CZASOPISMO RYNKU SECURITY

№ 06
2019 (18)
listopad /grudzień

a&S POLSKA

TEMAT NUMERU →16

Ranking największych firm security na świecie

Prezentujemy raport o światowych liderach branży zabezpieczeń technicznych na podstawie osiąganych przychodów ze sprzedaży i trendach na globalnym rynku security.

BEZPIECZEŃSTWO HOTELI I INSTYTUCJI BANKOWYCH →58

Bezpieczeństwo klientów

Zagrożenia wynikające ze wzrostu przestępczości czy terroryzmu zmuszają do podnoszenia poziomu bezpieczeństwa w hotelach i bankach. Ważną rolę odgrywają tu security menedżerowie.

RYNEK SECURITY →70

RODO w systemach VSS

Wraz ze zwiększającą się popularnością kamer dozorowych z algorytmami AI należy zadbać o przestrzeganie przepisów RODO dotyczących ochrony prywatności w systemach dozoru wizyjnego.

BEZPIECZEŃSTWO BIZNESU →90

Dżungla miasta

Ostatni odcinek opowieści o miejskiej dżungli i czyhających na nas zagrożeniach jest poświęcony nowej metodzie zarządzania kryzysem – *urban resilience*. O bezpieczne miasto musimy zadbać sami.

15 zł
(w tym 8% VAT)

ISSN 2451-5175
05
9 772451 517703

www.aspolska.pl

24/7 VIVID COLOR CAMERA

Super Aperture

HIKVISION

DEEP LEARNING DVR

False Alarm Filter

Quick Target Search

Target Extraction

WIĘCEJ NIŻ MOŻESZ ZOBACZYĆ
TURBO HD 5.0

HIKVISION NR 1 NA ŚWIECIE

Hikvision to światowy lider w dostawie innowacyjnych produktów i rozwiązań do monitoringu wideo. Dzięki najsilniejszej w branży kadrze R&D, firma Hikvision rozwija kluczowe technologie kodowania audio i wideo, przetwarzania obrazu wideo oraz związanego z tym przechowywania danych. Aby uzyskać więcej informacji, odwiedź nas na stronie www.hikvision.com/pl/.

ColorVu

Obrazy w żywych kolorach przez całą dobę

Kamery Hikvision ColorVu zapewniają obrazy w jasnych kolorach przez cała dobę, nawet w warunkach słabego oświetlenia. Dzięki zaawansowanym obiektywom i sensorom o wysokiej czułości doskonale radzą sobie z rejestrowaniem żywych obrazów w różnych, nawet trudnych do monitoringu miejscach.

AcuSense

Inteligentna precyzja

Oparty na algorytmach sztucznej inteligencji DVR AcuSense Turbo HD oferuje znacznie lepszą precyzję VCA.

Hikvision Poland
The Park Warsaw
ul. Krakowiaków 50
02-255 Warszawa
T +48 22 4600150
info.pl@hikvision.com

@HikvisionPoland
www.hikvision.com/pl/

EDYTORIAL

Drodzy Czytelnicy

Już po raz czwarty prezentujemy polską edycję Rankingu Security 50 (s. 16) wraz z obszernym raportem o światowym rynku zabezpieczeń technicznych. Dział analityczny a&s International zestawił firmy z branży security o globalnym zasięgu i porównał ich wyniki finansowe. Powstał w ten sposób pełen przegląd wskazujący kierunki rozwoju rynku. Większość firm ujętych w rankingu odnotowała dwucyfrowy wzrost sprzedaży (s. 18). Ale czy w najbliższych latach firmy chińskie utrzymają tak szybkie tempo wzrostu? (s. 28).

Jak co roku publikujemy także analizę brytyjskiej firmy badawczej Memoori (s. 26). Tym razem eksperci, na podstawie analizy wskaźników ekonomicznych globalnego rynku security, pokusili się o prognozy na najbliższe cztery lata. Analizując raport pod kątem przyszłości, zidentyfikowaliśmy trendy technologiczne, które napędzają rozwój branży (s. 30).

Raport „Security 50" ma wymiar globalny. Prezentujemy w nim charakterystykę i specyfikę poszczególnych światowych regionów, którą opracowali dla nas wiodący integratorzy systemów (s. 36), bowiem to właśnie oni mają najpełniejszy obraz rynku.

O najnowszych faktach z dziedziny sztucznej inteligencji piszemy na s. 42. Jak poradzić sobie z komunikacją pomiędzy protokołami komunikacyjnymi różnych producentów? Czy ONVIF nadal będzie organizacją otwartą zastanawiamy się na s. 46. Projektantom polecamy artykuł na temat ich roli na etapie tworzenia stanowiska operatora systemu dozoru wizyjnego (s. 48). Z kolei cenne wskazówki dotyczące wymogów RODO znajdą w artykule na s. 70.

Tematem przewodnim tego numeru jest „Bezpieczeństwo hoteli i instytucji finansowych". O tym, jakie wyzwania stoją przed profesjonalistami w zapewnieniu bezpieczeństwa gościom hotelowym, piszemy na s. 58, natomiast jak zapewnić właściwy poziom bezpieczeństwa w instytucjach finansowych można przeczytać na s. 66. W obu tych sektorach decydującą jest sprawna ewakuacja. O roli DSO i oznakowaniu dróg ewakuacyjnych piszemy na s. 76.

Ostatni odcinek ciekawego cyklu o miejskiej dżungli i czyhających zagrożeniach tym razem jest poświęcony sprawnemu zarządzaniu bezpieczeństwem miasta (s. 90). W dziale bezpieczeństwo biznesu zastanawiamy się, jakie mogą być skutki wzrostu płacy minimalnej (s. 94) i jak być mądrym przed stratą (s. 96).

Koniec roku to nie tylko czas podsumowań, ale także planów. Już teraz zapraszamy na kolejną edycję Warsaw Security Summit 2020. Zależy nam, aby ta największa w Europie Środkowo-Wschodniej konferencja naszej branży była jeszcze ciekawsza merytorycznie i bardziej wartościowa. W przyszłym roku zorganizujemy także inne wydarzenia, m.in. Security BootCamp w formie warsztatów strategiczno-terenowych dla security menedżerów. Obiecujemy też wiele pozytywnych zaskoczeń!

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

№ 06

2019 (18)
listopad/grudzień

a&S POLSKA

RAPORT 50 2019 SECURITY

NAJWIĘKSZYCH FIRM Z BRANŻY SECURITY NA ŚWIECIE

RYNEK SECURITY

HOTELE I INSTYTUCJE FINANSOWE

BEZPIECZEŃSTWO BIZNESU

SERWIS INFORMACYJNY

FELIETON O BEZPIECZEŃSTWIE

AXIS COMMUNICATIONS www.axis.com/pl

AXIS Q1798-LE
Nowa kamera 4K o wysokiej czułości

Kamera sieciowa AXIS Q1798-LE jest wyposażona w obiektyw Canon z 4-krotnym zoomem optycznym. Może pracować w ekstremalnych temperaturach w zakresie od **-40°C do 60°C**, jej obudowa ma klasę szczelności **IP66/IP67** i odporność mechaniczną **IK10**.

Oferuje także udoskonalone funkcje związane z cyberbezpieczeństwem, m.in. cyfrowo podpisane oprogramowanie sprzętowe. **Technologia Axis Lightfinder 2.0** poprawia jej światłoczułość, prezentowane obrazy mają bardziej realistyczne kolory, ostrzejszy jest obraz ruchomych obiektów. Wbudowany oświetlacz podczerwieni o zasięgu 50 m umożliwia pracę kamery w niemal całkowitej ciemności i uzyskanie wysokiej jakości nagrania bez konieczności instalowania kosztownego dodatkowego oświetlenia. Obsługa standardu zasilania PoE sprawia, że nowa kamera jest łatwa w instalacji, a dodatkowy zasilacz DC zapewnia, że zapisane dane nie zostaną utracone w przypadku przerwy w zasilaniu. **Technologia Axis** Zipstream z obsługą formatów kompresji **H.264 i H.265** znacznie zmniejsza zapotrzebowanie na przepustowość łączy i pamięć masową. Do kamery można podłączyć dodatkowy sprzęt, odpowiedzialny np. za włączenie alarmu - w przypadku zerwania połączenia, urządzenie samo wyśle odpowiednie powiadomienie.

Najważniejsze funkcje kamery:
- Rozdzielczość 4K / 10 Mpix
- Przetwornik obrazu o dużej czułości (min. poziom oświetlenia 00,3 lx w trybie kolor i 0,006 lx w trybie cz-b)
- Obiektyw Canon 12...48 mm
- Technologia Axis Lightfinder 2.0
- Technologia Axis Zipstream z obsługą kodeków H.264/H.265

BCS www.bcscctv.pl

Kamera sferyczna BCS-SFIP21200IR-II

Kamera BCS-SFIP21200IR-II to topowy przedstawiciel rodziny kamer z obiektywem typu *fisheye* w ofercie marki BCS. Cechami, które sprawiają, że ten model kamery to potężne narzędzie monitoringu wizyjnego, są przede wszystkim superczuły **12-Mpix** przetwornik **Sony STARVIS** oraz szerokokątny obiektyw 1,98 mm. Pozwalają uzyskać obraz o kącie widzenia 180° tworzący panoramę 360°, bez tzw. martwych stref. Kamera świetnie sprawdzi się w monitorowaniu rozległych, otwartych przestrzeni, gdy konieczne jest pełne pokrycie dozorowanego obszaru – np. o lotniska, centra handlowe, banki czy hotele.

Zastosowanie kamery **BCS-SFIP21200IR-II** zapewnia wiele niepodważalnych korzyści. Przede wszystkim pozwalają one zastąpić wiele kamer jedną typu *fisheye*. Obraz transmitowany do rejestratora można rozłożyć (funkcja *dewarping*), uzyskując w ten sposób maks. 8 wirtualnych kamer PTZ. Każdą z nich można wykorzystać do dokładniejszej obserwacji interesującej nas strefy. Kamera ma wbudowane funkcje inteligentnej analizy zawartości obrazu, m.in. przekroczenia linii i naruszenia strefy, ale przede wszystkim mapy cieplnej. Obrazuje ona w sposób graficzny strefy o największym natężeniu ruchu, uzyskując cenne dane analityczne.

Ponadto kamera jest wyposażona w promiennik podczerwieni i moduł audio. Ma obudowę o klasie szczelności **IP67** i wandaloodporności **IK10,** dzięki czemu może być również stosowana w monitorowaniu stref podwyższonego ryzyka, takich jak cele więzienne czy sale przesłuchań.

BOLD www.TabliceBHP.com

Znaki fotoluminescencyjne wg PN-EN ISO 7010

Zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych z 7.06.2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. nr 109, poz. 719) właściciele, zarządcy lub użytkownicy budynków oraz placów składowych i wiat są odpowiedzialni za oznakowanie znakami zgodnymi z polskimi normami, m.in. dróg i wyjść ewakuacyjnych.
Po kilku latach stagnacji na rynku oznakowania ewakuacyjnego pojawił się nowy producent. Firma Bold zaprezentowała innowacyjne podejście do oznakowania dedykowanego do wnętrz biurowych, hotelowych i gastronomicznych. W ofercie znalazły się m.in. znaki w ramkach imitujących szczotkowane aluminium. Znaki te wyróżnia nowoczesne wzornictwo, bardzo łatwy montaż i znakomite parametry fotoluminescencji.
Drugą nowością są znaki ekologiczne. W nowoczesnych wnętrzach architekci często stosują rozwiązania nawiązujące do ekologii. Drewno, sklejka, proste industrialne formy i naturalne materiały to typowe cechy współczesnych wnętrz. Zainteresowanych odsyłamy na stronę producenta TabliceBHP.com.

DAHUA TECHNOLOGY POLAND

www.dahuasecurity.com/pl

Kontrolery z identyfikacją wzorca twarzy

Firma Dahua Technology, wychodząc naprzeciw oczekiwaniom klientów, wprowadziła do oferty serię terminali ASI72XX identyfikujących użytkowników za pomocą wzorca twarzy. Urządzenia przed wprowadzeniem do oficjalnej sprzedaży były przez wiele tygodni testowane przez pracowników i zaprzyjaźnionych klientów firmy.

Kilkadziesiąt tysięcy identyfikacji, wielu użytkowników różnych narodowości i duża liczba pozytywnych odpowiedzi pozwalają stwierdzić, że tego typu terminale będę w przyszłości cieszyć się coraz większym zainteresowaniem. Wśród pozytywnych głosów najczęściej pojawiała się informacja o prawidłowej i jednoznacznej identyfikacji użytkownika, realizowanej dzięki dwóm modułom kamer oraz zaawansowanemu algorytmowi inteligentnej analizy obrazu, który wykrywa i odrzuca próby autoryzacji za pomocą zdjęcia lub nagrania wideo. Użytkownicy zwracali uwagę na duży zasięg identyfikacji, nawet z odległości **2,4 m**, i krótki czas weryfikacji nieprzekraczający **0,35 s**.

W celu podniesienia poziomu bezpieczeństwa do weryfikacji można dodatkowo użyć karty, kodu PIN lub wzorca linii papilarnych. Oprócz zaawansowanej funkcjonalności kontroli dostępu terminal ma **moduł RCP**, gdzie użytkownik z poziomu 7" wyświetlacza może wybrać właściwe zdarzenie. W logu zdarzeń, oprócz standardowych danych, można zapisać zdjęcie identyfikowanego użytkownika. Firmy instalatorskie wskazywały na łatwy montaż i wbudowany moduł Wi-Fi – wystarczyło podłączenie zasilacza **12 V DC/2 A**, aby rozpocząć konfigurację i móc korzystać z terminala.

HIKVISION

www.hikvision.com/pl

Klawiatury i sygnalizatory do centrali AXHub

Firma Hikvision poszerzyła ofertę o akcesoria do nowatorskiej centrali alarmowej do zastosowań w małych i średnich obiektach (mieszkalnych i biurowych). Centrala AXHub łączy w niewielkim urządzeniu system alarmowy obsługujący do 32 czujek bezprzewodowych oraz system wideoweryfikacji zdarzeń na podstawie podglądu z kamer IP **Hikvision**. Całość oparto na uznanym dwukierunkowym systemie bezprzewodowym Enforcer Pyronix, komunikującym się na częstotliwości **868 MHz** i doświadczeniu **Hikvision** jako producenta systemów dozoru wizyjnego.

Obecnie w ofercie pojawiły się nowe urządzenia bezprzewodowe: klawiatury, czytniki kart oraz sygnalizatory wewnętrzne i zewnętrzne, poszerzające spektrum zastosowań systemu **AXHub**. Na uwagę zasługuje klawiatura LED z czytnikiem kart **Mifare** i możliwością obsługi 4 partycji. W jednym systemie można zastosować nawet 4 klawiatury, zapewniając bezpieczeństwo i wygodę użytkowania systemu.

Ważnym atutem **AXHub** jest dostępność interfejsów komunikacyjnych, umożliwiających rejestrację w chmurze **Hik-Connect**, co ułatwia obsługę systemu i otrzymywanie powiadomień o zdarzeniach. Już podstawowa wersja urządzenia do komunikacji wykorzystuje Ethernet i Wi-Fi, są też wersje z dodatkowym modemem **GPRS lub 3G/4G**. W przypadku wystąpienia alarmu użytkownik otrzymuje powiadomienie **PUSH** z 7-sekundowym nagraniem wideo ze zdarzenia z powiązanej kamery. System wyposażony w nowe sygnalizatory, oprócz powiadamiania zdalnego będzie również alarmował otoczenie lokalnie, zarówno wewnątrz, jak i na zewnątrz budynku.

LINC POLSKA

www.linc.pl

Stwórz własne rozwiązanie z MOBOTIX M73!

Elastyczność i otwartość nowej platformy MOBOTIX oferuje wiele możliwości instalacji indywidualnych aplikacji, wzbogacających kamery o nowe funkcje.

MOBOTIX – bezpieczeństwo w sieci i indywidualne rozwiązania

Certyfikowane przez **MOBOTIX** aplikacje są profesjonalne, bazują na sieciach neuronowych i algorytmach pochodzących od renomowanych, zweryfikowanych partnerów. Spełniają najwyższe wymagania bezpieczeństwa w sieci. Są one preinstalowane w kamerach **MOBOTIX M73** i klient może je bezpłatnie testować przez 30 dni, po czym wybrać aplikację spełniającą jego wymagania. Liczba dostępnych aplikacji będzie rosła wraz z kolejnymi aktualizacjami.

MOBOTIX SDK – spersonalizowane aplikacje

Partnerzy, klienci i użytkownicy **MOBOTIX** mogą rozwijać i tworzyć własne rozwiązania oparte na bibliotekach **SDK i API**. Można ich używać do tworzenia spersonalizowanych aplikacji odpowiadających najbardziej specyficznym wymaganiom. Zweryfikowane aplikacje będą mogły być udostępniane innym klientom, generując dochód dla ich autorów.

MOBOTIX M73 z trzema modułami

M73 to połączenie najlepszych tradycji **MOBOTIX** z najnowszymi osiągnięciami techniki. Kamerę tę wyróżnia kompaktowa konstrukcja, wysoka jakość wykonania i silny procesor **Quad-Core-ARM Cortex-A53.** W obudowie jest miejsce aż na 3 przetworniki obrazu lub moduły funkcjonalne. To sprawia, że nowa kamera **MOBOTIX M73** jest bardzo wszechstronna i elastyczna w zastosowaniu.

SCHRACK SECONET POLSKA

www.schrack-seconet.pl

APS®-APROSYS: dźwiękowy system ostrzegawczy

Dźwiękowy system ostrzegawczy APSR-APROSYS (produkcji g+m elektronik AG) to przewodowy, modułowy system służący przede wszystkim do powiadamiania osób znajdujących się w zagrożonych obszarach o ewakuacji lub zmobilizowania ich do innego działania.
Dzięki wykorzystaniu technologii warstw i priorytetów może też służyć jako system rozgłaszania komercyjnego (PA –*public address*), system zegarowy czy system dystrybuujący tło muzyczne w obiekcie (**BGM – *background music***) w tym samym czasie.

Rozwiązaniem wyróżniającym system **APSR-APROSYS** jest m.in. możliwość optymalizacji instalacji **DSO** dzięki zastosowaniu elastycznego rozdziału mocy wzmacniaczy.
Zaawansowane kontrolery linii głośnikowych **APS-178.1-XX-EV** z wbudowanymi selektorami stref pozwalają na pełne wykorzystanie zakresów mocy oferowanych przez dobrane wzmacniacze. Gdy w obiekcie występuje wiele stref nagłośnienia małej lub średniej mocy obsługiwanych przez jedną lub kilka par linii głośnikowych, można tu zastosować tylko jedną końcówkę wzmacniacza!
Ponadto każda pożądana funkcja fakultatywna systemu to zaledwie jedna lub dwie karty systemowe dołożone do ramy montażowej **MC-03** systemu. Projektując system z użyciem kontrolerów linii z selektorami stref, można znacznie zredukować liczbę wzmacniaczy, a co za tym idzie wymaganą pojemność akumulatorów zasilania rezerwowego, okablowanie systemowe, rozmiar i liczbę szaf, bez zbędnego przewymiarowania systemu.

TP-LINK

www.tp-link.com.pl

TL-SG1218MPE – wielofunkcyjny gigabitowy przełącznik PoE+

TP-Link TL-SG1218MPE to zarządzalny przełącznik serii Easy Smart, który został wyposażony w 16 gigabitowych portów PoE+. Urządzenie wspiera standard 802.3af/at, dostarczając do 30 W na każdy port. Całkowita moc podłączonych urządzeń wynosi 192 W. Dwa porty SFP umożliwiają podłączenie przełącznika do istniejącej sieci.

Obsługa protokołu 802.1q VLAN oraz agregacji połączeń to funkcje, dzięki którym przełącznik idealnie nadaje się do zastosowań w nowoczesnych sieciach LAN. Dzięki funkcji priorytetyzowania portów urządzenie zapewnia wysoką jakość działania takich usług, jak monitoring **CCTV czy VoIP.**

Najważniejsze cechy i funkcje przełącznika TL-SG1218MPE
- 16 portów RJ45 PoE+ 10/100/1000 Mb/s,
- 2 gigabitowe porty SFP,
- 802.3af/at: do 30 W na każdy port PoE, 192 W łącznej mocy zasilanych urządzeń,
- obsługa 802.1q VLAN oraz agregacja połączeń,
- tryb priorytetowania portów oparty na o 802.1p/DSCP,
- QoS, IGMP Snooping,
- możliwość montażu w szafie rack,
- intuicyjny interfejs WebGUI lub aplikacja do zarządzania.

Integracja zadaniem przemysłu

Ożywiona dyskusja o wyzwaniach, wobec jakich stają security menedżerowie w sektorze przemysłowym, toczyła się podczas kolejnego śniadania ekspertów. Dziękujemy za merytoryczną debatę i aktywny udział. Naszych gości zaprosiliśmy tym razem do hotelu Novotel Centrum Warszawa.

