasad

1. Kontrola dostępu *(natural access control)* – zróżnicowane strategie kontroli dostępu: ochrona fizyczna (strażnicy); mechaniczna (bramy i zamki); naturalna (granice zdefiniowane przestrzennie) ograniczające potencjalnemu przestępcy dostęp do celu i zwiększające prawdopodobieństwo ujęcia sprawcy.

2. Zapewnienie naturalnego nadzoru *(natural surveillance)* – ułatwienie użytkownikom lub mieszkańcom obserwacji terenu wokół obiektu, dojść i wejść zarówno z wnętrza, jak i z ulicy. Celem jest odstraszanie potencjalnych napastników, zwiększa szansę wykrycia przestępstwa i ujęcia sprawcy.

3. Wzmocnienie terytorialne *(territorial reinforcement)* – tworzenie i poszerzanie strefy wpływu mieszkańców i użytkowników w celu spowodowania wrażenia przynależności do danej własności terytorialnej. Temu celowi mogą służyć elementy małej architektury: ławki, oświetlenie, nawierzchnie i odpowiednie oznakowanie. Tak zorganizowana przestrzeń sygnalizuje, że należy do stałych użytkowników, a niewłaściwe zachowania nie będą tu tolerowane.

4. Wzmocnienie i utwardzenie potencjalnych celów *(target hardening)* – zabezpieczenie ich środkami planistycznymi, technicznymi i elektronicznymi.

Podobnie jak wiele aspektów zarządzania bezpieczeństwem publicznym, biznesowym i państwowym, wszystko zmieniło się po 11 września 2001 r.. Nagle zauważono, że liberalne założenia otwartości miast, przynajmniej tych o wielkim znaczeniu politycznym, stanowiących ikony współczesnej kultury należy zabezpieczać zupełnie nienowoczesnymi metodami. Na Manhattanie natychmiast wprowadzono zabezpieczenia i bariery, których zadaniem było ułatwienie pracy służbom bezpieczeństwa publicznego oraz utrudnienie kolejnych potencjalnych zamachów antyterrorystycznych. Przy wszystkich mostach i tunelach ustawiono stałe posterunki policji. Za bardzo ważny dla terrorystów cel uznano gmach nowojorskiej giełdy i niebawem na obu krańcach Wall Street i innych przyległych do niej ulic rozstawiono posterunki kontrolne i bariery utworzone z betonowych elementów prefabrykowanych, przenośnych stalowych ogrodzeń (tzw. *French barricades*) i furgonetek wyładowanych piaskiem, pełniących funkcję przesuwnych bram. Naprędce fortyfikowano także najważniejsze budynki administracyjne i biurowe.
Wyjątkową cechą nowojorskich, wznoszonych ad hoc zabezpieczeń były prefabrykowane betonowe zapory drogowe (*Jersey barriers*) ustawiane bezpośrednio przed wejściami do budynków, na krawędziach chodników, równolegle do jezdni. Miały powstrzymać samochód z ładunkiem wybuchowym przed wtargnięciem do wnętrza budynku, gdzie eksplozja mogłaby przynieść katastrofalne skutki. Przed małymi bądź zabytkowymi budynkami nie stawiano takich barier, jednak wkrótce większość dużych korporacyjnych biurowców na Manhattanie została otoczona rzędami betonowych zapór. Skala tymczasowych zabezpieczeń określała wręcz rangę instytucji. Środki te, uzasadnione w sytuacji szokowej dla mieszkańców Nowego Jorku i Waszyngtonu, musiano z czasem przepracować w kierunku rozwiązań bardziej systemowych, mniej spontanicznych i przypadkowych.

Elementy małej architektury stanowiące betonową zaporę

Dość szybko okazało się, że pamięć o ofiarach zamachu jest żywa, ale zabezpieczenia stosowane przesadnie stają się dla mieszkańców uciążliwe. Dziennikarka „New York Timesa", Joyce Purnick, ustawiane na nowojorskich ulicach betonowe bariery określiła jako nieeleganckie, nieefektywne i niedrożne. Opisuje, jak przed reprezentacyjnym kompleksem Lincoln Center, stanowiącym siedzibę nowojorskiej filharmonii i opery, ustawiono rzędy betonowych prefabrykatów przyozdobionych plastikowymi doniczkami. Bariery rozpleniły się wszędzie, stały się „miejską zarazą". Autorka cytuje ekspertów bezpieczeństwa, którzy twierdzą, że betonowe zapory drogowe tzw. *Jersey barriers* – czy to swobodnie ustawione na podłożu, czy do niego solidnie przytwierdzone – nie gwarantują pełnego bezpieczeństwa, gdyż, jak dowiodły testy, mogą zostać sforsowane przez zwykłego forda fiestę.
Dziennikarka określa wznoszone *ad hoc* bariery mianem placebo, dającym ludziom pozory bezpieczeństwa. Tymczasem eksperci ds. bezpieczeństwa zalecają każdorazowo wykonanie analizy ryzyka oraz dobranie poziomu i sposobu zabezpieczeń do kontekstu i okoliczności.