Tomasz Guzikowski

grupa kapitałowa CIECH

→ ***Oczywiście bardzo dziękuję za zaproszenie.*** *Pierwszy raz uczestniczę w takim spotkaniu, które dało podstawę do przemyśleń z różnej perspektywy, zarówno ze strony dostawców różnych rozwiązań, jak i biznesu, czyli tych, którzy potrzebują tych rozwiązań. Najważniejszą w moim przekonaniu konkluzją, którą z tego spotkania wyniosę, jest kwestia brakującego w pewnym sensie ogniwa, czyli tzw. integratora, który pomagałby łączyć wiedzę wynikającą z rozwiązań technicznych z potrzebami, które leżą po stronie biznesu.*

Mirosław Lukowski

ekspert

→ ***Kolejny udział w cudownym wydarzeniu, jakim jest śniadanie ekspertów,*** *które powinno uzyskać nazwę śniadania mistrzów, ale już była zarezerwowana. Kolejny raz mamy okazję spotkać się w supergronie fachowców, zarówno dostawców, jak i odbiorców. Może uda się znaleźć odpowiedź na pytanie, które dzisiaj padło: kim jest integrator. Bo brakuje definicji słowa integrator i organizacji, która jest prawdziwym integratorem systemów. Jest to nisza. I ze strony odbiorców i dostawców szukamy tego, kto będzie prawdziwym integratorem systemów.*

Janusz Syrówka

Innogy Polska

→ ***Bezpieczeństwo nie istnieje już jako odrębna dziedzina,*** *jest elementem procesów biznesowych i w ten sposób musimy do tego podchodzić, bo w przeciwnym razie funkcjonowanie bezpieczeństwa jako odrębnego bytu traci jakikolwiek sens.*

Maciej Chachulski

SAS Institute

→ ***Jest mi bardzo miło znaleźć się tutaj, na tym śniadaniu,*** *posłuchać, jakie problemy są w tej chwili na porządku dziennym w dziedzinie bezpieczeństwa przemysłowego, nie tylko w firmach przemysłowych, ale szeroko rozumianego bezpieczeństwa.*

Jacek Tobiasz

Grupa Żywiec

→ ***Wymiana takich poglądów jest dla mnie świeżym dostępem do bezpośredniej wiedzy*** *w naturalny sposób przekazany przez osoby bez żadnych pośredników, bez czytanego słowa, przez zadawanie pytań i odpowiadanie na nie, żywej dyskusji – formalnej i nieformalnej. Dla mnie jest to wartość nieoceniona, więc zawsze staram się uczestniczyć z wielką przyjemnością.*

Zbigniew Morawski

Hikvision Poland

→ ***Wspólnie doszliśmy do wniosku, że my producenci sprzętu,*** *który jest dostępny na rynku, nie zawsze potrafimy spełnić indywidualne oczekiwania dużych firm, dużych obiektów. W tym momencie okazuje się, że między nami powinien zaistnieć jeszcze jeden partner, który będzie integratorem tego całego rozwiązania.*

Karol Narojczyk

Seagate Technology

→ ***Najważniejszy wniosek jest taki, że podczas dyskusji została poruszona kwestia obecności security menedżerów,*** *pozyskiwania danych i obróbki tych danych, co z punktu widzenia mojej firmy jest bardzo cennym elementem biznesowym. I bardzo się cieszę, że branża jest świadoma, że pierwszą rzeczą, jaką powinniśmy uzyskać, jest informacja, dane, a później ich wykorzystanie w codziennej pracy.*

Artur Nowakowski

Linc Polska

→ ***Dużo ciekawych informacji mogliśmy tutaj usłyszeć od strony potrzeb, niebezpieczeństw,*** *jakie w przemyśle dostrzegamy. Moglibyśmy długo opowiadać o systemach zabezpieczeń elektronicznych czy o kamerach, o analityce, o systemach radarowych, systemach napłotowych. Jednak każdy z tych systemów jest systemem niezależnym, a co jest najważniejsze, co zostało poruszone na spotkaniu, jest to, aby te wszystkie systemy współpracowały jednocześnie. Jest ważne, aby ich współpraca przynosiła relatywnie wysokie efekty.*

Bogumił Szymanek

Axis Communications

→ ***To śniadanie naprawdę pokazało, że czasami nie do końca rozumiemy pewne problemy pojawiające się u klientów, albo o nich nie wiemy.*** *Dlatego warto dzielić się tymi informacjami. Najważniejszą konkluzją z tego spotkania jest przede wszystkim to, że powinniśmy starać się, żeby przekaz – przepływ informacji między wszystkimi stronami, starającymi się dostarczyć właściwe rozwiązania dla klienta, był jak najlepszy.*

Piotr Rodak

Schrack Seconet

→ ***Spotkanie bardzo udane, dużo ważnych kwestii*** *zostało poruszonych, związanych z kosztem wdrażania systemów, z opłacalnością. Są to takie rzeczy, na które warto zwrócić uwagę. Myślę, że tego typu spotkania są jak najbardziej potrzebne.*

NAJWIĘKSZE FIRMY BRANŻY SECURITY NA ŚWIECIE

LIDERZY
NA RYNKU DOZORU WIZYJNEGO ZDOMINUJĄ NASTĘPNĄ DEKADĘ

Redakcja a&s prezentuje własny ranking i raport „Security 50" za rok 2019, w którym zestawia spółki giełdowe o silnej globalnej pozycji w branży zabezpieczeń technicznych (elektronicznych i mechanicznych) na podstawie przychodów uzyskanych w 2018 r. ze sprzedaży produktów.

T E K S T
William Pao
a&s International

Pierwszym wrażeniem może być zdziwienie, gdyż z pozoru nic się nie zmieniło i pierwsza piątka największych firm specjalizujących się w dozorze wizyjnym niemal nie różni się od ubiegłorocznej. Jeśli jednak wgłębić się w szczegóły, porównać wielkość przychodów, ich wzrost w latach 2017-2018 oraz marże brutto, to o zaskoczeniu nie może być mowy. Można wręcz zaryzykować twierdzenie, że ze względu na duży zasięg rynkowy, ekosystemy partnerów, a także możliwości technologiczne te firmy będą dominować przez kolejną dekadę.

Okazuje się również, że zajmujące pozycje nr 1 i nr 2 firmy Hikvision i Dahua wyszły bez szwanku ze sporów handlowych pomiędzy Chinami i Stanami Zjednoczonymi. Wysiłki USA zmierzające (poprzez sankcje) do powstrzymania ekspansji obu firm – polegające m.in. na odsunięciu ich od projektów rządowych i ograniczeniu możliwości współpracy z podmiotami amerykańskimi okazały się nieskuteczne. W rzeczywistości, ze względu na kapitalizację liderów oraz wysoki popyt na rozwiązania security na rynku chińskim, obaj producenci zostawili swoją konkurencję daleko w tyle.

Oddajemy w ręce Czytelników kolejne wydanie raportu „Security 50", który – obejmując różne tematy (od trendów technologicznych, po sytuację na rynkach w poszczególnych regionach) – daje kompleksowy obraz branży security. □

10 NAJWIĘKSZYCH GLOBALNYCH PRODUCENTÓW BRANŻY SECURITY
(na podstawie przychodów ze sprzedaży produktów w 2018 r.)

Miejsce	Firma
1	Hikvision Digital Technology
2	Dahua Technology
3	ASSA ABLOY
4	Bosch Security Systems
5	Axis Communications
6	FLIR Systems
7	Uniview Technologies
8	Allegion
9	Tiandy Technologies
10	IDIS

50 największych firm z branży security

nadal osiąga wzrost sprzedaży w tempie dwucyfrowym

ŚREDNI WZROST FIRM Z NASZEGO ZESTAWIENIA „SECURITY 50" BYŁ W 2018 R. DWUCYFROWY. ZA ROZWÓJ WIĘKSZOŚCI DOSTAWCÓW Z NASZEJ LISTY ODPOWIADAJĄ GŁÓWNIE NAJPOTĘŻNIEJSZE RYNKI W TEJ BRANŻY, CZYLI STANY ZJEDNOCZONE I CHINY. TRZEBA JEDNAK ZAUWAŻYĆ, ŻE WIĘKSZOŚĆ TAJWAŃSKICH FIRM NADAL ZNAJDOWAŁA SIĘ W FAZIE SPOWOLNIENIA.

TEKST
Jill Lsi, William Pao

Pięćdziesiątka największych dostawców urosła w ubiegłym roku średnio o ok. 16 proc., przy czym 37 z nich odnotowało wzrost przekraczający 20 proc. To dowód, że dla branży security rok 2018 był udany.

Miejsca od 1. do 10. dostawców, którzy w rankingu „Security 50" mogą pochwalić się największym wzrostem, to: Megvii Technology, CP Plus, Kedacom, Costar Technologies, Uniview Technologies, Identiv, IDIS, Dahua, ASSA ABLOY i Magal. Największy skok w tej kategorii odnotowała firma IDIS – z 25. miejsca w ub. roku na pozycję nr 10 w tym roku.

Amerykański oddział ASSA ABLOY odnotował 9-procentowy wzrost. W swoim raporcie finansowym firma stwierdza: –*Popyt był silny w Ameryce Północnej i Łacińskiej na większości tamtejszych rynków. W USA wzrost był wyjątkowo duży w obszarze zamków elektromechanicznych – zarówno w segmencie klientów komercyjnych, w sektorze publicznym, jak i na prywatnym rynku mieszkaniowym. Pomimo rosnących kosztów materiałowych rentowność była nadal wysoka.*

– Amerykański rynek systemów zabezpieczeń wyszedł z krótkotrwałego spowolnienia w 2017 r., którego doświadczyło wiele firm, powracając w 2018 r. na ścieżkę szybszego wzrostu – powiedział Dror Sharon, dyrektor generalny Magal Security Systems. – *Także w regionach EMEA i APAC odnotowano w 2018 r. wzrost popytu i większą aktywność na tych rynkach, co przełożyło się na większe zainteresowanie potencjalnych użytkowników końcowych.*

– W obu Amerykach zwiększyły się możliwości sprzedaży we wszystkich działach biznesowych Costar Technologies. Niektóre z naszych działów, w tym Arecont Vision Costar, odnotowały także większą liczbę projektów na Bliskim Wschodzie i w regionie Azji i Pacyfiku – twierdzi Jeff Whitney, wiceprezes ds. marketingu w Arecont Vision Costar/Costar Technologies. – *Na wielu rynkach rośnie popyt na produkty, rozwiązania i technologie zabezpieczeń. W naszym przypadku oferta złożonej z wysokiej klasy produktów dla wielu różnych branż, wytworzonych w USA oraz w innych krajach, przekłada się na stały wzrost sprzedaży w wielu obszarach.*

Na rynkach wertykalnych wzrosty zanotowano we wszystkich głównych branżach. – *W ostatnim roku odczuliśmy zwiększony popyt na naszą linię produktów kontroli dostępu Hirsch w sektorze publicznym na wielu poziomach administracji: federalnym, stanowym i lokalnym. Rośliśmy także w sektorze edukacji. Zaobserwowaliśmy wzrost sprzedaży naszych rozwiązań do analizy wideo 3VR i analityki danych w handlu detalicznym i bankowości. Zainteresowanie naszym webowym rozwiązaniem do zarządzania kontrolą dostępu Liberty wykazywały głównie małe i średnie przedsiębiorstwa, handel detaliczny oraz rozpoczynające swoją działalność start-upy. Z kolei wykorzystującym definiowaną programowo architekturę (SDA- software defined architecture) rozwiązaniem Freedom interesowała się branża IT, przedsiębiorstwa, szkolnictwo na poziomie K-12 (podstawowym i średnim) oraz firmy zajmujące się innowacyjnymi i przyszłościowymi technologiami* – mówi Mark Allen, dyrektor generalny, Premises, Identiv.

Co ważne, coraz więcej dostawców zajmuje się tworzonymi dla różnych branż projektami dotyczącymi aplikacji niezwiązanych z zabezpieczeniami. Mają one ułatwiać użytkownikom końcowym wprowadzanie rozwiązań analityki biznesowej (*BI – business intelligence*) i osiąganie większej efektywności w zarządzaniu.

– Jednym z najważniejszych sektorów, na których koncentruje się Axis, jest handel detaliczny. Popyt na rozwiązania z obszaru dozoru wizyjnego wynika w tej branży nie tylko z tradycyjnej potrzeby zapewniania bezpieczeństwa, ale także z zapotrzebowania na aplikacje, które podniosą poziom obsługi klienta i usprawnią cały biznes. Konkretne przykłady wykorzystania kamer z wbudowaną analityką obejmują optymalizację rozkładu i ekspozycji sklepu, ograniczanie kolejek do kas i oraz efektywniejszą obsługę w okresie szczytów zakupowych – mówi Ray Mauritsson, prezes i dyrektor generalny Axis Communications. – *Obserwujemy również coraz większe zainteresowanie rozwojem bezpiecznych (i inteligentnych) miast. W tym przepadku ważna jest poprawa bezpieczeństwa, gdy kamery są skomunikowane z organami ścigania, wspomagając policję i inne służby miasta w zapewnieniu ochrony. Z drugiej strony ważny jest także aspekt poprawy wydajności i zrównoważony rozwój – kamery mogą np. pomóc w regulacji i optymalizacji przepływu ruchu, łącząc obraz na żywo z innymi źródłami danych.*

W przyszłym roku wymienione technologie i zastosowania powinny nadal cieszyć się zainteresowaniem klientów, a zastosowanie w aplikacjach niezwiązanych z zapewnieniem bezpieczeństwa wciąż będzie rosło. Jeśli chodzi o rozwój globalnego rynku zabezpieczeń technicznych, analitycy z Memoori przewidują w latach 2019-2024 średnią roczną stopę wzrostu na poziomie 10,7 proc. Niewiadomą pozostaje wpływ wprowadzonych przez USA sankcji handlowych na kondycję chińskich firm. Wyniki sprzedaży w 2019 r., które pojawią się w pierwszej połowie 2020 r., powinny już dać odpowiedź.

NAJWIĘKSZE FIRMY BRANŻY SECURITY NA ŚWIECIE

2019	2018	NAZWA FIRMY	SIEDZIBA	GŁÓWNY OBSZAR DZIAŁANIA	PRZYCHODY W 2018 R. (MLN USD)	PRZYCHODY W 2017 R.	WZROST PRZYCHODÓW 2017-2018
1	1	**HIKVISION DIGITAL TECHNOLOGY**	CHINY	różne	**7 039,0**	6 008,8	17,1%
2	2	**DAHUA TECHNOLOGY**	CHINY	różne	**3 574,9**	2 846,6	25,6%
3	3	**ASSA ABLOY** (Zamki elektromechaniczne i elektroniczne)	SZWECJA	kontrola dostępu	**2 897,2**	2 362,1	22,7%
4	4	**BOSCH SECURITY SYSTEMS**	NIEMCY	różne	**2 334,9**	2 272,4	2,8%
5	5	**AXIS COMMUNICATIONS**	SZWECJA	różne	**1 180,9**	988,5	19,5%
6	6	**FLIR SYSTEMS** (Commercial, Government, Defense)	USA	telewizja dozorowa	**1 057,8**	1 128,3	-6,3%
7	N/A	**UNIVIEW TECHNOLOGIES**	CHINY	telewizja dozorowa	**614,8**	468,3	31,3%
8	7	**ALLEGION** (Elektronika i kontrola dostępu)	USA	kontrola dostępu	**573,7**	505,7	13,4%
9	9	**TIANDY TECHNOLOGIES**	CHINY	telewizja dozorowa	**544,1**	476,7	14,1%
10	25	**IDIS**	KOREA	telewizja dozorowa	**505,4**	398,2	26,9%
11	8	**HANWHA TECHWIN**	KOREA	telewizja dozorowa	**505,1**	527,6	-4,3%
12	16	**TKH GROUP** (Systemy optyczne i security)	HOLANDIA	różne	**457,7**	422,0	8,5%
13	11	**AIPHONE**	JAPONIA	kontrola dostępu	**419,6**	408,5	2,7%
14	12	**INFINOVA**	CHINY	telewizja dozorowa	**320,6**	274,4	16,8%
15	15	**CP PLUS**	INDIE	telewizja dozorowa	**230,0**	169,2	35,9%
16	17	**NEDAP**	HOLANDIA	różne	**181,9**	178,4	2,0%
17	20	**KEDACOM**	CHINY	telewizja dozorowa	**175,4**	131,3	33,6%
18	14	**VIVOTEK**	TAIWAN	telewizja dozorowa	**168,2**	182,6	-7,9%
19	N/A	**MEGVII TECHNOLOGY**	CHINY	telewizja dozorowa	**159,7**	25,4	529,4%
20	21	**KOCOM**	KOREA	Home Security	**148,7**	130,0	14,3%
21	19	**MILESTONE SYSTEMS**	DANIA	telewizja dozorowa	**147,9**	139,4	6,0%
22	18	**RAYSHARP**	CHINY	telewizja dozorowa	**144,2**	140,7	2,5%
23	22	**COMMAX**	KOREA	kontrola dostępu i Home Security	**131,2**	127,4	3,0%
24	13	**OPTEX** (Detektory Security)	JAPONIA	sygnalizacja włamania	**130,2**	126,2	3,2%
25	23	**TAMRON** (Commercial / IOptyka przemysłowa)	JAPONIA	telewizja dozorowa	**115,4**	107,1	7,7%
26	26	**TVT DIGITAL TECHNOLOGY**	CHINY	telewizja dozorowa	**92,1**	78,9	16,8%
27	24	**NAPCO SECURITY TECHNOLOGIES**	USA	różne	**79,7**	79,4	0,4%
28	27	**MOBOTIX**	NIEMCY	telewizja dozorowa	**78,3**	77,2	1,4%
29	30	**SUPREMA**	KOREA	kontrola dostępu	**77,1**	67,7	13,8%
30	31	**FERMAX**	HISZPANIA	kontrola dostępu i Home Security	**73,8**	66,4	11,3%
31	33	**IDENTIV**	USA	kontrola dostępu	**72,0**	56,4	27,6%
32	29	**WANJIAAN INTERCONNECTED TECHNOLOGY**	CHINY	telewizja dozorowa	**70,9**	67,9	4,5%
33	28	**DYNACOLOR**	TAJWAN	telewizja dozorowa	**68,7**	73,4	-6,3%
34	32	**SYNECTICS** (Dział Systemów)	WLK. BRYTANIA	telewizja dozorowa	**65,2**	61,4	6,2%
35	36	**COSTAR TECHNOLOGIES**	USA.	telewizja dozorowa	**58,9**	44 3	33,1%
36	38	**C-PRO ELECTRONICS**	KOREA	telewizja dozorowa	**54,1**	46,6	15,9%
37	34	**GEOVISION**	TAJWAN	telewizja dozorowa	**49,1**	52,7	-6,8%
38	39	**INDIGOVISION**	WLK. BRYTANIA	telewizja dozorowa	**46,0**	42,1	9,2%
39	46	**MAGAL SECURITY SYSTEMS**	IZRAEL	różne	**37,1**	30,7	21,0%
40	41	**HITRON SYSTEMS**	KOREA	telewizja dozorowa	**37,0**	34,1	8,5%
41	42	**VICON INDUSTRIES**	USA	telewizja dozorowa	**27,7**	26,7	4,1%
42	45	**HI SHARP ELECTRONICS**	TAJWAN	telewizja dozorowa	**25,4**	25,0	1,7%
43	43	**ITX SECURITY**	KOREA	telewizja dozorowa	**25,1**	28,3	-11,0%
44	35	**ZENO TECHNOLOGY** (Videopark)	CHINY	telewizja dozorowa	**21,9**	48,8	-55,3%
45	44	**ACTI**	TAJWAN	telewizja dozorowa	**19,3**	25,7	-24,9%
46	47	**EVERFOCUS ELECTRONICS**	TAJWAN	telewizja dozorowa	**14,1**	18,8	-25,3%
47	49	**AV TECH**	TAJWAN	telewizja dozorowa	**11,8**	12,8	-8,5%
48	N/A	**iCATCH**	TAJWAN	telewizja dozorowa	**9,5**	10,8	-11,4%
49	50	**HUNT ELECTRONIC**	TAJWAN	telewizja dozorowa	**8,2**	9,1	-9,5%
50	N/A	**EVERSPRING INDUSTRY**	TAJWAN	kontrola dostępu	**7,6**	11,7	-35,1%

O RAPORCIE

Od 17. lat redakcja a&s International w swoim raporcie „Security 50" przedstawia ranking 50 największych firm w branży zabezpieczeń - takich, które uzyskują najwyższe przychody ze sprzedaży produktów na całym świecie. Ranking obrazuje dynamikę branży na podstawie różnych czynników rynkowych. Jej liderzy zdobywają rynek i podbijają światową gospodarkę, zaspokajając najważniejsze potrzeby klientów, związane z oferowanymi rozwiązaniami.

Ale raport „Security 50" jest czymś więcej niż tylko promocją technologii i produktów. Jego rolą jest także budowanie silniejszych więzi w ramach światowej elity branży security, prezentowanie oryginalnych poglądów dot. zarządzania przedsiębiorstwami, a także kwestii związanych z badaniami i rozwojem, umacnianiem biznesu, budowaniem marki, wyborem partnerów i wiele innych.

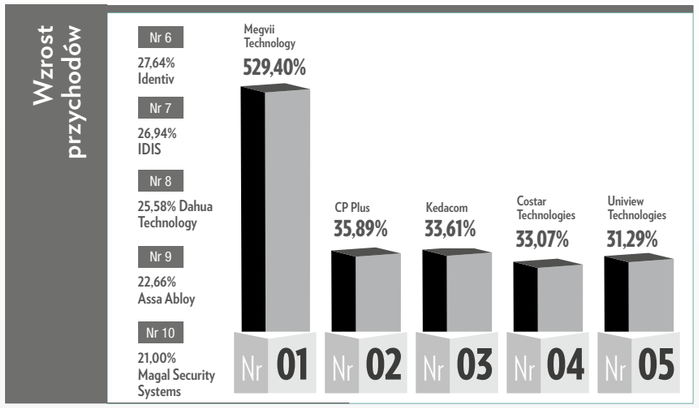
Redakcja dokonuje klasyfikacji światowych producentów wyłącznie na podstawie przychodów osiąganych ze sprzedaży produktów, zysku brutto, wielkości marży i zysku netto, ujawnionych w ich publicznych sprawozdaniach finansowych za rok budżetowy 2018. Zestawienie obejmuje zarówno producentów poszczególnych rozwiązań, jak i dostawców całościowych ofert.

W rankingu „Security 50" za rok 2019 mogły wziąć udział następujące firmy:

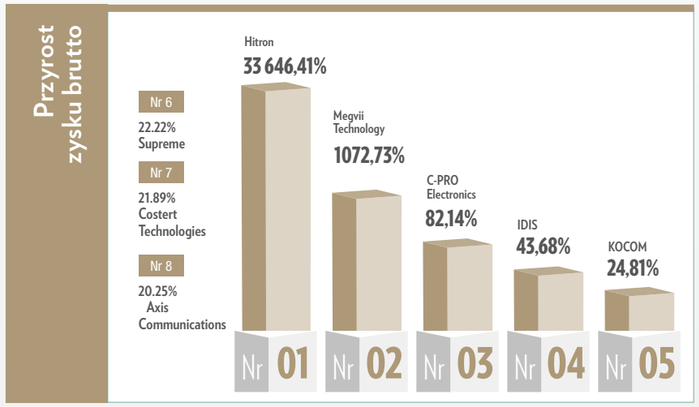
- Dostawcy elektronicznych urządzeń i systemów opartych na oprogramowaniu z zakresu: dozoru wizyjnego, kontroli dostępu i sygnalizacji włamania, którzy specjalizują się zarówno w kluczowych elementach, jak i wielu segmentach produktowych.
- Przedsiębiorstwa z branży ochrony lub zajmujące się wyłącznie produkcją, posiadające własne produkty, systemy, marki lub rozwiązania.
- Wyłączone zostały przychody z dystrybucji i integracji systemów, z działalności resellerskiej i dealerskiej, instalacji, usług ochrony, ochrony danych (informacji) i zabezpieczania ppoż. oraz inne powiązane.
- Podmioty, które przedstawiły sprawozdania finansowe za rok budżetowy 2018 i rok budżetowy 2017, zbadane i zatwierdzone przez biegłego księgowego lub firmę księgową.
- Publicznie notowane spółki giełdowe, a także niewielka liczba prywatnych, międzynarodowych firm, które wyraziły zgodę na udostępnienie swoich certyfikowanych raportów rocznych. Przed zakwalifikowaniem ich do rankingu są one szczegółowo weryfikowane przez zespół redakcyjny a&s pod kątem rozpoznawalności marki i udziałów w globalnym rynku.

Uwagi do danych finansowych:
a&s nie ponosi odpowiedzialności za informacje finansowe dostarczone przez poszczególne firmy. W celu rzetelnego porównywania walut spoza USA zostały one przeliczone na podstawie średnich rocznych kursów walut podanych przez *Internal Revenue Service*, działający według uchwalonej przez Kongres USA ustawy *Internal Revenue Code*. W rezultacie powstało jak najbardziej obiektywne zestawienie firm gotowych do dzielenia się swoimi wynikami sprzedaży. □

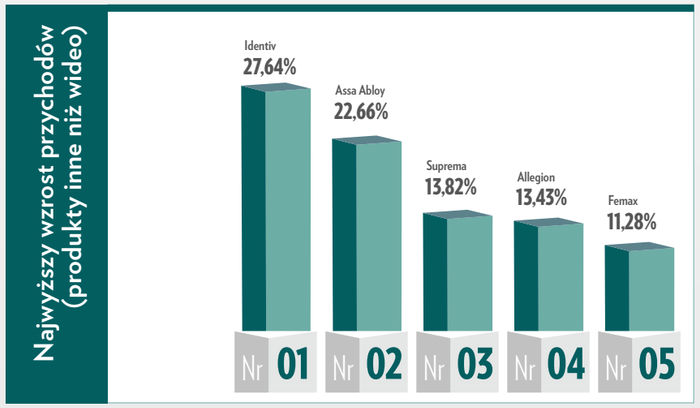
Z KOLEJNEGO RAPORTU „SECURITY 50", OBEJMUJĄCEGO WIELE TEMATÓW (OD TRENDÓW TECHNOLOGICZNYCH, PO SYTUACJĘ NA RYNKACH W POSZCZEGÓLNYCH REGIONACH) MOŻNA WYCIĄGNĄĆ CIEKAWE WNIOSKI. PREZENTUJEMY ANALIZY POD KĄTEM WYBRANYCH ZAGADNIEŃ.



W tym roku 37 firm odnotowało wzrost przychodów w latach 2017-2018, co wskazuje, że rok 2018 był kolejnym rokiem wzrostu dla graczy z branży security. Chińska firma Megvii zajmuje pierwsze miejsce pod względem wzrostu przychodów, osiągając wzrost o 529,4 procent w stosunku do przychodów w wysokości 25,37 mln USD w 2017 r. i 159,7 mln USD w zeszłym roku. Następne w kolejności są CP Plus, Kedacom, Costar Technologies i Uniview Technologies.



W tym przedziale dominują firmy koreańskie, Hitron zajął 1. pozycję ze wzrostem zysku brutto o prawie 34 procent w latach 2017-2018. Firma osiągnęła ujemny zysk brutto w 2017 r., ale w 2018 r. wzrósł on do 7,16 mln USD, by w 2018 r. osiągnąć przychód w wysokości 37,04 mln, co stanowi wzrost o 8,52 proc. w porównaniu z 34,14 mln w 2017 r. Po Hitronie kolejne miejsca zajmują Megvii, C-PRO Electronics, IDIS i KOCOM.

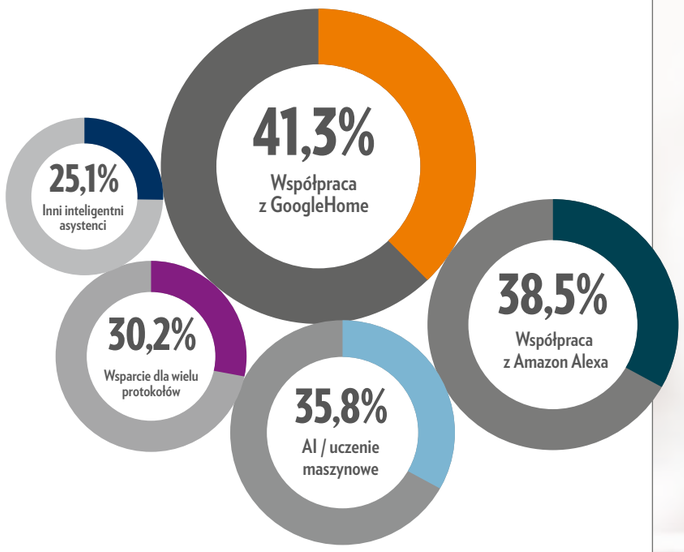


Interesujące jest, że firmy spoza sektora telewizji dozorowej zyskały najwyższy wzrost. W ramach tej kategorii Identiv, który oferuje kontrolę dostępu i rozwiązania RFID, zajmuje pierwsze miejsce, ze wzrostem o 27,64 proc. w porównaniu z 2017 r., przy wzroście 56,4 mln i 71,99 mln w zeszłym roku. Dalsze miejsca zajmują ASSA ABLOY, Suprema i Allegion.

Produkty automatyki domowej

Inteligentni asystenci, tacy jak Google Home czy Amazon, słynne głośniki rozwinęli w dużo większym stopniu niż tylko do zastosowań audio. W połączeniu z kilkoma innymi urządzeniami i sprzętem elektronicznym są one teraz wykorzystywane do zautomatyzowanych operacji, mogą m.in. uczyć się zachowań swoich właścicieli w czasie. Nic więc dziwnego, że tegoroczna integracja inteligentnych asystentów jest najbardziej poszukiwaną funkcją automatyki domowej.

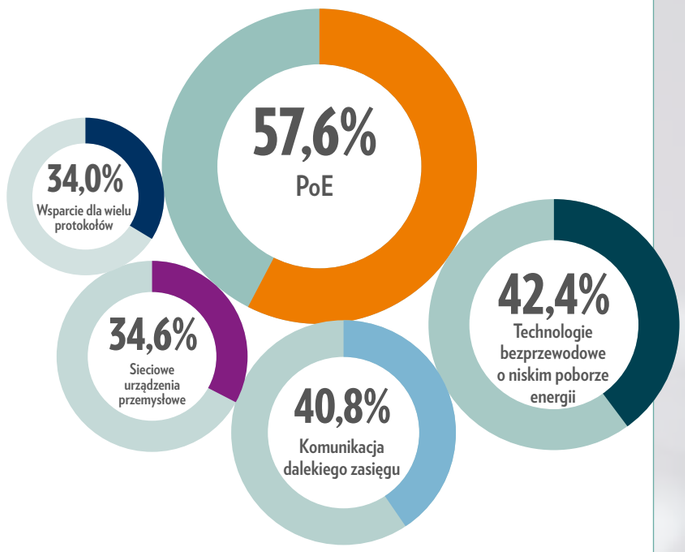
- 22,9% DIY
- 16,2% Współpraca z Apple Homekit
- 14,0% Współpraca z Microsoft Azure
- 10,1% Inne



Produkty transmisyjne

Klienci oczekują prostej instalacji i integracji z innymi systemami, co mogą uzyskać dzięki popularności technologii PoE (*Power-over Ethernet*). W miarę rozwoju technologii bezprzewodowej klienci są również zainteresowani rozwiązaniami komunikacyjnymi o niskim poborze mocy i dużym zasięgu. Wraz ze wzrostem liczby podłączonych urządzeń rozwiązania w zakresie bezprzewodowej transmisji mogą stać się kluczowym czynnikiem rozwoju w nadchodzących latach.

- 25,1% Komunikacja bliskiego zasięgu
- 15,7% Masowa transmisja danych



Rozwiązania kontroli dostępu

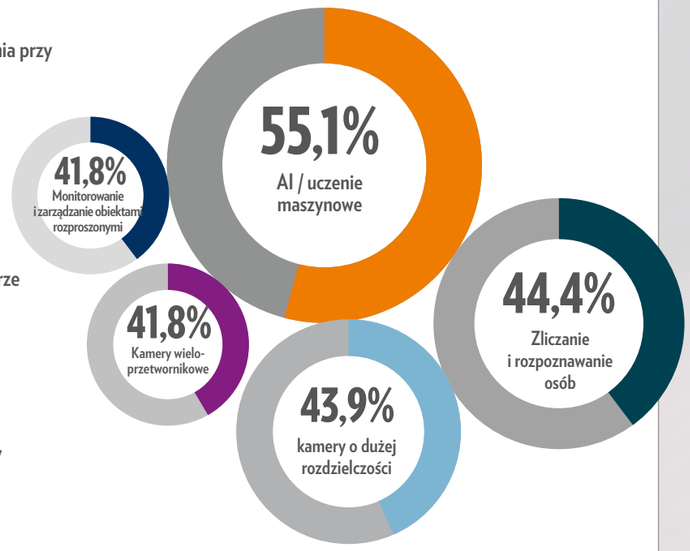
Kluczowym trendem kontroli dostępu, który pokazali producenci, jest coraz większe dostosowanie się do rozwiązań biometrycznych, takich jak rozpoznawanie twarzy i linii papilarnych. Biometria nie tylko zapewnia bezpieczniejszą niż tradycyjna metodę kontroli, ale także jest bardziej opłacalna, biorąc pod uwagę możliwą utratę kart dostępu. Integracja kontroli dostępu z innymi urządzeniami zabezpieczeń zyskuje także popularność wśród klientów zainteresowanych pozyskaniem kompleksowych rozwiązań.

- 30,6% Inna biometria: rozpoznawanie układu żył, tęczówki oka itp.
- 29,5% Skalowalny system zarządzania kontrolą dostępu
- 27,5% Uwierzytelnianie mobilne
- 24,4% Współpraca z innymi markami

Funkcje systemu dozoru wizyjnego

Wraz z najnowszymi osiągnięciami w dziedzinie sztucznej inteligencji klienci coraz częściej uświadamiają sobie potencjał zastosowania kamer dozorowych z funkcjonalnościami wykraczającymi poza rejestrowanie materiału. Użytkownicy końcowi chcą teraz móc identyfikować osoby za pomocą dostępnych funkcji, np. rozpoznawania twarzy i wesprzeć swój biznes, włączając takie funkcje, jak zliczanie osób.

- 38,3% Doskonałe rozwiązania przy słabym oświetleniu
- 38,3% Rozpoznawanie pojazdów i ich zliczanie
- 33,2% Zarządzanie w chmurze
- 25,0% Obrazowanie termowizyjne
- 22,4% Widok panoramiczny
- 5,6% Obrazowanie 3D



Rok 2019 był lepszy niż oczekiwano

Struktura popytu w sektorze dozoru wizyjnego wciąż jest jednak daleka od zrównoważonej

TEKST
Allan McHale
dyrektor, Memoori Research

WEDŁUG NAJNOWSZEGO RAPORTU FIRMY MEMOORI POŚWIĘCONEGO RYNKOWI ZABEZPIECZEŃ TECHNICZNYCH W ROKU 2019 WARTOŚĆ GLOBALNEJ PRODUKCJI W TEJ BRANŻY (LICZONA WEDŁUG CEN FABRYCZNYCH) WYNIOSŁA 34,31 MLD USD. OZNACZA TO WZROST O 8,5 PROC. W STOSUNKU DO 2018 R. ORAZ PRZEKŁADA SIĘ NA ŚREDNIĄ ROCZNĄ STOPĘ WZROSTU WYNOSZĄCĄ W OSTATNICH PIĘCIU LATACH 7,24 PROC.

To imponujący wynik, biorąc pod uwagę, że wzrost globalnego PKB wynosił w latach 2012-2017 średnio 2,7 proc. Tym samym branża security rośnie 2,6 razy szybciej.

W ciągu ostatnich 10 lat rynek zabezpieczeń technicznych rozwijał się w tempie liczonym średnią roczną stopą wzrostu na poziomie 6,27 proc. Prognozujemy, że w 2024 r. wartość oferty rynku osiągnie 56,76 mld USD, przy średniej rocznej stopie wzrostu wynoszącej do tego czasu 10,72 proc. Jednakże w każdym z trzech głównych segmentów (kontrola dostępu, dozór wizyjny i sygnalizacja włamania) oraz w poszczególnych regionach geograficznych będziemy obserwować wyraźne różnice tempa rozwoju.
W ciągu ostatnich 3 lat najszybciej rósł segment dozoru wizyjnego – w tempie 9,74 proc. rocznie. Zachodni producenci walczą tu z chińską konkurencją, wciąż jednak mając niewielkie możliwości penetracji chińskiego sektora publicznego. A Chiny to zdecydowanie największy i najbardziej jednolity lokalny rynek, odpowiadający szacunkowo za 35 do 40 proc. światowego popytu.

Można było oczekiwać, że nieco szybciej niż szacowane 8,2 proc. wzrostu będzie się rozwijał segment kontroli dostępu – przede wszystkim ze względu na coraz większe wykorzystanie sieci IP, wzrastające znaczenie biometrii i zarządzania tożsamością, rosnące zastosowanie systemów zamków bezprzewodowych, a także kontroli dostępu w formie usługi (ACaaS). Mógłby to być trzeci rok z rzędu o najwyższym tempie wzrostu spośród trzech segmentów rynku, ale na drodze stanęła presja cenowa i w pewnej mierze konsolidacja branży oraz niedoskonałość łańcucha dostaw. Wpłynęło to na mniejszy od spodziewanego wzrost wartości sprzedaży.

Segment systemów sygnalizacji włamania, na którym wyrosła cała branża zabezpieczeń elektronicznych, już dawno uzyskał swoją dojrzałość i stabilność. Jednakże coraz częstsze wykorzystanie radarów, a także kamer termowizyjnych i wielosensorowych przyczyniło się w 2019 r. do wzrostu o 3,8 proc. Wpływ na to miały także postęp w technologii czujników, technologie bezprzewodowe oraz integracja z systemami dozoru wizyjnego i kontroli dostępu oraz oświetleniem zewnętrznym. Trzeba przy tym założyć, że niektóre produkty dozoru wizyjnego mogą być wdrażane w projektach PP/IA, przez co nie są brane pod uwagę w tym segmencie. To może zakłócać szacunki tempa wzrostu na tym rynku.

Struktura popytu w branży nadzoru wideo nie jest ani zdrowa, ani zrównoważona, co wykazujemy w naszym raporcie. Okazuje się, że problem zagranicznych producentów, którzy starają się powiększyć swoje udziały na rynku chińskim, nie dotyczy kwestii technologicznych ani nawet wydajnościowych. U jego podstaw leżą wyzwania lokalne i geopolityczne. Największe znaczenie ma polityka rządzącej partii komunistycznej, która sprawuje pewną kontrolę także nad prywatnymi firmami produkującymi systemy dozoru wizyjnego. Chcąc więc robić interesy z sektorem publicznym (który odpowiada obecnie za ponad 50 proc. chińskiego rynku dozoru wizyjnego) i oczekując wsparcia w postaci długoterminowych tanich kredytów, trzeba postępować wg zasad ustalonych przez chiński rząd. A zdaniem administracji chińskiej w projektach obejmujących sektor publiczny nie mogą być stosowane urządzenia zagraniczne. W rezultacie nie ma mowy o otwartym handlu. Pozwoliło to dwóm głównym chińskim producentom (Hikvision i Dahua) zdobyć 40 proc. światowego rynku kamer CCTV/VSS – w dużej mierze dzięki agresywnej polityce cenowej. Żaden inny producent nie jest w stanie konkurować ceną na tak niskim poziomie, bo nie dysponuje takim wolumenem produkcji, jak dwaj wymienieni dostawcy.

Okazuje się, że także oni nie mogą spać spokojnie. Na horyzoncie pojawiają się inni chińscy producenci, którzy walczą o udział w ogromnych inwestycjach i projektach sektora publicznego, dotyczących budowy bezpiecznych miast. Przykładowo, Huawei – jedna z największych firm telekomunikacyjnych na świecie – rozwija obecnie produkcję kamer CCTV, a zajmujący się opartą na AI analizie zawartości wizji start-up Megvii chce oferować kompletne rozwiązania z zakresu dozoru wizyjnego. Nie ma wątpliwości, że ostatecznie będą oni wzmacniać swoją pozycję na rynku związanym z sektorem publicznym i powiększać własne udziały kosztem dwóch obecnych liderów. Efektem ubocznym mogłaby być przynajmniej mniejsza presja na niepochodzących z Chin producentów, działających na bardziej otwartym rynku światowym.

Prognoza rynkowa do 2024 roku

W naszej prognozie na najbliższe 5 lat (do 2024 r.) zakładamy brak poprawy sytuacji w światowym handlu oraz jedynie niewielki wzrost globalnego PKB przez następne dwa lata. Pomimo niesprzyjających warunków ekonomicznych, w ciągu ostatnich 5 lat branża security potrafiła osiągnąć solidny wzrost, na co wpływ miały nowe technologie zwiększające wydajność produktów oraz stale malejące koszty ich posiadania.

Należy zakładać, że w ciągu najbliższych 5 lat najprawdopodobniej nie dojdzie do zahamowania działań terrorystycznych, powinny więc rosnąć budżety państw przeznaczane na przeciwdziałanie temu zjawisku. Skorzystają na tym firmy działające w branży security. Z kolei w sektorze komercyjnym, obejmującym wszystkie trzy segmenty zabezpieczeń technicznych, będzie wzrastać zapotrzebowanie na coraz bardziej kompleksową komunikację, wspomaganą technologiami Internetu Rzeczy (IoT). Ten trend w pełni ujawni się do końca 2020 r. i będzie odpowiadać za wyraźne przyspieszenie rozwoju branży przez następne 4 lata.

Ostatecznie w ciągu najbliższych 5 lat (od 2019 do 2024 r.) przewidujemy średnią roczną stopę wzrostu rynku na poziomie 10,7 proc. (liczoną według wartości sprzedaży). Głównym czynnikiem rozwoju branży będzie oparte na sztucznej inteligencji (AI) oprogramowanie do analizy obrazu z kamer – niewielka dziś sprzedaż tego rodzaju rozwiązań ma do końca 2024 r. osiągnąć wartość 3,5 mld USD. Pociągnie to za sobą zwiększenie popytu na urządzenia systemów dozoru wizyjnego.