Cofając się w historycznych praktykach związanych z fortyfikowaniem centrów współczesnych miast, nie da się pominąć koncepcji *ring of steel*. Powstała ona pierwotnie jako odpowiedź władz brytyjskich na akcje IRA w Belfaście, swoją nazwę zawdzięczała systemowi drutów kolczastych i zapór stalowych regulujących i reglamentujących ruch wokół kluczowych obszarów Belfastu i innych miast Irlandii Północnej. Stopniowo model ten był przenoszony do Londynu, gdzie wraz z rozpowszechnianiem się zabezpieczeń elektronicznych (takich jak CCTV) były one włączane do systemu. Zatem już w latach 90. w Londynie rozpoczęto prace nad budową współczesnych barier i fortyfikacji mających wzmocnić bezpieczeństwo obywateli i kraju. Nowy model *Ring of Steel London*, co symptomatyczne dla stolicy Zjednoczonego Królestwa, zabezpieczał prawdziwe „klejnoty koronne", czyli londyńskie City. Ta dzielnica finansowa została wyposażona w system doskonale funkcjonujących podsystemów CCTV połączonych z zabezpieczeniami mechanicznymi oraz systemem zapór.

Rozwój rynku ma napędzać integracja systemów i wykorzystanie nowych, zaawansowanych technologii. Analitycy wskazują zwłaszcza na postęp, jaki dokonuje się w detektorach, technologiach bezprzewodowych i radarach

Automatyczne blokady antyterrorystyczne (tot. DFE Security)

Koncentrując się na zabezpieczeniach architektonicznych w miastach, warto zwrócić uwagę na dwa nurty myślenia o bezpieczeństwa. Wyrastający z tradycji i filozofii zapobiegania przestępstwom kryminalnym Brytyjczycy stworzyli kilka bardzo interesujących programów.
W roku 1989 rozpoczęto popularny program prewencyjny nazwany SBD – *Secured by Design* (co można przetłumaczyć jako „zabezpieczony przez projekt"), który dotyczył przede wszystkim zapewnienia bezpieczeństwa nieruchomości mieszkalnych i komercyjnych. Jest on adresowany do szerokiego kręgu odbiorców – właścicieli nieruchomości i profesjonalistów: projektantów, zarządców nieruchomości, deweloperów oraz producentów materiałów budowlanych i wyposażenia. Bardzo ciekawym aspektem jest merytoryczne zaangażowanie policji w ten program. W jednostkach policji pracują doradcy, którzy służą na etapie projektowania profesjonalną poradą – Local *Crime Prevention Design Advisors*.

W ramach programu jest też prowadzona akcja certyfikacji produktów i materiałów budowlanych związanych z bezpieczeństwem, poczynając od drzwi, zamków i okuć, przez powłoki antygraffiti, kończąc na specjalistycznych zabezpieczeniach przeciwwybuchowych, instalacjach alarmowych i programach komputerowych. Produktom, które spełniają wyznaczone standardy, nadawane jest logo programu SBD i tytuł produktu preferowanego przez policję (*Police Preferred Specification*).
Zasadniczym celem programu jest wzmocnienie odporności budynków na aktywność przestępców, włamywaczy i innych sprawców przestępstw kryminalnych. Podobną, zakrojoną na szeroką skalę akcją mającą na celu poprawę stanu bezpieczeństwa przestrzeni publicznej jest rządowy program *Safer Places* – „miejsca bardziej bezpieczne". Skierowany jest przede wszystkim do władz lokalnych, zarządców i administratorów nieruchomości, oficerów policji i członków innych służb odpowiedzialnych za bezpieczeństwo, a także do planistów i architektów zajmujących się projektowaniem przestrzeni publicznych. W jednostkach policji powołano specjalnych doradców – *Architectural Liason Officers*. W ramach programu został także wydany obszerny poradnik *Safer Places – The Planning System and Crime Prevention* („Miejsca bardziej bezpieczne – system planowania a prewencja kryminalna").
Poradnik *Safer Places* nie jest zbiorem nakazów, zakazów ani uniwersalnych recept. Prezentuje, często na konkretnych projektach i realizacjach (*case studies*), określone problemy i relacje, istniejące pomiędzy środowiskiem zabudowanym a zagrożeniem przestępczym, wzbogacając tym samym wiedzę decydentów oraz projektantów i dając im do dyspozycji narzędzia planistyczne i projektowe, które służą do rozwiązywania zastanych miejscowych problemów w indywidualny i twórczy sposób.