Przedstawione obserwacje i prognozy pochodzą z jedenastej edycji dorocznego raportu Memoori „*The Physical Security Business 2019-2024*”.

Czy tempo rozwoju chińskich firm spadnie?

OSTATNIA DEKADA TO DLA WIĘKSZOŚCI CHIŃSKICH FIRM OKRES NAJSZYBSZEGO ROZWOJU. ODKĄD USA STWORZYŁY SWOJĄ „CZARNĄ LISTĘ", WZROST CHIŃSKICH GIGANTÓW ZACZĄŁ JEDNAK WYHAMOWYWAĆ NIE TYLKO W STANACH ZJEDNOCZONYCH, ALE TAKŻE W INNYCH KRAJACH. NASUWA SIĘ WIĘC PYTANIE, CZY FIRMY TE BĘDĄ NADAL ROSŁY W SIŁĘ W NAJBLIŻSZYCH 5 LATACH.

TEKST
Jill Lsi, William Pao

Tegoroczny raport „Security 50" odnotował kolejny rekordowy przychód osiągnięty przez pięć największych firm w branży zabezpieczeń: Hikvision Digital Technology, Dahua Technology, Assa Abloy, Bosch Security Systems oraz Axis Communications. W sumie tych pięciu producentów generuje około 17 mld USD, co stanowi 68,4 proc. przychodów osiąganych przez wszystkie 50 firm ujęte w zestawieniu. Jeśli przyjrzeć się tylko segmentowi dozoru wizyjnego, to pierwsza piątka w tej kategorii (cztery firmy z globalnego TOP 5 oraz FLIR Systems), sprzedała produkty za 15 mld USD – to ok. 74 proc. całkowitych przychodów 41 firm specjalizujących się w monitoringu wizyjnym. Widać, że pięciu największych producentów zdominowało światowy rynek security i można zakładać, że w nadchodzących latach utrzymają one swoją wiodącą pozycję. Zajmujące pierwsze i drugie miejsce dwie chińskie firmy już osiągnęły ogromne rozmiary. Wielkie ambicje ma także Uniview Technologies, kolejny producent z Chin, który urósł o 31,3 proc. (z 468,3 mln USD w 2017 r. do 614,8 mln USD w 2018 r.) i chce stać się trzecią co do wielkości pochodzącą z Chin firmą w segmencie dozoru wizyjnego. Został on przejęty w 2018 r. przez China TransInfo, notowaną na giełdzie spółkę, która oferuje głównie systemy transportowe i rozwiązania bezpieczeństwa dla wielu lokalnych chińskich samorządów.

Więcej spółek giełdowych z Chin

Wraz z kapitalizacją, szybkim rozwojem rynku wewnętrznego i zachętami ze strony rządu będziemy obserwować, jak coraz więcej dużych chińskich graczy z branży security wchodzi na giełdę, i to niezależnie od toczącego się sporu handlowego między USA a Chinami. Nie można jednak zaprzeczyć, że ich rywalizacja z wieloma firmami spoza Chin nie jest oparta na uczciwych zasadach. Wskazuje na to analiza danych, które zbieramy każdego roku od większości spółek notowanych na giełdzie (IPO – *Initial Public Offering*) na całym świecie.
Nowym graczem na liście 20 największych dostawców w naszym rankingu „Security 50" jest też Megvii Technology. To wywodzący się z Chin start-up specjalizujący się w sztucznej inteligencji, a konkretnie w technologii rozpoznawania twarzy. W zeszłym roku firma osiągnęła rekordowy 529,4-proc. wzrost, zwiększając swoje przychody 25,37 mln USD w 2017 r. do 159,7 mln w 2018 r. Tym samym pod względem wzrostu przychodów jest niekwestionowanym liderem w naszym zestawieniu. Mimo że znajduje się na amerykańskiej „czarnej liście", firma przygotowuje się do swojego debiutu giełdowego. Jej śladem mogą chcieć podążać inne specjalizujące się w AI chińskie start-upy: SenseTime i YITU.

Hikvision i Dahua notują wzrost pomimo amerykańskiej „czarnej listy"

W 2018 r. firmy Hikvision i Dahua odnotowały przychody ze sprzedaży sprzętu w wysokości (odpowiednio) 7 mld USD i 3,6 mld USD, co stanowi wzrost o 17,14 i 25,58 proc. w porównaniu z 2017 r. Przez pierwsze trzy kwartały tego roku Hikvision zwiększał całkowity dochód operacyjny – do 39,84 mld RMB (ok. 6 mld USD), co stanowi wzrost o 17,9 proc. rok do roku. Obaj dostawcy nie przestają się rozwijać pomimo amerykańskiego zakazu sprzedaży ich produktów do agencji federalnych USA oraz umieszczeniu ich na „czarnej liście" ograniczającej amerykańskim firmom możliwości prowadzenia z nimi interesów. Struktura dochodów operacyjnych Hikvision ujawnia, że ich 71,53 proc. pochodzi z wewnętrznego chińskiego rynku, a rynki zagraniczne odpowiadają za 28,47 proc. W rezultacie, w porównaniu z 2017 r., krajowy rynek wzrósł o 20,18 proc., a sprzedaż zagraniczna o 15,9 proc. Można więc stwierdzić, że to lokalny biznes utrzymuje tempo wzrostu tej firmy.
Warto jednak zwrócić uwagę na dane sprzedażowe Dahua w okresie I-III kw. 2019 r. Przychód wyniósł 16,42 mld RMB (wskaźnik marży brutto), a wzrost rok do roku jedynie 9,30 proc. Ponieważ niektórzy amerykańscy klienci wyrażają obawy dotyczące możliwości współpracy z tymi dwoma gigantami (czy w ogóle z chińskimi firmami), to szybciej rosną przychody innych azjatyckich producentów, np. tajwańskiego VIVOTEK-a, który urósł w pierwszych trzech kwartałach 2019 r. o 34,72 procent - do około 189,6 mln USD.

W poszukiwaniu nowych rynków

Aby zrekompensować wszelkie straty na rynku amerykańskim, Hikvision i Dahua chętnie biorą udział w projektach w innych krajach i regionach. – *Zapotrzebowanie rynku na rozwiązania dla bezpiecznego miasta, inteligentnego handlu detalicznego oraz inteligentnego transportu szybko rośnie, zwłaszcza w Ameryce Łacińskiej i regionie Azji i Pacyfiku* – mówi Fu Liquan, prezes Dahua Technology. – *Jeden z naszych projektów dotyczy dostarczenia kompleksowego rozwiązania smart city dla metropolii w Ameryce Łacińskiej. Obejmuje ono ponad 1000 kamer, kompletne sieci transmisji, systemy przechowywania danych w chmurze, platformy zarządzania wideo, a także aplikacje big data do rozpoznawania pojazdów i ludzi (mające wspomagać lokalną policję w walce z przestępczością i zapewnić funkcje wczesnego ostrzegania w przypadku rozpoznania potencjalnie niebezpiecznych osób i pojazdów). Utworzone centrum monitorowania z ekranami LED oraz systemem dowodzenia i wsparcia służb pozwoliło znacznie poprawić wydajność pracy policji* – twierdzi Fu Liquan.

Skupienie się na branżach

Regionalna dywersyfikacja przychodów Hikvision i Dahua w dużej mierze wynika też ze strategii rozwoju tych firm. Obie przyjęły podejście „wertykalne" i postawiły na takie pozycjonowanie produktów i rozwiązań, by skupić się nie tylko na bezpieczeństwie, ale także na aplikacjach zwiększających wydajność i usprawniających procesy. Takie podejście, a także zwiększenia badań i rozwoju w zakresie sztucznej inteligencji i technologii głębokiego uczenia, przyczyniły się do wzrostu przychodów obu dostawców zarówno na rynku krajowym, jak i zagranicznych.
– *Hikvision uczestniczy w różnych projektach dotyczących zwiększenia efektywności biznesowej i automatyzacji na rynkach wertykalnych, rozwijając innowacyjne technologie, produkty i rozwiązania, szczególnie w obszarach zarządzania ruchem i handlu detalicznego wspartych AI* – mówi Keen Yao, wiceprezes Hikvision Digital Technology. – *Portfolio rozwiązań Hikvision z wbudowaną technologią AI w inteligentnym transporcie poszerzyło standardowy monitoring wizyjny o funkcje, które mogą w czasie rzeczywistym ostrzegać operatorów o problemach w ruchu drogowym. Dzięki temu mogą oni natychmiast podjąć działania, aby udrożnić trasy i utrzymać płynność komunikacji. Placówki handlu detalicznego wykorzystujące technologie AI otrzymują czytelny obraz przepływu klientów. Na tej podstawie mogą optymalizować rozkłady swoich sklepów, by zwiększyć sprzedaż i podnieść poziom obsługi kupujących, skracając kolejki do kas.*
– *Dahua rozwinęła rozwiązania oparte na standardach, dostarczając produkty dedykowane do zastosowań bezpiecznego miasta, inteligentnego ruchu, inteligentnego handlu detalicznego oraz w innych kluczowych branżach* – wyjaśnia Fu Liquan. – *Wprowadziliśmy również serię inteligentnych produktów front-end i serwerów, aby realizować scenariusze inteligentnych aplikacji nowej generacji i kompleksowo wspierać wdrażanie koncepcji Dahua HOC (Dahua Heart of City).*

Czego można się spodziewać w przyszłości? Chińskim firmom utrudniono ekspansję na rynki zagraniczne. To, czy giganci z Chin utrzymają wysokie wzrosty w ciągu najbliższych pięciu lat, będzie zależało od wielkości sprzedaży na rynku krajowym i zaufania zagranicznych klientów. ▫

Nowe możliwości przed branżą security

CHOĆ W BRANŻY ZABEZPIECZEŃ PANUJE OGROMNA KONKURENCJA, TO BRANŻOWI DOSTAWCY WCIĄŻ DOSTRZEGAJĄ NOWE SZANSE I OFERUJĄ ZAAWANSOWANE ROZWIĄZANIA MOGĄCE ZASPOKAJAĆ RÓŻNE POTRZEBY INTEGRATORÓW SYSTEMÓW I UŻYTKOWNIKÓW KOŃCOWYCH.

TEKST
William Pao

Nowe możliwości są związane ze sztuczną inteligencją (AI), przetwarzaniem w urządzeniach na brzegu sieci (*edge computing*), cyberbezpieczeństwem i wielu innymi zaawansowanymi technologiami.

Sztuczna inteligencja (AI)

Nie trzeba nikogo przekonywać, że analityka oparta na uczeniu maszynowym, głębokie uczenie czy sztuczne sieci neuronowe to obecnie bardzo gorące tematy. Rośnie liczba zastosowań, różnorodność i zasięg oddziaływania sztucznej inteligencji.

– Sztuczna inteligencja nadal będzie miała znaczący wpływ na transformację branży zabezpieczeń. AI radykalnie zwiększa skuteczność elektronicznych systemów zabezpieczeń, koncentrując uwagę operatorów na tym, co najbardziej istotne – mówi Alex Asnovich, wiceprezes ds. globalnego marketingu i komunikacji w firmie Avigilon. *– Podobnie jak obrazy o wysokiej rozdzielczości stały się podstawą działania nowoczesnych kamer dozorowych, tak przełomowym elementem systemów zabezpieczeń jest już dzisiaj i będzie w przyszłości technologia AI i korzyści, jakie ze sobą niesie. Umożliwiając przeszukiwanie treści obrazów wideo w czasie rzeczywistym, alarmy i automatyzację, Avigilon dostarcza skuteczne rozwiązania, dzięki którym łatwiej zmierzyć się z realnymi wyzwaniami dotyczącymi zapewnienia bezpieczeństwa.*

– W firmie Genetec aktywnie wykorzystujemy technologię głębokiego uczenia do tworzenia specjalizowanych rozwiązań, których działanie jest oparte na identyfikowaniu tendencji i odkrywaniu zależności obecnych w analizowanych danych. Obecnie zastosowaliśmy deep learning w AutoVu, naszym systemie rozpoznawania tablic rejestracyjnych (ALPR – Automatic License Plate Recognition), aby zwiększyć dokładność i wiarygodność odczytów numerów rejestracyjnych – wyjaśnia Daniel Lee, dyrektor zarządzający w Genetec, odpowiedzialny za region APAC. *– Dzięki zastosowaniu komputerowych algorytmów analizy wizji znacznie zmniejszyliśmy liczbę fałszywie pozytywnych odczytów w pracy funkcjonariuszy organów ścigania, którzy mają za zadanie zidentyfikować i zatrzymać podejrzany pojazd.*

Przetwarzanie na brzegu sieci

Rozwój technologii układów scalonych oraz udoskonalanie algorytmów AI sprawia, że na rynku jest coraz więcej kamer wspomaganych sztuczną inteligencją.

– Ciągły postęp w projektowaniu wydajniejszych procesorów (szybszych, o większej mocy obliczeniowej) pozwala nam tworzyć produkty, które są w stanie przetwarzać dane na brzegu sieci, czyli w pobliżu miejsca, w którym informacja jest generowana. W przypadku monitoringu wizyjnego oznacza to, że dane są przetwarzane w kamerze. W rezultacie pozwala to nie tylko zredukować szerokość pasma potrzebnego do transferu danych i pojemność pamięci masowej, ale także wdrażać wydajne i inteligentne systemy na dużą skalę. Co ważne, dane mogą być również anonimizowane i szyfrowane przed ich przesłaniem, co stanowi odpowiedź na obawy dotyczące ich bezpieczeństwa i prywatności – twierdzi Ray Mauritsson, prezes i dyrektor generalny Axis Communications.

– Jak mało kto w branży technologii wizyjnych wiemy, że wielu klientów, szczególnie z małych i średnich firm, nie potrzebuje złożonych systemów oraz skomplikowanego konfigurowania serwerów i pozostałej infrastruktury IT. Kiedy decydowali się na modernizację swojego systemu, wybierali rozwiązania CCTV IP, działające podobnie jak ich stare systemy analogowe, ale oferujące również wszystkie zalety sieciowego dozoru wizyjnego. To samo dotyczy dziś analityki opartej na algorytmach głębokiego uczenia. Dlatego to tak ważny powód, by dostarczać analitykę obsługiwaną wprost w kamerach – podkreśla Joon Jun, prezes Global Business Division w IDIS. *– Pracujemy obecnie nad wprowadzeniem do oferty nowej serii kamer AI 5MP z dokładniejszymi algorytmami analizy obrazu, które umożliwią zastosowanie aplikacji deep learning na brzegu sieci.*

Cyberbezpieczeństwo

To niezmiennie problem o kluczowym znaczeniu. Dostawcy potrafiący wykazać, że ich urządzenia są dobrze zabezpieczone przed cyberatakami, mogą liczyć na większe zainteresowanie integratorów i użytkowników końcowych.

– Rosnące zagrożenie cyberatakami to bardzo ważny problem dla wielu organizacji. Zwiększa się zapotrzebowanie na bezpieczniejsze i bardziej niezawodne rozwiązania, które mają funkcjonować w sieciach klientów. Dla takich rozwijających się gałęzi, jak centra danych, zakłady produkcyjne czy rynki finansowe, luki w zabezpieczeniach stają się sprawą kluczową – ocenia Richard Huison, dyrektor regionalny nowozelandzkiej firmy Gallagher Security na Wlk. Brytanię i Europę. *– Ochrona każdego systemu wymaga wiedzy, czy wszystko działa jak należy. W naszym centrum Gallagher Command Centre stale monitorujemy nasze zaszyfrowane urządzenia brzegowe, a tym samym na bieżąco jesteśmy w stanie wykryć każdą anomalię. Gdy to się stanie, informujemy o tym zdarzeniu odpowiedni zespół.*

– Wobec rosnącej skali cyberzagrożeń dostarczane oprogramowanie VMS musi być również zabezpieczone przed atakami hakerów, bez względu na to, czy ma być wykorzystywane lokalnie czy też – w celu obniżenia kosztów systemu i ulepszenia komunikacji – działać w chmurze. Kluczem w udanym wdrożeniu rozwiązań cyberochrony jest niezmiennie połączenie doskonalszych produktów, bardziej odpornych na ataki oraz edukacji użytkowników i integratorów – twierdzi Jeff Whitney, wiceprezes ds. marketingu w Arecont Vision.

– W początkowych fazach projektowania i rozwoju produktu stosujemy podejście zabezpieczeń wbudowywanych, którego celem jest standaryzacja protokołów cyberbezpieczeństwa w całym dziale badawczo-rozwojowym. Również po wprowadzeniu produktu na rynek nie przestajemy zajmować się potencjalnymi lukami w zabezpieczeniach, które można odkryć podczas testowania podatności. Analizujemy rodzaje cyberataków, które potencjalnie mogą przejmować, naruszać i unieruchamiać system – mówi Ross Wilks, dyrektor ds. komunikacji i marketingu w Vanderbilt. *– Firma Van-*

derbilt wdrożyła m.in. Flexible Secure Communications Protocol (FlexC), czyli wielościeżkowy, wielodostępny i wysoce zaszyfrowany protokół komunikacyjny, umożliwiający bezpieczne monitorowanie i kontrolę ścieżek komunikacyjnych IP. Protokół ten został zbudowany od podstaw wyłącznie pod kątem cyberbezpieczeństwa.

– Ciągłe doskonalenie naszego podejścia do bezpieczeństwa oznacza, że wbudowujemy je w nasze produkty i zmieniamy sposób myślenia o problemie. Niektóre z naszych zespołów zaczęły wykorzystywać Protection Poker – grę, której celem jest ograniczenie ryzyka w przepływie pracy – w celu oceny potencjalnego zagrożenia związanego z funkcjami aplikacji. W ten sposób zachęcamy zespoły do zwracania uwagi na kwestie bezpieczeństwa na wczesnym etapie procesu projektowania i do określenia działań zmierzających do wyeliminowania potencjalnych luk – wyjaśnia Tracy Kemp, wiceprezes w firmie Allegion. – *Zawody z obszaru cyberbezpieczeństwa wykorzystują rywalizację oraz celowo podatne na hakowanie aplikacje i strony internetowe. Członkowie zespołu dowiadują się, w jaki sposób aplikacje są atakowane, aktywnie wykorzystując elementy aplikacji podczas symulacji. Dzięki użyciu nowoczesnych narzędzi oraz budowaniu wiedzy i kompetencji z zakresu cyberbezpieczeństwa, Allegion może promować bezpieczne i odporne środowisko operacyjne.*

Ze sztuczną inteligencją, cyberbezpieczeństwem i gromadzeniem danych z różnych źródeł do celów szkoleniowych i analitycznych ściśle wiąże się prywatność informacji. Dlatego jej ochrona i sposób, w jaki te zbierane dane są zabezpieczane, to dziś bardzo ważny temat.

– W miarę jak branża wdraża najlepsze praktyki, by działać zgodnie z rygorystycznymi wytycznymi GDPR/RODO i innymi regulacjami dotyczącymi prywatności, konieczne będzie także rozwiązywanie kolejnych problemów. Będą one wynikać z tego, że zaufane rozwiązania z obszaru tożsamości gromadzą coraz więcej nowych danych, by móc podejmować bardziej inteligentne decyzje dotyczące uwierzytelniania i szkolić się w procesie optymalizacji obsługi użytkownika – twierdzi Alex Tan, dyrektor sprzedaży systemów kontroli dostępu w HID Global odpowiedzialny za region ASEAN.

Kontrola dostępu

W przypadku systemów kontroli dostępu możliwości również są ogromne, głównie dzięki Internetowi Rzeczy (IoT) i danym generowanym przez połączone w sieci urządzenia. – *Dostępne są nowe, bardziej elastyczne modele subskrypcji w obszarze usług kontroli dostępu, które umożliwiają odnawianie mobilnej tożsamości w przypadku, gdy użytkownik straci smartfon lub będzie musiał go wymienić. Można tworzyć lepiej skomunikowane i płynniej działające rozwiązania automatyki budynkowej do obsługi użytkowników, usuwając bariery w integracji systemów kontroli dostępu z aplikacjami inteligentnego budynku, usługami i wdrożeniami IoT. Można pozyskiwać cenne informacje ze współczesnych rozwiązań kontroli dostępu, korzystając z analityki opartej na uczeniu maszynowym. Efektem będzie poprawa bezpieczeństwa, spersonalizowana obsługa i łatwiejsze podejmowanie bardziej przemyślanych decyzji biznesowych. W naszych nowych produktach wykorzystujemy każdą z tych możliwości* – mówi Alex Tan.

Kolejne możliwości w obszarze kontroli dostępu dotyczą rozwiązań bezprzewodowych. – *Trendem, który ma duże przełożenie na sprzedaż, jest szybko rosnące zastosowanie rozwiązań bezprzewodowych. Systemy zamków bezprzewodowych są wygodniejsze w użytkowaniu, tańsze w instalacji i utrzymaniu, zużywają mniej energii* – wylicza Thomas Schulz, dyrektor ds. marketingu i komunikacji w ASSA ABLOY odpowiedzialny za region EMEA. – *Świadczą o tym dane przedstawione w naszym najnowszym raporcie „Wireless Access Control Report" z 2018 r. Trzy czwarte spośród ankietowanych instalatorów i integratorów potwierdza, że rozwiązania bezprzewodowe są łatwiejsze i szybsze w instalacji oraz bardziej opłacalne. Rynek coraz wyraźniej dostrzega te zalety, co znajduje odzwierciedlenie w rosnącej sprzedaży.*

Detekcja intruzów

W obszarze wykrywania wtargnięć systematycznie na znaczeniu zyskują technologie światłowodowe stosowane w ochronie obwodowej, zarówno detektory montowane na ogrodzeniu, jak i wkopywane w ziemię. – *Magal/Senstar niedawno wprowadził do oferty światłowodowy kabel sensoryczny FibrePatrol FP400 mocowany na ogrodzeniu, reagujący na jego wibracje spowodowane przez intruza. Jest przeznaczony do mniejszych instalacji. Każdy z sensorów obsługuje maks. cztery strefy wykrywania. Połączenie ich nieaktywnym kablem światłowodowym umożliwia zainstalowanie układu sterującego w odległości do 20 km od zabezpieczanego obwodu* – mówi Dror Sharon, dyrektor generalny Magal Security Systems. – *P400 dołącza do rodziny produktów Senstar FiberPatrol, która obejmuje montowane na ogrodzeniach detektory intruzów (instalacje o każdej wielkości), a także system zakopywany. Jako zaawansowane rozwiązanie ochrony perymetrycznej seria naszych produktów doskonale się sprawdza na dużych dystansach, np. w ochronie granic państwa lub zakopanych rurociągów.*

Inteligencja w celu poprawy wydajności

W ostatnim roku dostawcy rozwiązań security uczestniczyli w wielu złożonych projektach obejmujących różne branże. W takich wdrożeniach użytkownik końcowy dąży obecnie do zaspokojenia swoich potrzeb nie tylko związanych z ochroną, ale także skupiających się np. na usprawnianiu procesów i zwiększaniu wydajności.

- Handel detaliczny

Handel detaliczny działa w warunkach coraz większej konkuren-

cji. Dlatego firmy z tego sektora starają się lepiej rozumieć zachowania i potrzeby klientów, by optymalizować rozkład swoich sklepów, doskonalić ekspozycje towarów czy zapewniać lepsze wrażenia zakupowe. Mogą im w tym pomóc różne algorytmy analizy obrazu – od zliczania osób, które odwiedziły sklep czy zarządzania kolejkami. Kamera zintegrowana z systemem kasowym POS umożliwi określenie, jak wielu gości faktycznie dokonało zakupu. Powinno to ułatwić detalistom poprawę strategii sprzedażowych i marketingowych.

Dostępne są również zintegrowane rozwiązania mające zwiększać zaangażowanie klientów w trakcie zakupów określonych produktów. – *Poinformowaliśmy o poszerzeniu współpracy z Les Bouchages Delage, firmą produkującą specjalistyczne zamknięcia do butelek. Początkowo współpracowaliśmy z nią przy tworzeniu inteligentnych zakrętek z tagami NFC dla luksusowej marki koniaku, teraz wprowadzamy nasze technologie NFC do szerszej gamy korków i zakrętek z Les Bouchages Delage* – mówi Mark Allen, dyrektor generalny, Premises, Identiv. – *Chodzi o to, aby zwiększyć zaangażowanie konsumentów wokół produktu, butelki wina czy innego napoju alkoholowego. Konsumenci mogą teraz przyłożyć do nakrętki butelki smartfon z systemem Android lub iOS i łatwo zarejestrować swój zakup oraz otrzymać oferty specjalne. Chodzi więc o większe wykorzystanie technologii w celu kształtowania zachowań klientów, co jest korzystne dla wszystkich.*

– Media użytkowe i przemysł
To także sektory, których operatorzy coraz częściej polegają na rozwiązaniach telewizji dozorowej zintegrowanych z różnymi systemami automatyki w celu zapewniania kontroli jakości i serwisowania predykcyjnego (zapobiegawczego).

– *Obecnie dostawcy mediów użytkowych, takich jak energia elektryczna, surowce energetyczne, paliwo, woda, zaczynają stosować nasze kamery termowizyjne do obserwacji i detekcji w systemach ochrony obwodowej, a także radiometryczne kamery termowizyjne zintegrowane z oprogramowaniem do monitorowania zmian temperatury elementów, by zawczasu wyeliminować problemy procesów technologicznych* – wyjaśnia Daniel Gundlach, dyrektor generalny i wiceprezes ds. bezpieczeństwa w FLIR Systems. – *„Dane z oprogramowania analizującego obrazy z kamer skorelowane z danymi produkcyjnymi pozwalają zdalnie kontrolować sprzęt i stan wskaźników temperatury oraz identyfikować wszelkie elementy zagrożone przegrzaniem, zanim dojdzie do ich spalenia. Efektem są znaczne oszczędności dla klienta.*

– *Pewien szczególnie wymagający projekt wymagał zintegrowania systemu monitoringu wizyjnego IDIS ze zdalnie sterowanymi suwnicami pomostowymi, aby operatorzy mogli precyzyjnie, w czasie rzeczywistym synchronizować obrazy z kamer z funkcjonowaniem dźwigów* – mówi Joon Jun. – *Obraz z kamer został dostosowany do laserowego systemu pozycjonowania, a nowe rozwiązanie wdrożono w krótkim czasie podczas corocznej 20-dniowej przerwy. Obecnie, gdy operator steruje dźwigiem, system automatycznie przełącza widoki między ustawieniami kamery, a oparta na IP transmisja obrazu w czasie rzeczywistym umożliwia pozbawione opóźnień optymalne ruchy dźwigu. Rezultatem jest nie tylko poprawa wydajności i bezpieczeństwa, teraz wszystkie procesy są wsparte pełną wizualną ścieżką weryfikacji.*

– Transport, inteligentne miasto
W transporcie często stosuje się urządzenia security do usprawniania przepływu ruchu drogowego lub wykonywania innych zadań zarządzania ruchem. Przykładowo kamery zintegrowane z systemem zarządzania ruchem mogą umożliwiać samodostosowującej się sygnalizacji świetlnej ustalanie czasu świecenia się czerwonych lub zielonych świateł, w zależności od aktualnego natężenia ruchu. Kamery mogą też pomóc operatorom w opracowaniu lepszego planowania transportu. – *Przykładowo, są miasta wdrażające oferowane przez nas kamery razem z naszym oprogramowaniem Acyclica do zarządzania ruchem – celem jest poprawa mobilności. Gdy kamery termowizyjne wykrywają pojazdy, oprogramowanie analizuje statystyki miejsc docelowych, czasu podróży, postojów na świetle czerwonym lub jazdy na zielonym. Wszystkie te dane pomagają operatorom miast lepiej poznać wzorce dotyczące ruchu i zatorów, dzięki czemu mogą podjąć właściwe działania zmierzające do poprawy przepływności* – wyjaśnia Daniel Gundlach.

– Zarządzanie udostępnianiem obiektów
System kontroli dostępu można w coraz większym zakresie integrować z innymi systemami nie tylko w celu zwiększenia bezpieczeństwa, ale także usprawnienia zarządzania. – *Ostatnio Vanderbilt zastosował własne oparte na chmurze rozwiązanie kontroli dostępu i zarządzania obrazem wideo ACT365 w projekcie dla organizacji tenisowej LTA (Lawn Tennis Association). LTA chciała, by jej korty tenisowe były wykorzystywane w maksymalnym stopniu i codziennie udostępniane jak największej liczbie osób. Rozwiązanie ACT365 zostało zintegrowane z platformą ClubSpark, narzędziem do zarządzania obiektami firmy Sportlabs. W rezultacie powstał prosty w obsłudze system rezerwacji kortów, jednocześnie umożliwiający zarządzającym zdalną kontrolę dostępu na podstawie analizy „stanu bramki" w określonym obiekcie* – mówi R. Wilks. – *Korzystając z oprogramowania ClubSpark, gracze dokonują rezerwacji kortu i płacą za pomocą urządzeń mobilnych, a następnie otrzymują wiadomość tekstową z kodem PIN, który jest również przekazywany do systemu ACT365. Kiedy przybędą na kort i wprowadzą kod do czytnika, bramka się otwiera.*

Rosną potrzeby klientów

Branża security rozwija się we wszystkich regionach świata

NA CAŁYM ŚWIECIE ZAPOTRZEBOWANIE NA URZĄDZENIA I SYSTEMY ZABEZPIECZEŃ NIEZMIENNIE ROŚNIE. I NIC DZIWNEGO, UŻYTKOWNICY CHCĄ SIĘ BOWIEM ZABEZPIECZAĆ PRZED DZIAŁANIAMI PRZESTĘPCZYMI I TERRORYSTYCZNYMI. CORAZ WIĘCEJ KLIENTÓW STOSUJE TE ROZWIĄZANIA RÓWNIEŻ DO CELÓW NIEZWIĄZANYCH Z BEZPIECZEŃSTWEM, STARAJĄC SIĘ UZYSKAĆ WIĘKSZY ZWROT Z INWESTYCJI.

TEKST
William Pao

Wzrost sprzedaży na rynku amerykańskim utrzymuje się, użytkownicy końcowi niezmiennie inwestują w bezpieczeństwo. Pomimo obaw związanych z recesją w perspektywie krótkoterminowej można się spodziewać, że ten trend zostanie tu utrzymany. Także EMEA (Europa, Bliski Wschód i Afryka) oraz APAC (kraje Azji i Pacyfiku) to rynki przeżywające rozwój – w tych regionach użytkownicy inwestują w technikę ochronną nie tylko ze względów bezpieczeństwa.

Ameryka Północna

Jeśli przyjrzeć się danym makroekonomicznym, to wg Banku Światowego gospodarka amerykańska odnotowuje w ostatnich latach wzrost. Najnowsze dane mówią o 2,9-proc. w 2018 r. oraz o przewidywanym na ten rok na poziomie 2,5 proc.

Wyniki branży security w Ameryce Północnej są zatem w dużej mierze zgodne z opisanym trendem wzrostowym. – *Ameryka Północna jest tradycyjnie jednym z największych rynków zbytu dla producentów zabezpieczeń elektronicznych. Silna w ostatnich latach tamtejsza gospodarka napędzała inwestycje w zabezpieczenia. Przewiduje się, że na tym rynku stopa wzrostu w naszej branży wyniesie 5–7 proc.* – mówi Daniel Gundlach, dyrektor i wiceprezes ds. bezpieczeństwa w firmie FLIR Systems.

– W roku 2018 nadal obserwowaliśmy dużą tendencję wzrostową w naszej działalności. Zanotowaliśmy duży wzrost, bo o ponad 25 proc., na co złożył się wzrost zarówno organiczny, jak i wynikający z przejęć. Ogólne wrażenie jest takie, że nasza branża stale się rozwija – twierdzi Mike Mathes, wiceprezes Convergint Technologies.

Zwiększenie zagrożeń i regulacje to czynniki mające wpływ na inwestycje

Obawy związane z bezpieczeństwem to nadal główny powód inwestowania użytkowników końcowych w zabezpieczenia, niezależnie od branży. – *Większość firm nadal wydaje znaczne kwoty, a projekty rządowe i związane z sektorem publicznym są stabilne* – ocenia Thomas Cook, wiceprezes ds. sprzedaży w Hanwha Techwin America. – *Sporo inwestuje szkolnictwo na poziomie podstawowym i średnim (K-12). Ten sektor szybko się rozwija, głównie ze względu na pilną potrzebę zabezpieczenia przed atakami z użyciem broni palnej. Strzelaniny to prawdziwa epidemia w Ameryce Północnej, dlatego szkoły wprowadzają wzmocnioną ochronę jako środek zapobiegawczy.*

– Nasi najważniejsi klienci z obszaru ochrony obwodowej: lotniska, centra danych, dostawcy mediów użytkowych inwestują w kamery termowizyjne o dużym zasięgu i rozwiązania radarowe. W ten sposób chcą zapewnić redundancję i zwiększone pokrycie w celu identyfikowania zagrożeń poza obszarem objętym ochroną obwodową, zanim intruz dotrze do linii ogrodzeń. Z kolei nasi klienci komercyjni inwestują w rozwiązania zdalnego monitoringu i weryfikacji wizyjnej, aby lepiej chronić swój majątek i zmniejszyć ewentualne straty – wyjaśnia D. Gundlach. – *Międzynarodowy port lotniczy Norman Y. Mineta San Jose w Dolinie Krzemowej to ważny projekt wykorzystujący rozwiązania FLIR w systemie wykrywania włamań na obwodzie zabezpieczanego terenu.*

Również przepisy prawne mają bardzo istotny wpływ na zwiększanie popytu w różnych branżach, począwszy od infrastruktury krytycznej, skończywszy na handlu produktami z konopi indyjskich. – *Rynki w wysokim stopniu regulowane nadal są motorem inwestycji w bezpieczeństwo. Porty lotnicze i morskie, instytucje finansowe i przedsiębiorstwa użyteczności publicznej – w tych obiektach infrastruktury krytycznej zaostrzone przepisy mają wpływ na stosowanie systemów zabezpieczeń. Tacy klienci muszą nie tylko działać zgodnie z przepisami prawa, ale także w sposób jak najbardziej efektywny, wykorzystując systemy, w których zostały uwzględnione także kwestie cyberbezpieczeństwa* – mówi Mike Mathes.

– OObserwujemy ekspansję działalności biznesowej związanej z obrotem produktów z konopi indyjskich, który zalegalizowano w większej liczbie stanów USA i Kanadzie. Surowe przepisy dotyczące bezpieczeństwa w tym sektorze również przyczyniają się do rozwoju naszej branży – twierdzi Thomas Cook.

Nie tylko bezpieczeństwo

Użytkownicy końcowi w Ameryce Płn. w dążeniu do maksymalizacji zwrotu z inwestycji zaczynają wykorzystywać urządzenia zabezpieczające także do zastosowań innych niż ochrona. Trend ten jest szczególnie widoczny w sektorze handlu detalicznego.

– *Użytkownicy coraz częściej poszukują zaawansowanych rozwiązań, które nie tylko zapewniają bezpieczeństwo, ale także przyczyniają się do poprawy wyników swojej działalności. Sztuczna inteligencja ma coraz większy wpływ na handel detaliczny, umożliwiając lepsze poznanie zachowań klientów oraz identyfikowanie zagrożeń dla biznesu* – mówi Mike Mathes.

NAJWIĘKSZE FIRMY BRANŻY SECURITY NA ŚWIECIE

– Handel detaliczny jest branżą, która chce korzystać z rozwiązań security wspieranych analityką biznesową (business intelligence), chociaż mogę wymienić też inne, takie jak spedycja, zakłady produkcyjne i przetwórcze. Detaliści coraz chętniej korzystają z analityki biznesowej, aby dynamicznie podnosić poziom obsługi swoich klientów podczas zakupów – podkreśla Thomas Cook.

Kolejnym sektorem, w którym rozwiązania branży security są integrowane z innymi systemami, jest transport. Pomaga to np. w zarządzaniu ruchem drogowym i inteligentnym parkowaniu. – *Przykładem są miasta wdrażające oferowane przez nas kamery termowizyjne wraz z naszym oprogramowaniem Acyclica do zarządzania ruchem – celem jest poprawa mobilności. Gdy kamery termowizyjne wykrywają pojazdy, oprogramowanie analizuje statystyki miejsc docelowych, czasu podróży, postojów na czerwonym lub jazdy na zielonym świetle. Wszystkie zebrane dane pomagają miastom lepiej rozumieć wzorce dotyczące ruchu i przyczyny tworzenia się zatorów, dzięki czemu mogą podjąć właściwe działania zmierzające do poprawy przepływności* – mówi Daniel Gundlach.

W przyszłym roku firmy z branży security w regionie Ameryki Północnej będą zmuszone działać w niepewnym otoczeniu gospodarczym. Rozwój rynku może być utrudniony przez trwający spór handlowy pomiędzy Chinami a USA oraz wybory prezydenckie w Stanach Zjednoczonych.

– Przyszły 2020 rok to czas wyborów prezydenckich w USA. Jeśli spojrzeć wstecz, to w takich latach zawsze dochodziło do spowolnienia gospodarczego. Głównym powodem jest to, że wiele dużych korporacji zaczyna zachowywać się ostrożniej, jeśli chodzi o wydatki, i trwa to aż do zakończenia wyborów, czyli do listopada – wyjaśnia T. Cook. – Ale nawet nie biorąc pod uwagę wyborów, większość analityków finansowych przewiduje recesję. Obecnie przeżywamy najdłuższy okres bez recesji, więc jeśli ona nadejdzie, wpłynie to na całą gospodarkę.

Większość rynkowych graczy – przynajmniej z branży zabezpieczeń – wykazuje jednak sporo optymizmu. Ich zdaniem rynek nadal będzie podążał ścieżką wzrostu. – *Słyszymy obawy dotyczące ogólnego spowolnienia, do którego miałoby dojść w 2020 r. Nie zauważamy, by którykolwiek z naszych klientów zachowywał się w sposób zwiastujący ograniczanie wydatków w przyszłym roku* – ocenia Mike Mathes.

– Kwestią, która może znacząco wpłynąć na poziom wzrostu, są natomiast sankcje gospodarcze. Jednakże we FLIR sami projektujemy i wytwarzamy większość naszych produktów, nie korzystając z komponentów, na które mogą mieć wpływ obecne lub przyszłe ograniczenia w handlu – twierdzi Daniel Gundlach.

EMEA (Europa, Bliski Wschód i Afryka)

Region EMEA jest kolejnym rosnącym rynkiem, na którym użytkownicy końcowi inwestują w ochronę, ale nie tylko ze względów zapewnienia bezpieczeństwa, lecz także innych powodów.

Według Banku Światowego gospodarki państw z regionu EMEA powiększą się w 2020 r. średnio o 2,7 proc. (Europa) i o 3,2 proc. (Bliski Wschód i Afryka Północna). Ten wzrost znajduje odzwierciedlenie w wynikach finansowych firm działających w tych rejonach świata – *Choć tempo, w jakim rośniemy, różni się w zależności od kraju, to osiągnęliśmy 8-9-proc. wzrost w regionie, a na niektórych rynkach lokalnych nawet 18-proc.* – twierdzi Thomas Lausten, dyrektor generalny MOBOTIX.

Siłą napędową rozwoju branży jest wciąż potrzeba rozwiązań, które zapewniają ochronę techniczną i cyberbezpieczeństwo. – *Kwestie cyberbezpieczeństwa zyskały na znaczeniu w 2018 r. ze względu na stosowanie urządzeń niedostatecznie zabezpieczonych przed atakami hakerów, a także w odpowiedzi na pogarszającą się sytuację geopolityczną. Uważam, że te czynniki będą stanowić wyzwanie dla naszej branży w nadchodzących latach, ale mogą też pomóc rynkowi osiągnąć dwucyfrowe stopy wzrostu* – twierdzi Thomas Lausten.

Z cyberbezpieczeństwem ściśle wiąże się ochrona prywatności. Wraz z przyjęciem dyrektywy GDPR/RODO dostawcy, których produkty i rozwiązania są certyfikowane pod kątem

spełniania wymogów nowych przepisów, mogą skuteczniej konkurować i wyróżniać się na rynku.

– Poświęciliśmy wiele czasu, by upewnić się, że nasz system VMS jest zgodny z GDPR. Możemy z dumą pochwalić się, że byliśmy pierwszym dostawcą zaawansowanego oprogramowania do zarządzania wideo, które uzyskało tak pożądaną certyfikację zgodności z nowymi przepisami – podkreśla Malou Toft, wiceprezes EMEA w Milestone Systems. Rozwiązanie tej firmy XProtect Corporate 2019 R2 uzyskało niedawno certyfikat GDPR-ready wydany przez niezależny instytut EuroPriSe (*European Privacy Seal*). *– Dzięki certyfikacji GDPR-ready użytkownicy końcowi mogą być pewni, że dysponują odpowiednią podstawą do stworzenia instalacji dozoru wizyjnego zgodnego z ustawą o ochronie danych osobowych. Dokładamy również starań, aby operatorzy monitoringu wizyjnego wiedzieli, jak planować i radzić sobie z wymogami GDPR. Oferujemy szkolenia dla operatorów, którzy mogą nie wiedzieć, jak się do tego zabrać. Całemu personelowi operacyjnemu zapewnimy wsparcie w zdobyciu niezbędnej wiedzy – dodaje.*

Aplikacje niezwiązane z zapewnieniem bezpieczeństwa

Coraz więcej użytkowników z różnych branż ma świadomość korzyści, jakie można odnieść, wykorzystując rozwiązania oferowane przez branżę security w zastosowaniach innych niż ochrona. *– Generalnie klienci są coraz bardziej świadomi dostępnych opcji. Wiedzą, że zwrot z inwestycji nie opiera się już tylko na zapewnieniu bezpieczeństwa, ale także może wynikać z wykorzystania wielu danych, dzielenia się informacjami i stosowania konwergentnych rozwiązań* – mówi Thomas Lausten. *– Zastosowanie kamer dostarczających wysokiej jakości obraz może nie tylko zaspokoić coraz większe potrzeby w zakresie ochrony, ale także dzięki wbudowanej sztucznej inteligencji pomóc w osiąganiu lepszych wyników sprzedaży lub ograniczaniu strat w zakresie wydajności.*

Swoją tezę Malou Toft ilustruje kilkoma przykładami. *– W wielu krajach sposób tworzenia rozkładów jazdy transportu publicznego, np. pociągów, opiera się na danych historycznych lub niewielkich porcjach informacji, często zbieranych ręcznie. Wykorzystując anonimizowane metadane wizyjne, można śledzić, gdzie i kiedy zatłoczenie jest wysokie, by zaplanować rozkłady jazdy pociągów znacznie efektywniej. To tylko jeden z wielu procesów, które można zautomatyzować i uczynić bardziej precyzyjnymi* – wyjaśnia. *– W naszym regionie funkcjonuje sieć detaliczna, która testuje nową koncepcję sprzedaży w swoich sklepach. Stworzenie projektu sklepu od nowa wiąże się z ogromnymi kosztami, dlatego trzeba mieć 2, 3 placówki pilotażowe, w których wprowadza się alternatywne układy i ekspozycje, a następnie wykorzystuje dostępne czujniki i kamery do testowania przepływu klientów i ich reakcji na nowy projekt. Zasadniczo dane wizyjne ułatwiają eksperymentowanie i sprawdzanie prototypowych rozwiązań przed wprowadzeniem nowej koncepcji na wielką skalę. W ten sposób zyskujemy większą pewność przy podejmowaniu decyzji, co oczywiście będzie miało duży wpływ na wyniki finansowe* – wyjaśnia.