PORADNIK SAFER PLACE JEST DOKUMENTEM NA WSKROŚ PRAKTYCZNYM W SWOJEJ STRUKTURZE. ZDEFINIOWANO W NIM 7 KLUCZOWYCH ATRYBUTÓW PROGRAMU:

1. Dostęp i organizacja ruchu *(access and movement)* – klarowna, sprawna i bezpieczna organizacja ruchu, jasna definicja dróg, przestrzeni pieszych i wejść.
2. Struktura funkcjonalna *(structure)* – organizacja struktury funkcjonalnej w taki sposób, aby nie dochodziło do konfliktów pomiędzy różnymi funkcjami i sposobami wykorzystania przestrzeni.
3. Nadzór *(surveillance)* – miejsca, gdzie wszystkie przestrzenie publiczne znajdują się pod nadzorem i kontrolą.
4. Własność terytorialna *(ownership)* – miejsca, które odzwierciedlają poczucie własności i terytorialnej przynależności do danej społeczności.
5. Ochrona fizyczna *(physical protection)* – miejsca wyposażone w niezbędne i dobrze zaprojektowane środki i systemy bezpieczeństwa.
6. Aktywność *(activity)* – miejsca, w których poziom aktywności jest właściwy dla ich przeznaczenia, zapewniając tym samym poczucie bezpieczeństwa.
7. Zarządzanie i utrzymanie *(management and maintenance)* – miejsca, które zaprojektowano z myślą o ich odpowiednim zarządzaniu i utrzymaniu we właściwym stanie.

Każdy z wymienionych atrybutów jest poddany analizie przedstawionej na konkretnych przykładach. Ponadto w poradniku prezentowano ponad 20 zrealizowanych projektów, w których implementowano zasady programu, co w rezultacie przyniosło poprawę stanu bezpieczeństwa. Przedstawione przykłady dotyczyły zróżnicowanych funkcjonalnie terenów: zarówno mieszkaniowych, jak i śródmiejskich, obszarów usług komercyjnych i handlowych, szkół, parków, garaży i dworców.

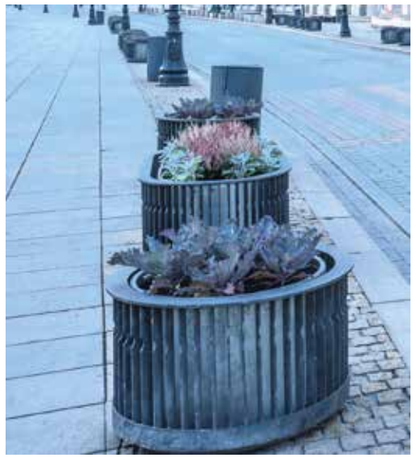
Inne systemowe podejście znajdujemy w programie zapewnienia bezpieczeństwa w stolicy USA, Waszyngtonie. Kompleksowym narzędziem planistycznym – które za zadanie miało połączyć wysiłki zmierzające do zbudowania zabezpieczeń z upiększeniem miasta, zapewnić wybranym budynkom pożądaną ochronę strefową przed atakiem bombowym (przy zachowaniu historycznych wartości założenia urbanistycznego) oraz poszerzyć paletę atrakcyjnych mebli miejskich i elementów małej architektury wykorzystywanych w celach prewencyjnych – był Plan urbanistyczny zabezpieczenia stolicy (*The National Capital Urban Design and Security Plan*). Założenia planu, który był przygotowany we współpracy z agencjami federalnymi odpowiedzialnymi za transport, budownictwo i bezpieczeństwo publiczne76, zostały opublikowane w październiku 2002 r., rok po zamachu z 11 września, i zaktualizowane w 2005 r.

Betonowe zapory w formie ławek

Nowością tego dokumentu i pewnego rodzaju metodologii była zmiana spojrzenia na zabezpieczenia i „fortyfikacje" współczesnych miast. Mamy tutaj do czynienia z zastąpieniem nazewnictwa zabezpieczeń z „prefabrykowanych zapór" na „meble miejskie o zastosowaniach dla bezpieczeństwa publicznego". Zasadniczo ciągle chodzi o to samo: aby w wyniku analiz, doświadczeń i zdobywanej wiedzy z analizy ryzyka miasto tak podzielić na strefy, aby każda z nich miała adekwatne do charakteru i potrzeb zabezpieczenia.
Meble miejskie, które – oprócz kształtowania terenu zgodnie z zasadami CPTED stają się głównym elementem zabezpieczenia przestrzeni – muszą zapewniać funkcje bezpieczeństwa i użyteczności dla mieszkańców, muszą być estetyczne! Najlepiej, żeby były pięknymi meblami miejskimi.
Projekt przewiduje kilka typów takich instalacji: śmietniki, latarnie uliczne, przystanki autobusowe i ławki, klomby i donice na rośliny oraz zapory. Wszystkie te elementy powinny wkomponować się w otoczenie, muszą być mocne, wpisywać się w szerszą koncepcję zarządzania bezpieczeństwem, zintegrowane z systemami bezpieczeństwa, *smart city* itp.

Meble miejskie są wykonywane w różnych technologiach i z różnych materiałów. Zasadniczo stosuje się trzy kategorie materiałów: beton w postaci prefabrykowanych elementów, stal i inne formy metali oraz drewno. Oferta rynkowa mebli miejskich jest dość bogata. Zazwyczaj producenci specjalizują się w tych materiałach, zdarzają się też połączenia materiałów w kombinowane zestawy. Z punktu widzenia bezpieczeństwa, a szczególnie w odniesieniu do zagrożeń terrorystycznych materiałem najbardziej efektywnym jest beton. Betonowe zapory, ławki, „odpoczywalniki", nazwy miast wykonane z prefabrykowanych liter alfabetu stanowią najskuteczniejszą barierę.
Ostatnio Europa była wstrząsana atakami tanią, ale bardzo śmiercionośną bronią: kradzioną ciężarówką – wszyscy mamy w pamięci zdarzenia w Berlinie i Lyonie. Były one możliwe z dwóch powodów: scenariusz i ryzyko, że ktoś ukradnie ciężarówkę i będzie nią masakrował mieszkańców, było albo zbyt absurdalne, albo trudno było stworzyć narzędzia prewencyjne. Brak ciężkich, mocnych i trudnych do przesunięcia barier spowodował, że ciężarówka stała się narzędziem masowej zbrodni.

Szpaler donic z roślinnością skutecznie odgradza od ulicy



Odpowiedzą na ten trend są coraz częściej pojawiające się projekty mebli miejskich, które spełniając wszystkie kryteria skutecznych narzędzi, są jednocześnie pięknymi przedmiotami zaprojektowanymi przez artystów projektantów i wykonane przez bardzo sprawnych rzemieślników lub zakłady prefabrykacji żelbetowych. Służby bezpieczeństwa i zarządzania kryzysowego miast coraz częściej są zainteresowane takimi elementami miejskiego krajobrazu. Coraz więcej właścicieli i zarządców nieruchomości komercyjnych jest skłonnych uzupełnić system bezpieczeństwa swoich budynków czy całych nieruchomości takimi elementami małej architektury.

Reasumując, charakterystyka ludzkich strachów ma dość stały charakter, a narzędzia, które realnie i skutecznie zapobiegają zagrożeniom, też mają katalog w swoim trzonie dość stabilny. Przed zagrożeniem należy się osłonić, zasłonić lub zagrodzić. W odpowiedzi na nowe zagrożenia zmienia się sukcesywnie katalog rozwiązań – pojawiające się nowinki techniczne działają zgodnie z logiką odgrodzenia się lub umożliwiają prowadzenie skutecznej obserwacji.
W Polsce z zazdrością możemy się przyglądać zaawansowanej metodyce działań w USA czy Wielkiej Brytanii. Również w tej dziedzinie sprawy idą jednak ku lepszemu, więc nowych możliwości należy wypatrywać. □

Poradnik Safer Places wzbogaca wiedzę decydentów i projektantów, dając im do dyspozycji narzędzia planistyczne i projektowe, które służą do rozwiązywania zastanych miejscowych problemów w indywidualny i twórczy sposób

BIO

Jacek Pałkiewicz

reporter, jeden z najbardziej aktywnych podróżników i eksploratorów naszych czasów. Trener i twórca pierwszej szkoły survivalu w Europie. Członek rzeczywisty Królewskiego Towarzystwa Geograficznego w Londynie.
Na swoim koncie ma wiele osiągnięć i wyróżnień, m.in. odkrycie źródła Amazonki, szkolenia kosmonautów i jednostek antyterrorystycznych.
Autor ponad 40 książek i wielu publikacji w prasie międzynarodowej.

BIO

Jacek Tyburek

menedżer bezpieczeństwa organizacji. Doświadczenie zdobywał w różnych obszarach bezpieczeństwa; od przemysłu i logistyki, przez BPO, po bezpieczeństwo w rzeczywistości wirtualnej. Promotor pojęcia Organisational Resilience. Entuzjasta bezpieczeństwa miast, realizujący swoją pasję w powstającej pracy doktorskiej.

Targi IFSEC International umacniają swoją pozycję na światowym rynku obowiązkowych imprez dla specjalistów branży security. Londyńskie centrum wystawienniczo-konferencyjne ExCeL Arena odwiedziło w tym roku 34 756 gości z 117 krajów.

IFSEC International 2019

W porównaniu z 2018 r. liczba gości na stoiskach wzrosła o 7%. IFSEC stał się światowym centrum generowania biznesu i budowania ważnych relacji dla dostawców systemów zabezpieczeń.

Spotkanie całej branży

IFSEC ma wyjątkową zdolność przyciągania całej branży security – instalatorzy, integratorzy, dystrybutorzy, konsultanci, producenci, przedstawiciele instytucji rządowych i szereg innych podmiotów zajmujących się zabezpieczeniami mogli wspólnie odkrywać wyjątkowe premiery produktów, oglądać rozwiązania w działaniu, spotykać się twarzą w twarz z dostawcami i wykorzystać trzy dni pełne merytorycznych treści.

Platforma do wprowadzania produktów na rynek

Na IFSEC International firmy prezentowały najlepsze i najbardziej innowacyjne produkty i rozwiązania światowego rynku zabezpieczeń. Podczas tegorocznych targów premierowe pokazy miało wiele nowych rozwiązań, które zaprezentowano tysiącom potencjalnych nabywców.