APAC (Azja i kraje Pacyfiku)

Sprzedaż rośnie także w regionie APAC, chociaż jej skala różni się w zależności od kraju. *– Na szybko rozwijających się rynkach, takich jak Wietnam, Filipiny, Indie i Indonezja, notujemy dwucyfrowy wzrost. Ugruntowane rynki, np. Singapur, będą miały dość niskie tempo wzrostu* – mówi Patrick Lim, dyrektor ds. strategii w Ademco Security Group. *– Z kolei gospodarka Hongkongu najprawdopodobniej poniesie spore straty spowodowane problemami wewnętrznymi, chociaż z powodu wielu szkód w infrastrukturze projekty związane z jej odtworzeniem mogą w rzeczywistości nieznacznie przyspieszyć rozwój branży bezpieczeństwa.*

– W regionie APAC nasze przychody wzrosły o 22,5 proc. Odnieśliśmy duży sukces w Australii, szczególnie w sektorach transportu i centrów danych, w bezpieczeństwie publicznym i obszarze egzekwowania prawa. W Indiach coraz częściej współpracujemy z sektorem budownictwa i klientami z branży przemysłowej, a w regionie ASEAN (Stowarzyszenie Narodów Azji Południowo-Wschodniej) odnieśliśmy wiele sukcesów, realizując projekty dotyczące BPO, ropy i gazu, szpitali i lotnisk. Obserwujemy również zwyżkowy trend w obszarze bezpiecznego i inteligentnego miasta oraz nowe możliwości związane z coraz większą liczbą modernizowanych i budowanych od podstaw lotnisk – twierdzi Daniel Lee, dyrektor zarządzający w Genetec odpowiedzialny za region APAC.

Główne czynniki wzrostu są związane z działaniami samorządów regionalnych w kierunku budowy inteligentnych miast, z różnymi projektami infrastrukturalnymi i generalnie z boomem budowlanym w regionie. Kluczową rolę odgrywają również regulacje rządowe wymagające, by budynki i obiekty spełniały określone normy. *– Rozwój branży zabezpieczeń stymulują rządowe przepisy dotyczące wysokich budynków i obiektów publicznych, tworzących różnego rodzaju centra. Powstaje wiele wieżowców, hoteli i projektów deweloperskich* – ocenia Sovan Hok, dyrektor generalny S Era Automation. *– Boom w budownictwie pobudza zapotrzebowanie na systemy zabezpieczeń.*

Nie ma wątpliwości, że branża security będzie nadal rozwijać się w tym regionie, chociaż pojawiły się pewne problemy, które mogą mieć negatywny wpływ na wzrost tego rynku. *– Wojna handlowa na linii USA – Chiny, a także możliwe globalne spowolnienie gospodarcze to czynniki, które mogą spowalniać rozwój branży – zauważa S. Hok.*

– Wojna handlowa USA-Chiny to poważny problem wpływający na rynek zabezpieczeń w Państwie Środka. Gdy dojdzie do wzrostu niepokojów społecznych i napięć w handlu, to poziom zaufania w obszarze inwestycji spadnie, a to będzie rzutować na całą Azję – twierdzi P. Lim. *Od połowy 2019 r. narastają wątpliwości wokół sporu handlowego między USA i Chinami, pojawiająca się niepewność znacznie spowolniła rynek. Sądzę, że w 2020 r. nadal będzie wiele obaw. Coraz więcej chińskich produktów jest „pod lupą", co odbija się na kosztach i będzie prowadzić do dylematów wokół zamówień związanych z projektami.* □

Sztuczna inteligencja *(**AI**) była gorącym tematem ostatnich targów ISC West, największej amerykańskiej imprezy w branży zabezpieczeń. Jej praktyczne zastosowania wiązały się głównie z kamerami dozoru wizyjnego i analizą wizyjną. Ważna ścieżka tematyczna, będąca niejako zaproszeniem dla firm zainteresowanych tworzeniem aplikacji AI, dotyczyła potrzeby nowych standardów dla kamer i możliwości współpracy urządzeń różnych firm.*
***Producenci rozwiązań wciąż pracują nad tym**, jak najlepiej wykorzystać pokaźną ilość gromadzonych danych. Potencjał sztucznej inteligencji można wykorzystać wyłącznie poprzez korelację wielu punktów danych i analizowanie mnóstwa informacji.*

SZTUCZNA INTELIGENCJA coraz chętniej wykorzystywana

GŁÓWNI GRACZE W BRANŻY SECURITY RYWALIZUJĄ, TWORZĄC WŁASNE PROCESORY (UKŁADY SCALONE SPECJALIZOWANE, CHIPSETY) PRZYSTOSOWANE DO WYMAGAŃ SZTUCZNEJ INTELIGENCJI.

TEKST
a&s International

Branża zabezpieczeń stoi na progu ery sztucznej inteligencji. Zainteresowanie użytkowników tą technologią jest bardzo duże. Większość producentów kamer zamierza implementować AI w swoich urządzeniach. Sposób, w jaki to zrobią, zależy m.in. od wykorzystanych typów układów (np. x86, ARM, FPGA). W pozyskiwaniu niezbędnych technologii firmy stosują różne podejścia.
Duzi gracze – tacy jak Hikvision, Hanwha Techwin czy Axis – dysponują możliwościami, by rozwijać własne procesory (chipsety – układy scalone specjalizowane) wspierające AI. Procesory najnowszej generacji muszą być przystosowane do potrzeb uczenia maszynowego – wymagają ogromnych możliwości obliczeniowych, muszą być wydajniejsze i bardziej energooszczędne od procesorów Nvidia. Mniejsi będą najprawdopodobniej technologie AI kupować od dostawców niezależnych w postaci obowiązkowego zestawu algorytmów wprowadzonych do systemu operacyjnego, układów scalonych lub oprogramowania układowego.

Jednym z przykładów stworzonego we własnym zakresie procesora z wbudowaną AI jest prezentowany podczas targów w Las Vegas ARTPEC 7 firmy Axis Communications. Według producenta zapewnia on lepszej jakości wyraźniejszy obraz poruszających się obiektów i większą szczegółowość w scenach prześwietlonych (technologia forensic WDR), ma więc większe możliwości analizy zawartości wizji. Możliwość przeprowadzania analizy wizyjnej w urządzeniach brzegowych ogranicza wymaganą przepustowość łącza i pozwala efektywnie wykorzystać pamięć masową.
Zaimplementowany w procesorze ARTPEC7 mechanizm detekcji obiektów w czasie rzeczywistym jest wspierany algorytmami uczenia maszynowego, które automatycznie wykrywają i rozpoznają ludzi, twarze i obiekty. Co ważne, układ został w całości opracowany przez firmę Axis. Producent zadbał przy tym o wysoki poziom kontroli mający kluczowe znaczenie w zapewnieniu cyberbezpieczeństwa. Wbudowane mechanizmy ochronne sprawiają, że można zainstalować tylko bezpieczne i autoryzowane oprogramowanie układowe oraz dostarczane przez zewnętrznych producentów aplikacji ACAP (Axis Camera Application Platform).

Z kolei chipset AI tworzony przez Hanwha Techwin – wg zapowiedzi producenta – ma się pojawić pod koniec tego roku. Tom Cook, wiceprezes ds. sprzedaży w Hanwha Techwin America, zdradził w Las Vegas kilka szczegółów na jego temat. Będzie się wyróżnić dokładnością detekcji i funkcjami cyberbezpieczeństwa. Rdzeń pamięci i rdzeń jego oprogramowania są odseparowane od funkcji analitycznych, w rezultacie otrzymujemy dwa układy scalone w jednym, z wbudowaną zaporą sieciową. Wszystkie układy scalone Hanwha Techwin tworzy sam – produkcja, projektowanie, kontrola jakości, a także testy cyberbezpieczeństwa oraz ocena jakości AI są wykonywane w ramach jednej firmy.

Odmienną drogę wybrała firma Arecont Vision Costar. Ten producent kamer obecnie współpracuje z firmą zewnętrzną nad rozwojem sztucznej inteligencji w swoich produktach. Zdaniem przedstawiciela producenta na wczesnym jeszcze etapie rozwoju rynku kamery z wbudowanymi układami sztucznej inteligencji będą się od siebie wyraźnie różnić pod względem działania. Będą albo niewiele warte z powodu kiepskiej jakości AI, albo – jeśli AI będzie dobra – odpowiednio droższe. Branża zabezpieczeń będzie musiała przejść proces uczenia się. Zarówno projektanci, jak i integratorzy systemów, a także użytkownicy będą musieli stopniowo opanowywać technologię AI. Przez kolejne 10 lat co roku na rynku zaczną się pojawiać nowe typy kamer wspomaganych przez AI. Już w tym albo przyszłym roku wejdzie na rynek dobrze zaprojektowana sztuczna inteligencja, ale o ograniczonym zastosowaniu.

Technologie wizyjne z AI wspierają rozwój analityki biznesowej

Coraz więcej firm z branży security oferuje kamery z wbudowaną sztuczną inteligencją. Dzięki implementacji AI analizę obrazu można przeprowadzać wprost w kamerze. Taka technologia jest wdrażana w wielu miejscach, m.in. na parkingach, w sklepach detalicznych czy na lotniskach. Wbudowane w kamerę sztuczne sieci neuronowe trenuje się metodą uczenia maszynowego. Do systemu wprowadza się mnóstwo przykładowych obrazów – danych. Na ich podstawie i korelacji łączących różne punkty danych sieć uczy się rozpoznawać w obrazie prawidłowości (wzorce), wykrywać kształty i obiekty. W efekcie urządzenie jest w stanie rozpoznać charakterystyczne cechy ludzi, a także przedmioty, np. samochody, łodzie, broń czy torby – zależnie od zdefiniowanego celu. Zazwyczaj kamera z zaimplementowanymi algorytmami głębokiego uczenia potrzebuje kilkunastu dni treningu, aby nauczyć się kształtu nowego obiektu. Pytani podczas targów ISC West przedstawiciele branży twierdzili, że jest obecnie w stanie dokonywać identyfikacji z 90-proc. dokładnością.
Tego typu kamery są coraz częściej wdrażane w sektorze związanym z transportem. Przykładowo wiele kamer montuje się na skrzyżowaniach ulic w celu kontroli ruchu drogowego. Urządzenia potrafią identyfikować rodzaj, prędkość i kierunek przejeżdżających pojazdów, a także określać godziny szczytowego natężenia ruchu. Firma Bosch demonstrowała m.in. sposób, w jaki można wykorzystać analizę obrazu na parkingach. Kamera tego producenta, monitorując pojazdy wjeżdżające na parking i opuszczające go, oblicza w czasie rzeczywistym całkowitą liczbę samochodów. Potrafi także identyfikować liczbę pojazdów parkujących w strefach dla niepełnosprawnych, zliczać samochody elektryczne lub luksusowe z segmentu F.

• Rozpoznawanie twarzy

Rozpoznawanie twarzy zyskuje popularność nie tylko w zastosowaniach związanych z bezpieczeństwem, ale także jako sposób na rozwijanie analityki biznesowej.
Powszechnie wprowadzaną przez wielu producentów funkcją jest anonimizacja twarzy – wynika to z przepisów UE dotyczących ogólnego rozporządzenia o ochronie danych osobowych (GDPR/RODO). Jednym z przykładów tej funkcjonalności jest rozwiązanie analityki wizji firmy Honeywell. Jej wewnętrzny al-

gorytm pozwala stwierdzić, czy osoba zidentyfikowana w kamerze jest systemowi znana, czy też nie. Jeśli jest nieznana, niebieskie pole zakrywa jej twarz na ekranie. W sytuacji, gdy została wcześniej zidentyfikowana i zarejestrowana w systemie, jej twarz zostanie pokazana.

Czy branży zabezpieczeń są potrzebne standardy dotyczące AI?

Nawet na obecnym, wczesnym etapie rozwoju technologii branża zabezpieczeń potrzebuje standardów w zakresie sztucznej inteligencji, by pojęcie AI dla wszystkich oznaczało to samo

Rośnie wykorzystanie sztucznej inteligencji w obszarze security. Coraz więcej producentów kamer uczy się, jak wbudowywać nową technologię w swoje produkty, i zgłasza pilną potrzebę standaryzacji. Przy braku standardów niektóre terminy mogą dla poszczególnych firm oznaczać co innego. Jako przykład weźmy funkcję szerokiego zakresu dynamiki WDR w kamerach dozorowych. Chociaż wielu producentów twierdzi, że oferuje taką funkcję, to ich definicje WDR się różnią. Nie ma też standardowych definicji dotyczących analityki wizyjnej.
O standardach w dziedzinie sztucznej inteligencji zapewne będzie decydowało kilku największych graczy w branży – 6 czy 7 dużych producentów, którzy udowodnią klientom, że mają najlepsze rozwiązania AI. Ścieżka rozwoju standardów sztucznej inteligencji może przypominać standaryzację interfejsu ONVIF dla kamer IP, który jest obecnie powszechnie stosowany. Powinna powstać grupa branżowa, która ustali zasady dotyczące standardów AI. Trudno jednak spodziewać się, że to branży zabezpieczeń przypadnie główna rola w ich opracowywaniu. Ten sektor to tylko niewielka część rynku sztucznej inteligencji, na którym dominują: przemysł motoryzacyjny, wojsko, producenci smartfonów i innych towarów konsumenckich.

Jak OSSA chce wspierać współpracę w branży?

Stowarzyszenie Open Security & Safety Alliance (OSSA) przygotowało platformę, która umożliwia współpracę producentów urządzeń, twórców oprogramowania, integratorów, specjalistów, konsultantów i innych podmiotów wnoszących ze sobą doświadczenie z sąsiednich rynków w tworzeniu innowacji dla branży elektronicznych systemów zabezpieczeń

W erze Internetu Rzeczy (IoT) powstają ogromne zbiory danych. Branża zabezpieczeń musi wykorzystać możliwości, jakie dają te wielkie zasoby informacji. Jednym ze sposobów jest stworzenie spójnego środowiska opartego na standardach, w którym firmy będą mogły ze sobą bez problemów współpracować. Celem powołanego stowarzyszenia OSSA jest m.in. opracowanie wspólnego systemu operacyjnego (OS). Oparcie wszystkich kamer dozoru wizyjnego na tej samej platformie pozwoli użytkownikom końcowym uruchamiać te same aplikacje na różnych urządzeniach (tak jak działa to od lat na smartfonach dostosowanych do systemu operacyjnego Android).

• Potencjał wykorzystania danych

Standaryzacja od dawna jest przedmiotem zainteresowania rynku zabezpieczeń. Zapytany, dlaczego OSSA teraz zajęła się tym tematem, Johan Jubbega, prezes Stowarzyszenia, twierdzi, że katalizatorem było pojawienie się Internetu Rzeczy (IoT).
IoT zmienił rolę urządzeń zabezpieczeń elektronicznych, które pracując w sieci, pełnią jednocześnie funkcję czujników. Rosnąca wszechobecność różnego typu czujników wymieniających między sobą informacje tworzy środowiska bogate w dane, ale pozyskiwane informacje nie są jeszcze wykorzystywane w sposób wystarczający. Ogromne zbiory danych oferują wiele możliwości analitycznych i budzą nadzieję związaną ze sztuczną inteligencją, wciąż jednak nie użytkujemy w pełni tego potencjału.
Dzięki różnym aplikacjom kamery stają się obecnie coraz bardziej smart. Sklepy detaliczne stosują kamery dozorowe nie tylko do ochrony ludzi i mienia, ale także w celu pozyskania informacji biznesowych (analityka biznesowa – *Business Intelligence*). Dostępne są aplikacje mierzące przepływ i liczbę odwiedzających sklep, a także wykrywające określone zachowania klientów.
Wspólna platforma zachęci większe grono programistów aplikacji do zainteresowania się rynkiem security, co będzie stymulowało kolejne innowacje.

• Współpraca w branży

Wspólna platforma będzie również sprzyjać współpracy. Obecnie większość firm funkcjonuje w osobnych silosach, a potencjał innowacji zależy od możliwości pojedynczych firm.
Bliższe relacje między firmami mogą również wpłynąć na poprawę cyberbezpieczeństwa. Mając to na względzie, OSSA powołała specjalną grupę roboczą zajmującą się tym właśnie obszarem.

• Cyfrowy sklep dla integratorów systemów

Kolejnym celem Stowarzyszenia OSSA jest promocja działań zmierzających do stworzenia sklepu z aplikacjami, w tym mechanizmu umożliwiającego integratorom systemów dzielenie się doświadczeniami związanymi z aplikacjami. Członkami Stowarzyszenia są producenci urządzeń, integratorzy systemów, twórcy aplikacji (programiści) i dystrybutorzy. Obecnie, na wczesnym etapie działania organizacji, większość stanowią producenci, ale OSSA chciałoby w swoim gronie mieć więcej integratorów systemów, ponieważ to oni są użytkownikami końcowymi oferty rynkowej i to integrator systemów tworzy rozwiązanie dostosowane do potrzeb klienta.

SAST tworzy otwartą platformę programistyczną wspierającą AI

Uruchomiony przez firmę Bosch start-up SAST pracuje nad opartym na Androidzie systemem operacyjnym dla kamer, który pozwoli wdrażać różne aplikacje sztucznej inteligencji

Podczas targów w Las Vegas start-up *Security and Safety Things* (SAST), będący partnerem Stowarzyszenia OSSA, przedstawił swoją wizję opartego na Androidzie systemu operacyjnego dla kamer dozorowych. Chodzi o platformę, która kamerom różnych marek pozwoli działać z tym samym systemem operacyjnym. Jej rozwój ma się opierać na otwartych standardach, ma ona przypominać znany ze środowiska smartfonów model sklepu z aplikacjami. Ujednolicona platforma ułatwi pracę twórcom aplikacji. Bez wspólnego systemu operacyjnego muszą oni projektować oddzielne aplikacje dla poszczególnych producentów kamer. W rezultacie samo ich testowanie może zajmować więcej czasu niż opracowywanie. Innymi słowy, ponieważ dziś każda firma tworzy coś innego, OSSA chce doprowadzić do porozumienia dostawców w kwestiach standaryzacji.
Podczas targów ISC West aplikacje, takie jak „Liczenie osób", „Analiza przechodzących ludzi" i „Ochrona obszaru" zostały wdrożone na wybranych kamerach. Stworzony system operacyjny działa już na pierwszych prototypowych urządzeniach firm należących do OSSA.
W sklepie z aplikacjami jest dostępnych blisko 25 aplikacji. Obliczenia przez nie wykonywane są w większości prowadzone bezpośrednio w kamerze. Dzisiejsza oferta aplikacji jest nastawione na analizy, takie jak pomiar przepływu ludzi, ale w przyszłości mogą dotyczyć nawet bardziej zaawansowanych zastosowań, np. wykrywania trzęsień ziemi.
SAST ma nadzieję, że do końca roku powstanie ponad 100 aplikacji. Jak informuje start-up, planowane zastosowania, poza obszarem bezpieczeństwa, dotyczą przede wszystkim analityki biznesowej.

• Większy udział innych branż

Platforma przyciągnie nowe rozwiązania różnych producentów nie tylko z obszaru security. Będą mogły do niej dołączyć firmy technologiczne z wielu branż. Do tej pory twórcami aplikacji były przeważnie zajmujące się analityką wizyjną małe firmy, zatrudniające nie więcej niż 20 pracowników. SAST umożliwia wszystkim podmiotom rozwój sztucznej inteligencji stosowanej w kamerach.