Seminaria

Seminaria towarzyszące targom były okazją do przemyśleń i rozmów nt. dokonującego się rozwoju technologicznego, w szczególności jego wpływu na przyszłość branży. Odzwierciedlając niepokój związany z cyberzagrożeniami, znaczna część seminariów skupiała się na problemach zabezpieczeń w systemach IP. Temat ten był widoczny w wielu obejmujących łącznie ponad 35 godz. sesjach, którym patronowała brytyjska instytucja akredytacyjna CPD Certification Service.
Podczas *National Surveillance Camera Day* – zorganizowanego po raz pierwszy na IFSEC International, komisarz Tony Porter zaprezentował zestaw wytycznych „Secure by Default", które określają minimalne wymagania dla „cyberbezpiecznych" kamer dozorowych. Spełnienie tych wytycznych, przygotowanych „przez producentów dla producentów", ma zapewnić, że systemy dozorowe będą miały wbudowane funkcje zabezpieczające, będą zgodne z zasadami sztuki i będą mogły ewoluować, aby sprostać zmieniającym się zagrożeniom.

Kolejna edycja za rok

IFSEC International 2020 odbędzie się w Londynie w dniach 19-21 maja 2020 r. Tradycyjnie będą mu towarzyszyć targi FIREX International, Safety & Health Expo, Facilities Show i Smart Buildings Expo, a po raz pierwszy dołączą Counter Terror Expo i Ambition and Forensics, co pozwoli objąć całościowo branżę zabezpieczeń.

Polski akcent

Na swoim stoisku na targach IFSEC firma SATEL zaprezentowała m.in. nowości oraz zapowiedziała produkty, które już niedługo pojawią się na rynku. Największym zainteresowaniem cieszyły się:
ABAX 2 – dwukierunkowy system bezprzewodowy (Grade 2) o dalekim zasięgu działania urządzeń (do 2 tys. m w otwartej przestrzeni), długim czasie pracy urządzeń zasilanych bateryjnie bez konieczności wymiany baterii (nawet do 8 lat) oraz szerokiej gamie dostępnych urządzeń.
SLIM Line – nowa rodzina czujek ruchu o ciekawym designie, rozwiązaniach ułatwiających montaż i oferowaną funkcjonalność.
INTEGRA – zaawansowana centrala alarmowa, prezentowana w kontekście możliwości integracji systemu alarmowego z Control4, Crestron, RTI i KNX.
Z zainteresowaniem spotkały się także zestawy PERFECTA KIT, skomponowane specjalnie z myślą o potrzebach brytyjskiego rynku. Lokalni instalatorzy docenili w szczególności elementy zestawu, łatwy montaż, możliwość sterowania m.in. poprzez aplikację mobilną oraz szybką konfigurację z użyciem intuicyjnego oprogramowania.

Dzień z bezpieczeństwem pożarowym

Na stadionie PGE NARODOWY pod koniec lipca odbył się XVI Kongres Pożarnictwa FIRE SECURITY EXPO 2019. Uczestniczyło w nim 60 wystawców i ekspertów branżowych. Kongres odwiedziło ponad 900 projektantów, instalatorów, specjalistów ppoż., wykonawców i inwestorów branży budowlanej.

Spotkanie było okazją do omówienia bieżących, najważniejszych i najtrudniejszych problemów ochrony ppoż. i zabezpieczeń technicznych budynków. Wykłady dotyczyły konfrontacji przepisów z ich praktyczną realizacją na różnych etapach: od projektu, po odbiory i eksploatację. Przeprowadzono szereg testów, pokazów, warsztatów technicznych.
Na stoiskach wystawowych rozwiązania w dziedzinie zabezpieczeń i ochrony przeciwpożarowej prezentowały czołowe firmy branży ppoż.

V Branżowe Spotkanie Kobiet 2019

W połowie czerwca br. firma Schrack Seconet Polska zorganizowała jubileuszowe V Branżowe Spotkanie Kobiet. W tym wyjątkowym wydarzeniu wzięło udział kilkadziesiąt Pań reprezentujących firmy z całego kraju – przedstawicielek kadry zarządzającej, projektantek, specjalistek z różnych dziedzin systemów bezpieczeństwa.

W tym roku Branżowe Spotkanie Kobiet odbyło się poza Warszawą, w malowniczej okolicy pałacu i folwarku w Łochowie. Rozpoczęło się szkoleniem z wizualnego myślenia, które pozwoliło uczestniczkom trochę lepiej poznać siebie i techniki wizualnej komunikacji.
Przed wieczorną kolacją Panie miały czas na chwilę relaksu i oderwanie się od codzienności w strefie wellness i SPA. Równolegle odbywały się także zajęcia z jogi i zumby.

W spotkaniu w Łochowie uczestniczyło ponad sześćdziesiąt Pań z 32 firm z całej Polski. Niezależnie od czasu współpracy pomiędzy poszczególnymi firmami to wydarzenie było okazją do bezpośredniego spotkania się wielu Pań po raz pierwszy.
Więcej na stronie www.schrack-seconet.pl

Trwa Wielka Urodzinowa Loteria Hikvision!

Firma Hikvision już od 5 lat działa w Polsce i dostarcza najlepsze rozwiązania dla rynku zabezpieczeń. Dzięki rozbudowanej ofercie, zintegrowanym rozwiązaniom oraz ciągłemu, dynamicznemu rozwojowi w obszarze R&D Hikvision jest obecnie uznawana za najszybciej rozwijającego się producenta branży zabezpieczeń. Potwierdza to też stały wzrost przychodów rok do roku. Anna Makowska, Marketing Specialist Hikvision Poland, powiedziała: *Jesteśmy dumni z tego, co udało nam się osiągnąć w ciągu mijających w tym roku, pełnych wyzwań 5 lat. Z okazji urodzin, trochę przewrotnie, to my postanowiliśmy obdarzyć prezentami naszych klientów. Każdy ma szansę wygrać, a to nasze podziękowanie za to że klienci są z nami i wierzą w niezawodność produktów Hikvision.*
Loteria jest częścią kampanii z okazji 5. urodzin firmy. Z tej okazji Hikvision rozdaje samochody! Pierwszy Fiat Fiorino już trafił do nowego właściciela! W puli nagród pozostają jeszcze 4 samochody. Jedyne, co musisz zrobić, to zarejestrować swój zakup na stronie loterii i czekać na ogłoszenie wyników losowania. Za każde wydane 1000 zł netto otrzymasz jeden los.

Szczegóły i regulamin loterii na stronie www.loteriahikvision.pl

MOBOTIX c26 to mała kamera hemisferyczna, idealna do montażu w sklepie. Pojedyncze urządzenie umożliwia monitoring wizyjny i rejestrację (ciągłą i sterowaną zdarzeniami) pomieszczenia. Zastosowany przetwornik o rozdzielczości 6 Mpix gwarantuje wysoką szczegółowość obrazu.

MOBOTIX c26 – więcej niż kamera...

Wbudowana funkcja korekcji obrazu sprawia, że niezależnie od sposobu montażu kamery jakość obrazu jest na najwyższym poziomie, przy jednoczesnym naturalnym odwzorowaniu kształtów.
Istotnym atutem są bezpłatne funkcje analizy obrazu MxAnalytics, umożliwiające m.in. zliczanie osób i generowanie map ciepła bez konieczności posiadania zewnętrznego oprogramowania, szczególnie przydatne w analizie ruchu klientów.
Dodatkową funkcjonalnością tego rozwiązania jest możliwość wygenerowania sygnału alarmu, np. gdy klient zatrzyma się w określonej strefie. Może nim być m.in. uruchomienie materiału wideo na ekranie lub komunikat głosowy odtwarzany bezpośrednio z kamery. MOBOTIX oferuje też bezpłatną platformę wideo MxMC do zarządzania i monitorowania podłączonych kamer. Wszystkie te udogodnienia sprawiają, że rozwiązanie marki MOBOTIX jest idealnym wyborem dla branży *retail*.

Więcej informacji: www.linc.pl

Akribos to wewnętrzna kamera 3D będąca licznikiem przepływu osób. Jego główna funkcjonalność wiąże się z możliwością śledzenia złożonego ruchu w czasie rzeczywistym (wejście/wyjście – w prawo/w lewo/na wprost). Automatycznie transferuje dane przez TCP/IP w formacie XML lub TXT, wykazując przy tym dużą odporność na zakłócenia spowodowane cieniami czy zmianami oświetlenia.

OPTEX Akribos

W ofercie naszego partnera – firmy Xenometrix – pojawiło się oprogramowanie do analizy danych generowanych przez licznik przepływu osób OPTEX Akribos. Jest ono dostępne w wersji instalowanej na komputerze lokalnym lub w chmurze danych. Istnieje możliwość pobrania 30-dniowej wersji próbnej.

Akribos określa przemieszczenie osoby w 4 kierunkach, a Xenometrix zapewnia przejrzystą i łatwą do interpretacji wizualizację danych

Licznik może być wykorzystany w centrach handlowych, sklepach wielkopowierzchniowych, obiektach użyteczności publicznej, centrach konferencyjnych i wystawienniczych, obiektach transportowych (dworce, lotniska itp.). Innym jego zastosowaniem jest monitorowanie liczby osób w budynku na potrzeby ewakuacji.

Więcej na stronie www.optex.com.pl

Milestone XProtect® Corporate **z certyfikatem GDPR-ready**

XProtect Corporate 2019 R2 to pierwsze oprogramowanie do zarządzania materiałem wizyjnym, które otrzymało certyfikat GDPR-ready przyznawany przez niezależny i ceniony na świecie instytut EuroPriSe (European Privacy Seal). Użytkownicy końcowi zyskali tym samym podstawy do budowania systemu dozoru wizyjnego zgodnego z przepisami RODO.

Certyfikacja GDPR-ready obejmuje wszystkie podstawowe możliwości oprogramowania związane z cyberbezpieczeństwem. Milestone Systems dostarczył holistyczny zestaw narzędzi, w tym obszerny przewodnik z gotowymi do użycia szablonami, pomocny integratorom i użytkownikom w projektowaniu, wdrażaniu i obsłudze systemów dozoru wizyjnego zgodnie z RODO. Zapewnił także szkolenia w zakresie świadomości zachowania prywatności.
W 2017 roku Milestone Systems dołączył do ponad 150 firm technologicznych z całego świata, podpisując w Kopenhadze deklarację – tzw. List Kopenhaski – wzywającą firmy technologiczne do stosowania technologii w sposób odpowiedzialny oraz skoncentrowany na człowieku i jego prawach. Zapewnienie klientom ochrony ich danych osobowych gromadzonych i przetwarzanych przez systemy XProtect VMS stanowi naturalne rozszerzenie tego zobowiązania – powiedział Bjørn Skou Eilertsen, dyrektor ds. technologii w Milestone Systems.
Certyfikacja GDPR-ready obejmuje XProtect Corporate – najbardziej funkcjonalny produkt Milestone Systems. Ambicją firmy jest certyfikacja całej gamy produktów XProtect VMS.