• Masowe wdrażanie aplikacji

Oprócz sklepu z gotowymi aplikacjami SAST oferuje programistom również portal z narzędziami do testowania oraz udostępnia przestrzeń do tworzenia społeczności mającej służyć wzajemną pomocą i inspiracjami. Integratorzy systemów mogą przy użyciu komputerów PC uzyskiwać dostęp do sklepu z aplikacjami i kupować programy, a następnie wdrażać je w kamerach. Dzięki portalowi mogą uruchamiać te aplikacje na wielu urządzeniach jednocześnie. To bardzo pomocna funkcja, szczególnie w przypadku dużych obiektów, np. lotnisk, gdzie liczba kamer może sięgać nawet 20 tysięcy.
Kamery z systemem Android powinny zostać wprowadzone na rynek do końca tego roku lub na początku 2020.

ONVIF

Open / Closed Network Video Interface Forum

TEKST
Jan T. Grusznic

ONVIF to organizacja od 10 lat działająca na rzecz ustandaryzowania komunikacji pomiędzy produktami elektronicznych systemów zabezpieczeń opartych na protokole IP, u której podstaw powstania leżą interoperacyjność bez względu na markę i otwartość na wszystkie firmy i organizacje. Ostatnio zdecydowała się zawiesić członkostwo sześciu firmom, w tym aż trzem z najwyższym statusem...

Założona w 2008 r. przez Axis Communications, Bosch Security Systems i Sony Corporation organizacja ONVIF doczekała się solidnej bazy członków na sześciu kontynentach. W założeniach członkostwo w ONVIF jest otwarte dla producentów, programistów, konsultantów, integratorów systemów, użytkowników końcowych i innych grup interesu, które chcą uczestniczyć w działaniach forum. Praktyka okazuje się inna.

W wyniku aktualizacji w dniu 9 października 2019 r. amerykańskiego wykazu podmiotów zarządzających eksportem (*Export Administration Regulations Entity List*) ONVIF zawiesił dostęp do informacji zarezerwowanych dla członków organizacji firmom: Dahua Technology, Hikvision Digital Technology, Huawei Technologies, Shanghai Yitu Technology, Pixel Design Sdn. Bhd – związanej z Hikvision i Lorex – związanej z Dahua. Jak wynika z noty prasowej, *ONVIF podjęło te działania w celu zapewnienia zgodności z amerykańskim prawem eksportowym, a zawieszenie pozostanie w mocy do czasu usunięcia przedsiębiorstw z listy EAR przez rząd USA*[1].

[1] https://www.onvif.org/pressrelease/media-statement-membership-suspension/

Ta decyzja komitetu sterującego ONVIF została podjęta wkrótce po tym, jak prezydent Donald Trump podpisał dekret wykonawczy zakazujący firmom amerykańskim kupowania lub sprzedawania sprzętu telekomunikacyjnego takich firm, jak Huawei, które są uważane za stwarzające zagrożenie bezpieczeństwa narodowego Stanów Zjednoczonych. Departament Handlu USA umieścił członków ONVIF wraz z 22 innymi organizacjami rządowymi i komercyjnymi na swoim „wykazie podmiotów"[2] za domniemane naruszenia praw człowieka.

Wykaz podmiotów jest zasadniczo rządową czarną listą, która zakazuje przedsiębiorstwom amerykańskim eksportowania swoich produktów do wymienionych organizacji. Chociaż umieszczenie podmiotu w wykazie nie jest całkowitym embargiem, wymaga zgody rządu, zanim jakakolwiek firma z siedzibą w Stanach Zjednoczonych będzie mogła sprzedawać im towary w przyszłości. Do nich zalicza się również organizacja ONVIF, która rozwija specyfikacje na sesjach zamkniętych przed publikacją, a rząd USA dostęp do nich przez firmy zewnętrzne traktuje jako eksport technologii.

Jak działa ONVIF?

Praca w ONVIF jest prowadzona i wykonywana przez jej członków w różnych komitetach i grupach roboczych. Struktura organizacyjna składa się z Komitetów: Sterującego, Technicznego, Usług Technicznych i Komunikacji.

Komitet Sterujący jest odpowiedzialny za strategię i budżetowanie ONVIF. Obecnie członkami tego komitetu są Axis, Bosch, Honeywell, Pelco i Sony.

Komitet Techniczny jest motorem rozwoju podstawowych specyfikacji ONVIF, jak również kierunku technicznego i mapy drogowej. Obecnie członkami są Axis, Bosch, Hanwha Techwin, Hikvision (zawieszony), Pelco, Sony i Tyco Security. Grupy robocze w ramach Komitetu Technicznego opracowują podstawową specyfikację ONVIF, kwestie bezpieczeństwa, fizycznego dostępu i poprawy jakości obrazu.

Komitet Usług Technicznych jest odpowiedzialny za opracowanie profili, specyfikację metodologii testów, narzędzia testowego i procesu zgodności. Obecnie jego członkami są Anixter, Axis, Bosch, Honeywell, Pelco i Sony. Grupy robocze w ramach Komitetu Usług Technicznych pracują nad sposobem testowania urządzeń, aplikacji klienckich, Profilem D i Profilem M.

Komitet ds. Komunikacji jest odpowiedzialny za komunikację zewnętrzną i wewnętrzną organizacji. Członkami tego komitetu są obecnie Axis, Bosch, Dahua Technology (zawieszony), Hikvision (zawieszony), Honeywell, Huawei (zawieszony) i Sony. Grupy robocze w ramach tego komitetu opracowują scenariusze zastosowania dla opracowywanych rozwiązań.

ONVIF oferuje cztery klasy członkostwa rocznego w celu dostosowania się do różnych poziomów uczestnictwa: pełne, wspierające, użytkownik i obserwator. Członkowie pełnoprawni i członkowie wspierający mogą aktywnie wpływać na rozwój standardu poprzez udział w pracach organizacji. Poziom członkowski jest otwarty dla organizacji, które chcą korzystać ze specyfikacji interfejsu i mają dostęp do propozycji specyfikacji, ale nie chcą uczestniczyć w żadnej pracy organizacji.

2) Po raz pierwszy wykaz podmiotów opublikowało Biuro Przemysłu i Bezpieczeństwa Stanów Zjednoczonych w lutym 1997 r. jako część swoich wysiłków na rzecz informowania opinii publicznej o podmiotach, które zaangażowały się w działalność mogącą spowodować zwiększone ryzyko przekierowania eksportowanych, reeksportowanych i przekazywanych (w kraju) produktów do programów dotyczących broni masowego rażenia. Od czasu pierwszej publikacji podstawy do wpisania na listę podmiotów zostały rozszerzone na działania usankcjonowane przez Departament Stanu, a także działania sprzeczne z interesami bezpieczeństwa narodowego i/lub polityką zagraniczną Stanów Zjednoczonych.

Poziom obserwatora jest otwarty dla organizacji, które nie chcą uczestniczyć w żadnej pracy w ONVIF, ale którym przyznano pewne ograniczone korzyści, np. prawo dostępu do narzędzi testowych. Jednak członkowie obserwatorzy nie mogą prezentować, domagać się, wprowadzać na rynek lub promować jakiegokolwiek produktu sprzętowego, oprogramowania lub innego urządzenia, które ma być zakwalifikowane jako produkt zgodny z ONVIF. Zatem producenci urządzeń lub dostawcy oprogramowania klienckiego nie mogą być obserwatorami.

Co decyzja ONVIF oznacza dla branży?

Obecnie nie ma powodu do niepokoju. Jak potwierdzają to same władze ONVIF, zawieszenie obejmuje możliwość dostarczenia przez członka nowych produktów w celu uzyskania zgodności opartej na przyszłych wersjach narzędzi testowych oraz uniemożliwienie jego przedstawicielom udziału w komitetach i grupach roboczych ONVIF. W wyniku sankcji status istniejących produktów zgodnych z przepisami członków nie zmienia się. W tym duchu wypowiadają się również zawieszeni członkowie, twierdząc, że obecny stan nie wpływa negatywnie na dostępne produkty zgodne z ONVIF (lista dostępna na stronie internetowej organizacji). Co więcej – nowo wytworzone urządzenia również mogą być zgodne ze standardem w zakresie tych profili, do których dokumentację oraz narzędzia potwierdzania zgodności posiadali producenci przed dniem ich zawieszenia w członkostwie.

Jednak kontynuacja zakazu będzie miała wpływ na zgodność produktów z przyszłymi profilami w dłuższej perspektywie. Co prawda w 2019 r. nie pojawiły się nowe wersje, ale wiadomo że ONVIF pracuje nad nowymi rozwiązaniami dla rynku, jednak dostęp do nich został odcięty dla wymienionych firm. □

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.

Rola projektanta w procesie tworzenia stanowiska operatora systemów dozoru wizyjnego

KAŻDY, KTO MA WIELOLETNIE DOŚWIADCZENIE PRACY W BRANŻY ZABEZPIECZEŃ ELEKTRONICZNYCH, ZAUWAŻYŁ NIEJEDNOKROTNIE, JAK MAŁO UWAGI PROJEKTANCI POŚWIĘCAJĄ STANOWISKOM OPERATORA SYSTEMU DOZORU WIZYJNEGO (VSS – *VIDEO SURVEILLANCE SYSTEM*)[1].

TEKST
Cezary Mecwaldowski

W projektach systemów zabezpieczeń elektronicznych najczęściej można odnaleźć nie więcej niż pół strony opisu stanowiska oraz wykaz urządzeń w zestawieniu materiałów. W nielicznych projektach pojawia się rysunek, jakaś aranżacja pomieszczenia i stanowiska operatora. Niezbędny, precyzyjnie określony cel systemu zostaje spłycony do określenia obszarów poddanych dozorowi za pomocą kamer i czasu archiwizacji zapisu sygnału wizyjnego.

Współczesne systemy można łatwo rozbudowywać, z kilkudziesięciu kamer robią się setki i tysiące. Ściana monitorów rozrasta się, dopóki znajduje się miejsce na kolejny monitor. W konsekwencji pojawia się rozczarowanie użytkownika lub inwestora, gdy taki system nie spełnia założonych oczekiwań. Dochodzi do zdarzeń: wandalizmu, rozboju, kradzieży, a operator nie tylko nie dostrzega początku zagrożenia, ale także dowiaduje się o nim po czasie, z innych źródeł, a nie własnej obserwacji. W skrajnych przypadkach dochodzi do tragedii w „oku kamery", np. stale monitorowani osadzeni w więzieniach dokonują samobójstw lub duża dynamika pożaru w markecie po kilkunastu sekundach pozbawia operatora wglądu w sytuacje i praktycznie uniemożliwia prowadzenie ewakuacji osób[2].

To projektant, jako doradca inwestora, projektując system dozoru wizyjnego na podstawie analizy zagrożeń i ryzyka ich wystąpienia, powinien oprócz parametrów technicznych systemu, określić liczbę operatorów wymaganych do jego obsługi, w zależności od:

- celu stosowania systemu dozoru wizyjnego lub zintegrowanych systemów zabezpieczeń,
- ograniczeń psychofizycznych operatora i ergonomii stanowiska,
- obciążenia zadaniami, procedurami.

Skąd inwestor miałby posiadać wiedzę, ilu operatorów jest niezbędnych do efektywnej obsługi systemu i realizacji zadań, jeśli nie od projektanta. Należy przy tym rozróżnić możliwość wykonywania założonych zadań przez operatora, od jego kompetencji i szkoleń.

Podstawą projektu zabezpieczeń elektronicznych jest precyzyjne określenie celu stosowania, który zostanie zapisany w dokumentacji „Wymagania użytkowe" systemu. Cel ten powinien wynikać z rzetelnej analizy zagrożeń uwzględniającej np. ryzyko występowania zdarzeń, ich liczbę oraz ocenę ważności. Wskazany cel to jednocześnie określona rola, jaką będzie spełniał system VSS w systemie bezpieczeństwa obiektu lub obszaru i stanowi podstawę do jego prawidłowego zaprojektowania, w tym stanowiska operatora. System dozoru wizyjnego może spełniać następujące podstawowe role:

- prewencyjną – zapobieganie zdarzeniom,
- zdarzeniową – działanie w trakcie zdarzeń,
- postzdarzeniową – działanie po zdarzeniu, dowodowe.

Powyższy podział ról wpisuje się także w typy operatorów wymieniane w literaturze[3]:

- **Typ 1** – typowy operator systemu dozoru wizyjnego, który reaguje na dostrzeżone zagrożenie w obserwowanych obrazach, steruje kamerami i systemem, korzysta ze środków łączności do powiadamiania.
- **Typ 2** – operator zintegrowanych systemów zabezpieczeń (a także SCADA), który reaguje na różne sygnały alarmowe i dopiero do ich weryfikacji korzysta z dozoru wizyjnego, z obrazu z kamer lub jego zapisu – to także ta sytuacja, gdy do wspomagania operatora zastosowano analizę obrazu VCA *(video content analysis)* lub/i sztuczną inteligencję AI.

W skrajnym przypadku system dozoru wizyjnego może być bez operatora (pełni jedynie funkcję dowodową), w pośrednim operator będzie pracował tylko w określonych godzinach funkcjonowania obiektu lub reagował na alarmy i korzystał z dozoru wizyjnego do ich weryfikacji, po rolę prewencyjną w obiektach infrastruktury krytycznej i innych. Pomieszczenie, w którym znajduje się stanowisko operatora, musi spełniać co najmniej wymagania przepisów BHP i ergonomii stanowiska. W obiektach wymagających zdalnego monitorowania i odbioru alarmów parametry pomieszczeń centrum monitoringu i odbioru alarmu podaje norma PN-EN 50518:2019 – Centrum monitoringu i odbioru alarmu. Wprowadza ona podział centrów monitorowania alarmów na dwie kategorie: pierwszą, gdy monitoruje się sygnały z zastosowań dotyczących ochrony obiektów, oraz drugą, gdy występuje monitorowanie sygnałów z zastosowań pozaochronnych. Zgodnie z założeniami w przypadku monitorowania alarmów należy brać pod uwagę 2. typ operatora.

Niestety często próbuje się połączyć zadaniowo wspomniane typy operatorów na jednym stanowisku. Dochodzi wtedy do rozczarowania, gdyż operator nie spełnia oczekiwań efektywnej obsługi zdarzeń. Tylko precyzyjne założenia na etapie uzgodnień, gwarantują podjęcie właściwych kroków w projektowaniu stanowiska operatora, przy uwzględnieniu zasad wiedzy technicznej i ergonomii. Projektant znajdzie niezbędne informacje w kilku normach[4]. Mogą być różne konfiguracje samego stanowiska i urządzeń, przy czym należy brać pod uwagę dwa główne rodzaje monitorów:

- monitory stanowiskowe, szczegółowe, incydentalne – służą do szczegółowej, stałej lub doraźnej obserwacji. Są z nimi związane parametry określające wymaganą wielkość obiektu na obrazie, np. zawarte w normie PN-EN 62676 – Systemy dozorowe CCTV stosowane w zabezpieczeniach (niezbędna wielkość bodźca wzrokowego zależna od rozdzielczości obrazu);
- ściana monitorów, tzw. *Video Wall* - służy do ogólnej, doraźnej obserwacji oraz współpracy i wymiany informacji pomiędzy operatorami.

[1] Artykuł powstał na podstawie wniosków z wystąpienia eksperckiego „Rola projektanta w tworzeniu stanowiska operatora systemu dozoru wizyjnego" podczas konferencji SPIN 17 w dniu 26 września 2019 r. oraz dyskusji, która wywiązała się w jego trakcie jak i po zakończeniu.
[2] Pożar marketu w miejscowości Kemerovo w Rosji, https://www.youtube.com/watch?v=d8m14KWrx_I dostęp dnia 24.11.2019 r.
[3] R. Pikaar, D. Lenior, K. Schreibers, D. Bruijn, "Human Factors Guidelines for CCTV system design" Melbourne 2015
[4] PN-EN 62676; PN-EN 1104; PN-EN 50518; PN-EN 50398; PN-EN 50131; PKN-CLC/TS 50131-7

Najważniejsze zasady dotyczące monitorów na stanowisku operatora:

- Wielkość piksela obrazu niezbędna do obliczenia odległości obserwacji (z uwzględnieniem parametrów optycznych oka). Odległość obserwacji monitora lub ekranu można wyliczyć ze wzoru prezentowanego w normach: odległość [mm] = wielkość piksela ekranu [mm] x 3,4.
- Przy zastosowanej rozdzielczości obrazu wielkości piksela zgodnie z normą należy uwzględnić wielkość obiektu w obrazie, który spełnia warunki odpowiedniego bodźca wzrokowego pozwalającego operatorowi na wymaganą reakcję: monitorowanie – detekcja – obserwacja – rozpoznanie – identyfikacja – inspekcja.
- System musi być łatwy w obsłudze i umożliwiać szybkie przełączanie obrazów pomiędzy monitorami zgodnie z PN-EN 62676-4 (Wytyczne stosowania). Ta zasada umożliwienia szybkiej reakcji operatora dotyczy całego systemu zgodnie z normą PN-EN 62676-1 (Wymagania systemowe – Postanowienia ogólne).
- Rozmieszczenie monitorów z zachowaniem zasad ergonomii pozycji operatora, z uwzględnieniem wysokości montażu, kąta prostego pomiędzy płaszczyzną ekranu a linią wzroku, zakresu widzenia ostrego – centralnego – peryferyjnego oraz czasu niezbędnego do świadomego rozpoznania na obrazie czy zagrożenie występuje, czy nie (2-3 sekundy na jeden obraz lub scenę o niewielkim stopniu złożoności).

Powyższe zasady odnoszą się również do nowych technologii wyświetlania obrazów, które pojawiają się obecnie:

- ekrany bezramkowe, wielkoformatowe,
- ekrany wielkoformatowe, modułowe LED full HD *(fot. 1)*,
- projektory laserowe,
- monitory Ultra Wide 32:9 5k *(fot. 2)*.

Zapewniają nową jakość wyświetlania, pozwalającą uzyskać niespotykany dotychczas kontrast i odwzorowanie czerni, w niewielkim stopniu zależną od poziomu oświetlenia w pomieszczeniu – przy pełnym wsparciu procesorów obrazu, realizujących dowolne układy wyświetlania, podziału ekranów i skalowania. Trwają także próby zastosowania okularów HoloLens i VR (uwaga! technologia VR może wywoływać efekt choroby lokomocyjnej, zaburzenia równowagi, lęk wysokości itp.).
Z powyższych zasad wynika, jak wiele jest czynników mogących wpłynąć negatywnie na efektywność pracy operatora:

- odległość obserwacji sięga poza parametry optyczne jego wzroku,
- umiejscowienie monitorów w sposób nieergonomiczny, poza obszarem widzenia centralnego,
- efektywność obserwacji maleje ze wzrostem liczby obserwowanych obrazów, scen i monitorów: mniej rozpoznanych zdarzeń i dłuższy czas reakcji na zdarzenie,
- nie każda osoba nadaje się na operatora ze względu na brak predyspozycji psychofizycznych.

Systemy dozoru wizyjnego stały się w wyniku agresywnego marketingu producentów i dostawców, przede wszystkim w miastach, synonimem bezpieczeństwa. Tylko czy słusznie? Ostatnie statystyki[5] plasują Warszawę na 23. miejscu pod względem miast o największej liczbą kamer (ok. 14 tys.). Od razu pojawia się pytanie o liczbę operatorów. Z raportu pokontrolnego NIK[6] z 2013 r. wynika, że w Warszawie były 323 kamery, które obsługiwało 188 operatorów w 17 Centrach Oglądowych. Jak jest obecnie? Kolejne pytane – czy to za dużo, za mało, a może w sam raz, by efektywnie realizować zadania? Wg badań BBC, mieszkaniec Londynu znajduje się w oku kamery średnio 12 razy w ciągu dnia[7]. To znaczące ograniczenie prawa do prywatności, a okazuje się, że wraz ze wzrostem liczby kamer poziom bezpieczeństwa nie rośnie, wręcz odwrotnie – obniża się.

Podam kilka przykładów cech psychofizycznych, które powinien uwzględnić projektant stanowiska operatora na etapie analizy ryzyka, określania parametrów technicznych, przygotowania procedur oraz doboru niezbędnej liczby operatorów systemu:

Fot. 1. Ekran wielkoformatowy w technologii modułowej mini LED (piksel LED 1,5 mm) full HD. Źródło: materiały autora

Fot. 2. Przykład monitora Ultra Wide 5K 32:9. Źródło: https://www.technologydeskingtradingdesks.com/news/lg dostęp 24.11.2019 r.