Więcej na stronie: www.milestonesys.com

SICUREZZA 2019 – w centrum rozwijającego się rynku

Uruchomieniem kupna biletów online na www.sicurezza.it rozpoczęło się oficjalnie odliczanie do SICUREZZA 2019. To największe targi branży security we Włoszech i jedne z najważniejszych w Europie poświęcone tematyce bezpieczeństwa i zabezpieczeń przeciwpożarowych.

Wydarzenie, które odbędzie się w Mediolanie, w dniach 13–15 listopada 2019 r. w Fiera Milano - Rho, będzie gościło włoskich i międzynarodowych profesjonalistów w szczególnie pomyślnym dla rynku czasie. Według najnowszych danych we Włoszech w 2018 r. potwierdzono wzrost przychodów sektora zabezpieczeń i automatyki budynkowej o 6,8%, dynamicznie rozwijał się też eksport z 9,2% wzrostem (źródło: *ANIE Sicurezza*). W tym kontekście targi ponownie staną się płaszczyzną oferującą znakomite szanse biznesowe firmom, które chcą wykorzystać rozwój rynku.
W tegorocznej edycji targów SICUREZZA jeszcze więcej miejsca zostanie poświęcone tematowi zabezpieczeń ppoż. z najciekawszymi produktami w sektorze, przy jednoczesnym podkreśleniu dążenia do innowacji we wszystkich obszarach bezpieczeństwa: od dozoru wizyjnego i kontroli dostępu, przez zaawansowane systemy antywłamaniowe, po zabezpieczenia mechaniczne i drony, wykorzystywane jako narzędzie do monitorowania.
Kolejną mocną stroną tej edycji targów będzie Smart Building Expo, wydarzenie poświęcone najnowszym technologiom stosowanym w nowoczesnych budynkach i inteligentnych miastach. Odbędzie się równolegle z targami SICUREZZA i będzie je można zwiedzać, mając ten sam biletu wstępu. Na tarach będzie też można zapoznać się z najciekawszymi Case Study. Firmy będą mogły dzielić się doświadczeniami z integratorami zainteresowanymi konkretnym obszarem wdrożenia, a odwiedzający profesjonaliści będą mogli poznać rozwiązania dostosowane do ich potrzeb.
Wizytę na SICUREZZA można zaplanować już dziś. Odwiedzający mogą wstępnie zarejestrować się lub kupić bilet bezpośrednio na stronie www.sicurezza.it, co pozwoli im zaoszczędzić do 50% ceny biletu.

Fiera Milano Press Office

Krajobraz **po bitwie**

TEKST
Andrzej Popielski

Dziennikarz, fotograf. Autor felietonów o bezpieczeństwie w „Systemach Alarmowych” (w latach 2005–2015).

Nie trzeba terrorystów i łajdaków innych specjalności, żeby życie przestało być bezpieczne i ustabilizowane. Wystarczy, że w naszych stechnicyzowanych społeczeństwach zacznie coś źle działać w banalnych dziedzinach, bo taka jest sfera zarządzania kryzysowego. To m.in. kłopoty z dostawami wody, paliw, żywności, prądu, leków, z dostępem do pomocy medycznej. Także źle funkcjonujące banki, nieużytkowa w sferze publicznej informatyka, kłopoty z transportem i łącznością. Najbardziej dotkliwy jest brak energii elektrycznej – co ważnego dzisiaj nie jest na prąd? Gdy go braknie, zaczynają się *blackouty*, które co jakiś czas są faktem w różnych krajach, na szczęście odczuwane w większości bardziej jako bolesne epizody niż katastrofy. Niedawno np. na kilka godzin zabrakło prądu w prawie całej Ałma Acie w Kazachstanie (1,8 mln mieszkańców).

Ciemność, gdy nie jest traktowana w kategoriach żartu z sypialni, nie jest humorystyczna. *Nomen omen* 13 lipca 1977 r. światło zgasło na 25 godzin w niemal całym Nowym Jorku. Straty obliczono na 300 mln ówczesnych dolarów. Obrabowanych zostało ponad 1600 sklepów, zatrzymano kilka tysięcy przestępców, areszty zorganizowano w piwnicach. Ile osób umarło dlatego, że nie można się było skontaktować lub dojechać? Statystyki raczej nie miały bystrego wzroku.

Palec losu jakby coś wskazywał. Ale kto uczy się na własnych błędach? Kogo przestrasza wizja kolejnej cegły na krawędzi dachu czyhającej na jego głowę. Niedawno, również 13 lipca br., czyli dokładnie 42 lata później, znowu w Nowym Jorku w 73 tysiącach domostw i biur na Manhattanie na kilka godzin zgasło światło z powodu pożaru transformatora. Ciemności na Times Square oraz Broadwayu, gdzie ulokowały się teatry, kina i lokale rozrywkowe, oświetlały reflektory samochodów. Nie działały uliczne latarnie i światła sygnalizacji drogowej. W stojących pociągach metra i budynkowych windach uwięzione były setki ludzi, często kilka godzin w zupełnych ciemnościach. Przerwano koncert Jennifer Lopez i spektakle teatrów muzycznych na Broadwayu. Aktorzy śpiewali na ulicy *a capella*.

Upał smaży ciała i umysły, czas jest ogórkowy, a tematy felietonowe niekoniecznie ciężkostrawne. Ciężka jest dola złodzieja, a ludzie są dla nich niemiłosierni w opiniach, chociaż w dziedzinie miłosierdzia też panuje poglądowy pluralizm. Chwilę się zamyśliłem nad komentarzami internautów do prasowej notki ostrzegającej przed włamywaczami na Ursynowie. Ci ożywili się sezonowo, bo jak koty lubią ciepło i dyskretną aktywność w niezatłoczonych pomieszczeniach. Zwykle wiedzą, gdzie i po co idą broić. Niektórzy pracują jednak społecznie, sądząc po opiniach z Internetu:

Co dzisiejszy złodziej może ukraść z mieszkania? Telewizor za 1 K kupiony na promocji? (młodzieżowo mówiąc jedno koło, czyli 1000 zł). Laptop pewnie firmowy? Mikrofalówkę? A może szafę po babci z drewna, które las widziało? Pieniądze są w banku. Łańcuszek z komunii nosimy na szyi. Macie brylanty – to raczej w sejfie... Trzeba uważać, żeby używanych butów nie zabrali. Bycie złodziejem nie zawsze bywa świetnym interesem.

Ale dla złodziei perspektywy złe nie są. Wciąż są rodacy, którzy oszczędności trzymają w skarpecie, choć razi ich brak porządku: *Ukradzione rzeczy nie były specjalnie cenne, ale te zniszczenia i wymiana drzwi albo okna. I trauma po widoku łomu śpiącego na łóżku.*

Potrzebujesz replikę dokumentu prawa jazdy czy dowodu osobistego? Zrobimy ją takiej jakości, że nie odróżnisz od oryginału. Nie miałem pojęcia o istnieniu branży drukarskiej w dziwnej specjalności tzw. dokumentów kolekcjonerskich. To zamawiane w Internecie repliki prawdziwych dokumentów publicznych, podobno tylko do użytku własnego. Nie trzeba mieć umysłu ostrego jak brzytwa, żeby pojąć, że mogą ułatwiać życie oszustom przy podszywaniu się pod inne osoby, np. przy wyłudzeniach dóbr i kredytów. Znowelizowana ustawa o dokumentach publicznych miała ograniczyć ten proceder. Rynek się nie zwinął, bo wyszukiwarka pokazała mi oferty firmowe. Co prawda po zmianach w prawie, a weszły one w życie 12 lipca, nie można już zamówić repliki dokumentu na cudze nazwisko, ale czy na pewno? Rozrzewnił mnie troskliwy producent – pewnie miłośnik RODO – gwarantujący klientom poufność danych osobowych, usuwanych bez zwłoki po transakcji i wysyłający nieopisane paczki. Bezpieczeństwo – jak widać – wszystkim leży na sercu.

Czarny humor z Twittera i Facebooka z ofertą pewnego (podejrzewam, że fikcyjnego) zakładu pogrzebowego: *W ramach wprowadzania nowych technologii oferujemy przeniesienie klienta do chmury.* □

Sztuczna inteligencja

Nowa era monitoringu wizyjnego

- **Czarna lista:** precyzyjnie zidentyfikuj podejrzanego oraz wyzwalaj alarm w czasie rzeczywistym. Przechwytuj twarze z wielu kamer oraz śledź trasy obserwowanych osób.
- **Kilenci VIP:** błyskawicznie identyfikuj klientów VIP w systemie i wyzwalaj operacje towarzyszące, w celu zwiększenia ich stysfakcji.
- **Metadane:** w szybki sposób wyszukuj interesujące fragmenty nagrań dzięki informacjom przechowywanym w postaci metadanych: wiek, płeć, ekspresja itp.
- **Wyszukuj według wzorca:** sprawnie przeszukuj nagrania używając zdjęcia, a nawet portretu pamięciowego.

Polecane modele

IPC-HFW7442H-Z

4 Mpx IR
kamera sieciowa AI

SDT5A404VA-2F

2 Mpx + 4x 4 Mpx
kamera sieciowa AI

SD8A820WA-HNF

4K 20 x zoom Starlight+
IR kamera sieciowa AI

NVR5432-16P-I

32-kanałowy 1,5U 16PoE
sieciowy rejestrator AI

CE FC 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@dahuatech.com
www.dahuasecurity.com/pl