- Czy operator może wykonywać równocześnie wiele zadań? Nie powinien. Mózg przełącza uwagę pomiędzy zadania. W tym samym czasie można realizować tylko jedno świadome zadanie (różne zadania można wykonywać równocześnie tylko wtedy, gdy są one automatyczne, wyuczone, bez udziału świadomości). Wykonywanie wielu zadań jednocześnie fragmentuje uwagę i zwiększa ryzyko błędu.
- Czynność obserwacji stanowi znaczny wysiłek dla mózgu – pochłania około 30% energii.
- Ile monitorów i obrazów może obserwować operator? Odpowiedź zależy od trzech wspomnianych już zależności:
  1. ile zadań jednocześnie on może wykonywać,
  2. jaki ma wyznaczony zakres widzenia centralnego i peryferyjnego *(fot. 3)*,
  3. jaką wyznaczono odległość obserwacji zależną od ergonomii obserwacji, typu monitora i wielkości piksela obrazu (wg podanego wyżej wzoru).
- Zjawisko „torowania uwagi" (perswazja) może spowodować, że operator nie zauważy zdarzeń poza tymi, na które wybiórczo skierowano jego uwagę – wskazanie wybranych celów obserwacji.
- Zjawisko widzenia tunelowego – w sytuacji silnego stresu, widzenie ostre i centralne dodatkowo zawęża się.
- Zjawisko A. L. Yarbusa to przykład kierowania uwagi i wybiórczego dostrzegania szczegółów, gdy obserwator ma za zadanie przyjrzeć się obrazowi; kiedy później odpowiada na pytania dotyczące szczegółów obrazu, z reguły nie potrafi ich szczegółów podać, choć wydają się oczywiste (fot. 4).
- Zjawisko ślepoty z powodu braku podzielnej uwagi, tzw. efekt goryla - w nieco odmiennej formie doświadcza tego zjawiska osoba oglądająca film na ekranie telewizor, tak pochłonięta akcją, że nie zauważa pojawiającej się informacji o zbliżającym się automatycznym wyłączeniu odbiornika. Nie zauważa tej informacji, mimo iż zajmuje ona prawie 1/3 ekranu (fot. 5).

Nasza psychika ma zbyt dużo wad, aby zapobiec kryzysowi, dlatego systemy muszą być konstruowane tak, aby maksymalnie wspierać operatora, a nie pogłębiać ryzyka popełnienia błędów. Obecnie projektant może zastosować dedykowane wyposażenie i umeblowanie dla stanowisk operatorów. Mając gwarancję producentów tegoż wyposażenia, iż uwzględnia ono aktualne zasady wiedzy technicznej oraz obligatoryjne wymagania ergonomii.
Co ważne, projektant powinien zadbać w projekcie o zapisy dotyczące testów systemu dozoru wizyjnego, zarówno w zakresie sprawdzenia parametrów jakościowych systemu po jego wykonaniu, jak i testów realizacji założonych zadań oraz procedur przez operatorów. Wykonanie tych testów, będzie niezbędne do rozliczania pracy operatorów i ich ewentualnej odpowiedzialności. □

Fot. 3. Zjawisko widzenia centralnego do 30° i peryferyjnego od 30° do 120° (bez uwzględnienia ruchu gałek ocznych i głowy). Źródło: materiały autora

Fot. 4. Zjawisko z obserwacji obrazu na przykładzie A.L. Yarbusa. Źródło: http://www.datadeluge.com/2012/10/the-unexpected-visitor.html dostęp z 22.11.2019 r.

Fot. 5. Zjawisko „ślepoty z braku podzielności uwagi" na przykładzie komunikatu „Telewizor zostanie wkrótce wyłączony". Źródło: materiały autora

BIO

Cezary Mecwaldowski

Wykładowca zajmujący się szkoleniami zawodowymi i specjalistycznymi z zakresu zabezpieczeń elektronicznych, stosowania urządzeń do kontroli, nowych rozwiązań w dziedzinie systemów alarmowych. Projektant z praktyką zagraniczną. Absolwent Politechniki Łódzkiej o specjalizacjach: energetyka przemysłowa i informatyka stosowana.

[5] P. Bischoff: „The world's most – surveilled cities", www.comparitech.com dostęp 15.11.2019 r.
[6] Raport NIK „Funkcjonowanie miejskiego monitoringu wizyjnego" LLU - 4101-01-00/2013, 2013
[7] Kanał BBC HD „Ziemia 2050", dostęp 18.09.2017

SLIM LINE – nowe oblicze detekcji ruchu

W listopadzie br. SATEL wprowadził do swojej oferty nowe czujki ruchu – serię SLIM LINE.
Nowe urządzenia, oprócz niezwykłej skuteczności w wykrywaniu ruchu, oferują wiele dodatkowych ciekawych rozwiązań.

Rodzinę SLIM LINE tworzą:

- SLIM-PIR
- SLIM-DUAL
- SLIM-PIR-PET
- SLIM-DUAL-PET
- SLIM-PIR-LUNA
- SLIM-DUAL-LUNA
- SLIM-PIR-LUNA-PET
- SLIM-DUAL-LUNA-PET
- SLIM-PIR-PRO
- SLIM-DUAL-PRO

Za co odpowiadają poszczególne części nazw tych urządzeń? Modele z oznaczeniem PIR są wyposażone w pasywny czujnik podczerwieni, natomiast czujki DUAL zawierają dodatkowo czujnik mikrofalowy. PRO to urządzenia spełniające wymagania dla systemów Grade 3. Wyjątkową cechą czujek LUNA jest funkcja oświetlenia. Z kolei urządzenia z PET w nazwie ignorują niewielkie zwierzęta domowe.Co wyróżnia SLIM LINE na tle innych czujek dostępnych na rynku?

Wygląd, obudowa i wskaźnik LED

Każdy egzemplarz jest zamknięty w smukłej, charakteryzującej się lekkim designem obudowie – wszystkie czujki ruchu pracujące w obiekcie mogą wyglądać tak samo. Utrudnia to intruzowi rozpoznanie modelu nadzorującego dane pomieszczenie i wpływa na estetykę instalacji alarmowej. Innym rozwiązaniem, podnoszącym atrakcyjność wizualną nowych urządzeń, jest możliwość wyboru koloru świecenia wskaźnika LED (nawet spośród 7 barw).

Skuteczna detekcja ruchu

Doświadczenie zebrane przez lata produkcji czujek ruchu, w połączeniu z zastosowaniem najnowszych technologii, zaowocowało opracowaniem zaawansowanego algorytmu detekcji. Jest on dynamicznie dopasowywany do temperatury otoczenia, więc jej zmiany nie mają wpływu na stabilność pracy czujek – efektem jest niezawodne wykrywanie intruzów i brak niepożądanych alarmów.
Użyta w SLIM LINE soczewka to zupełnie nowa konstrukcja optyczna, zapewniająca niezwykle skuteczną detekcję ruchu w obrębie całego nadzorowanego obszaru (nawet 20 m x 24 m, 90°). Dostępność wymiennych frontów z soczewkami kurtynowymi lub dalekiego zasięgu umożliwia szybkie przystosowanie czujki np. do nietypowego kształtu pomieszczenia.

LUNA i PRO – więcej niż „zwykłe" czujki

Tym, co wyróżnia modele LUNA i PRO, jest zintegrowane uchylne zwierciadło umożliwiające ochronę obszaru bezpośrednio pod czujką – czyli tzw. strefy podejścia.
Modele LUNA posiadają zestaw białych diod LED załączanych zdalnie lub w reakcji na ruch. Znajdą zastosowanie np. w korytarzach czy innych miejscach niewymagających do przemieszczania się głównego oświetlenia. Oferują także możliwość zaprogramowania i zdalnego przełączania między dwoma zestawami parametrów pracy (m.in. progami czułości). W jakim celu? Np. gdy strefa, do której przypisana jest czujka, czuwa – wykorzystywane są ustawienia eliminujące niepożądane alarmy. Natomiast gdy czuwanie jest wyłączone, urządzenie może załączać światło w odpowiedzi na najdrobniejszy ruch.
Czujki PRO mają aktywny antymasking IR zgodny z wymogami EN 50131 dla Grade 3. Pozostałe przedstawicielki rodziny SLIM LINE spełniają wymagania dla Grade 2.

Szybki montaż i wygodna konfiguracja

Rozwiązania, takie jak wygodny mechanizm otwierająco-zamykający, zintegrowane rezystory 2EOL czy dostępna w modelach LUNA i PRO rozłączalna listwa zaciskowa (demontaż elektroniki bez odkręcania przewodów) oraz możliwość zmiany ustawień czujki za pomocą pilota to udogodnienia wprowadzone z myślą o ułatwieniu i przyspieszeniu pracy instalatorskiej.

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

Centrale alarmowe NeoGSM-IP – ochrona i automatyka domowa

NeoGSM-IP, NeoGSM-IP-64 to nowoczesne centrale alarmowe z wbudowanymi funkcjami automatyki domowej, przeznaczone do domów jednorodzinnych, mieszkań oraz małych obiektów komercyjnych.

Produkty te są dedykowane dla użytkowników, którzy cenią sobie prostą i intuicyjną obsługę oraz pełną kontrolę nad systemem zarówno w domu, jak i poza nim. Sterowanie dostępne jest na wiele sposobów: lokalnie za pomocą paneli dotykowych, smartfonu, tabletu lub pilotów radiowych. Poza domem system skomunikuje się z użytkownikiem za pomocą sieci GSM lub Internetu, a smartfon i tablet będzie centrum kontroli w dowolnym miejscu na świecie. Aplikacja mobilna RopamNeo jest dostępna na systemy Android i iOS oraz obsługuje zarówno smartfony, jak i tablety powyżej 10".

Podstawową funkcjonalnością centrali jest system sygnalizacji włamania umożliwiający profesjonalną ochronę domu. Dzięki modułowej konstrukcji, możliwości rozbudowy i uniwersalnym funkcjom pozwala na dostosowanie do większości typowych instalacji alarmowych oraz umożliwia podłączenie praktycznie dowolnych czujek i sygnalizatorów oferowanych na rynku. Dzięki temu można dobrać je do wymagań użytkownika i wykończenia wnętrza.
Szybkość powiadomienia i obsługi jest kluczowa, dlatego weryfikacja zdarzeń i dostęp do sterowania jest w czasie rzeczywistym. W momencie alarmu lub innego ważnego zdarzenia centrala powiadomi użytkownika lub firmę ochrony o źródle zdarzenia, wraz z dodatkowymi informacjami, np. nazwą pomieszczenia czy wzbudzonej czujki. Informacje mogą być wysyłane za pomocą SMS, komunikatu głosowego lub powiadomienia PUSH do aplikacji RopamNeo. Ponadto możliwe jest wysyłanie wiadomości e-mail. Dzięki różnym typom powiadomień można je dopasować do priorytetów zdarzeń i preferencji użytkownika.

Poza funkcjami alarmowymi centrala pozwala na stworzenie „automatyki domowej". Poprzez panele dotykowe lub aplikację RopamNeo system może sterować „na życzenie" urządzeniami w domu, np. bramą wjazdową, bramą garażową, roletami, oświetleniem. Ponadto pozwala na utworzenie typowych scenariuszy, schematów lub kalendarzy dotyczące sterowania, np. automatycznym oświetleniem po wejściu do domu, sterowaniem pompami CO, wentylacją. Dzięki integracji „alarm + automatyka" czujki systemu alarmowego można wykorzystać do automatyki domowej, np. jako wykrywanie obecności do sterowania oświetleniem, ogrzewaniem czy roletami. Centrala ma także funkcje termostatów pokojowych z kalendarzem i dobowymi nastawami temperatury. Pomiar temperatury jest realizowany za pomocą czujników przewodowych lub bezprzewodowych. Termostaty są dostępne jako graficzne menu w panelach dotykowych i aplikacji mobilnej. System wyróżnia się nie tylko funkcjonalnością, ale też niskim kosztem utrzymania. Komunikacja IP wykorzystuje transmisję poprzez WIFI/ETH, a kanałem zapasowym jest GPRS (karta SIM). Ponadto zasilacze o wysokiej sprawności energetycznej i z autokompensacją napięcia ładowania akumulatorów pozwalają na realne obniżenie zużycia energii.

Podstawowe właściwości NeoGSM-IP/NeoGSM-IP-64:
- 2/4 niezależne strefy, z dwoma typami czuwania,
- wbudowana komunikacja GSM i Wi-Fi, opcja ETH,
- powiadomienia: SMS/CALL/PUSH/e-mail
- do 32/64 wejść programowalnych,
- do 24/40 wyjść programowalnych,
- do 16/32 modułów roletowych,
- obsługa czujników temperatury 2/8,
- termostaty pokojowe 1/8,
- do 32 użytkowników (kodów)

Ropam Elektronik s.c.

www.ropam.com.pl
www.ochronadladomu.pl

Kronos Alicja – nowa generacja oprogramowania do stacji monitorowania

Zmiany w obrębie technologii i nasz do niej stosunek wzajemnie na siebie wpływają i w dużej mierze definiują punkt, w którym znajduje się nasza cywilizacja. Dotyczy to zwłaszcza technologii związanej z przetwarzaniem danych. O ile na wcześniejszych etapach ekonomia była napędzana dostępnością zasobów, następnie dostępnością kapitału i ostatecznie dostępnością do rynku zbytu, o tyle obecnie znaleźliśmy się w nowym punkcie. Kluczem staje się dostęp i zdolność do przetwarzania informacji oraz coraz bardziej powszechna akceptacja technologii jako stałego elementu naszego życia.

T E K S T

Sławomir Piela, Bartłomiej Dryja

NEXT! s.c.

W Next! od kilku lat z uwagą przyglądamy się zmianom technologicznym w branży ochrony. Wybuch marketingowej bańki pt. „chmura" pozostawiliśmy obok na półce jako konkretne narzędzie do konkretnych celów. Uznaliśmy, iż ta w sumie dość stara technologia nie jest kluczem do rozwoju. Przeniesienie usług w chmurę, z jednoczesnym gromadzeniem danych wszystkich klientów w jednym miejscu, obniża poziom bezpieczeństwa i zwiększa skalę komplikacji, utrudniając jednocześnie to, co dla agencji ochrony najważniejsze: pełną kontrolę nad procesem.

Czy jesteśmy pewni, kto korzysta z informacji złożonych na serwerze w chmurze? I nie chodzi tu o złą wolę dostarczyciela usługi monitoringu, ale zmiany prawa, które stając się rzeczywistością w Chinach i USA, otwierają dostawców chmur na żądania agencji rządowych. Szczególnie przerażające jest to w przypadku Chin, gdzie tamtejsze ustawodawstwo w praktyce znosi jakąkolwiek prywatność i tajemnicę handlową, czym objęte są także firmy zagraniczne.
Nie można też zapomnieć o zmianach w planie zarządzania bezpieczeństwem wymagających uwzględnienia kilku dodatkowych elementów poza naszą kontrolą. Mowa o infrastrukturze dostawcy Internetu, serwerach DNS, producentach platform chmurowych i wreszcie o dostarczycielach usług monitorowania. Problemy Google'a, Amazona, Facebooka i Microsoftu z zapewnieniem dostępności usług dowiodły, że chmury mogą się zatrzymać, niezależnie od tego, ile środków na ich konstrukcję przeznaczymy. Jako odbiorcy nie mamy żadnego wpływu na takie sytuacje, a co z kumulacją ryzyka? Atak na serwer w Internecie ma konkretną cenę w Darknecie (niezbyt zresztą wygórowaną). Chmura, aby być tania, musi łączyć na jednej maszynie kilku odbiorców. Mamy więc sytuację, w której wyłączenie usługi na skutek ataku DoS na jedną agencję ochrony pracującą w chmurze wyłącza pozostałe.

> Tę technologię można i należy wykorzystywać, ale do obszarów, gdzie powyższe problemy można w wystarczającym stopniu zneutralizować.

Koncepcja chmury jako panaceum jest tylko przykładem. Nasza perspektywa zakłada, że to nie poszczególne technologie same w sobie są tym, co stanowi oś rewolucji, ale umiejętność ich doboru i wykorzystania w kontekście coraz większej akceptacji dla komunikowania się z „systemem". Uznaliśmy, iż ze względu na wystarczający próg akceptacji technologii nadszedł czas, by wprowadzić nową generację systemów monitoringu, które nie porzucając rzecz jasna obecnego zakresu działania, jedynie zastępują ludzi w czynnościach powtarzalnych.

Tak powstał KRONOS Alicja – zestaw sieci neuronowych i usług, które wciąż będą rozwijane i zaczną przejmować coraz szerszy zakres pracy operatora. Dzisiaj Kronos Alicja to jeszcze prototyp, jednak o już dość dużym zakresie kompetencji. Może samodzielnie wykonać wideoobchód, rozpoznać osoby, pojazdy, przedmioty i zwierzęta, do kogoś zadzwonić i poinformować głosem o alarmie, a także wysłać grupę interwencyjną. Potrafi odebrać od klienta informacje zwrotne i reagować na przekazane polecenia, np. otworzyć szlaban. Wkrótce będzie potrafić więcej.
Kronos Alicja to koncepcja i kierunek, który zmieni całą branżę monitoringu. Cieszymy się, iż jesteśmy tymi, którzy tę zmianę rozpoczynają.

Next! s.c.

ul. Cieszyńska 365, 43-300 Bielsko-Biała
Tel.: 33 810 56 45, E-mail: office@next.biz.pl

Unowocześniona seria Q

TEKST
Sylwester Krupa
Hanwha Techwin

W sierpniu br. Hanwha Techwin zaprezentowała swoją unowocześnioną serię Q kamer. Nowe modele kopułkowe mają zaledwie 99 mm średnicy. Zastosowano w nich także nowe przetworniki obrazu, dzięki czemu ich rozdzielczość wzrosła do 5 Mpix.

Seria Q mini jest wyposażona w funkcje mające zapewnić użytkownikom końcowym czerpanie maksymalnych korzyści z rozwiązań oferowanych przez system dozoru wizyjnego.
Nowe kamery są o 40% mniejsze od poprzednich modeli. Zredukowanie wielkości nie wpłynęło jednak na ich możliwości. Nowe minikopuły zapewniają rzeczywiste korzyści licznym użytkownikom końcowym, a w szczególności sprzedawcom detalicznym, dla których ważne jest, aby zainstalowane na ścianach i sufitach kamery były atrakcyjne pod względem estetycznym. W nowej serii zastosowano kompresję H.265 wraz z technologią Wisestream II, która dotychczas była spotykana w modelach serii X.

Business Intelligence w handlu detalicznym

Funkcje zliczania osób, zarządzania kolejkami oraz mapy ciepła – z tych algorytmów analizy obrazu w nowej serii kamer można korzystać bezpłatnie. Umożliwiają sprzedawcom monitorowanie wydajności (efektywności) pracy sklepu pod kątem liczby odwiedzin w stosunku do liczby transakcji (sprzedaży). Menedżerowie mogą wykorzystać uzyskane dane do oceny wpływu promocji i innych działań marketingowych na liczbę osób odwiedzających sklep, mogą również zoptymalizować zasoby ludzkie tak, aby najefektywniej rozlokować personel sklepowy w godzinach największego ruchu klientów.

Nowe minikopuły zostały zintegrowane z Retail Insight, niedawno uruchomionym rozwiązaniem Business Intelligence, które wykorzystuje dane z wideo analityki wbudowanej w kamerach: licznika klientów, zarządzania kolejkami i map ciepła.. Przykładowo, mapy ciepła ze wszystkich kamer z obiektywem *fisheye* (QNF-8010) zainstalowanych w sklepie można wykorzystywać, przedstawiając je jako prezentację graficzną natężenia ruchu klientów. Oprogramowanie to jest w stanie zebrać dane z maks. 500 kamer, dzięki czemu można je zastosować w dużych sieciach handlowych. Wygenerowane dane, dzięki analizie układu (aranżacji) sklepu, mogą przyczynić się do wzrostu sprzedaży oraz zmniejszenia kosztów operacyjnych w efekcie odpowiedniego doboru liczby personelu.
Kamery serii Q mini mają też funkcje umożliwiające ich dopasowanie do warunków panujących w obiektach. Są to m.in. korekcja zniekształceń obiektywu (LDC), szeroki zakres dynamiki (WDR), który działa do 120 dB. Ponadto modele QND-8011 i QND-8021 są wyposażone w wyjście wideo HDMI, umożliwiające wyświetlanie obrazów na monitorze publicznym.

Więcej informacji pod adresem
www.hanwha-security.eu

Hanwha Techwin Europe
ul. Posag 7 Panien 1,
02-495 Warszawa
tel. 607 445 858
www.hanwha-security.eu

Zasilacze buforowe w elektronicznych systemach zabezpieczeń

Elektroniczne systemy zabezpieczeń wymagają urządzeń gwarantujących ciągłość zasilania na wypadek przerw w dostawie energii elektrycznej – nawet przez wiele godzin. W tym celu stosuje się zasilacze buforowe. Wśród nich największą efektywność mają konstrukcje z bezpośrednim przetwarzaniem napięcia sieciowego.

Urządzenia te, wyposażone w przetwornicę impulsową, obniżają napięcie sieciowe i dostosowują je do wymagań danej instalacji. W razie potrzeby wykorzystują akumulatory zewnętrzne, jako awaryjne źródło prądu stałego. Gdy układ jest podłączony do sieci, są one ładowane i utrzymywane w stanie gotowości. W momencie zaniku prądu zgromadzona w nich energia jest kierowana na wyjście zasilające.

Niezawodne i uniwersalne

Doskonałym przykładem impulsowych zasilaczy buforowych są nowe, uniwersalne modele firmy SATEL: APS-1412 oraz APS-724. Jednostki te różnią się między sobą napięciem wyjściowym – 12 V DC w pierwszym przypadku i 24 V DC w drugim. Umożliwia to wybór urządzenia o napięciu odpowiednim dla docelowej instalacji: SSWiN, CCTV, domofonowej, kontroli dostępu, automatyki budynkowej i wielu innych.

Wysoka sprawność energetyczna

Opisywane urządzenia zasilające mają wysoką sprawność energetyczną przekraczającą 90%. Optymalizacja konstrukcji, w tym zastosowanie wysokosprawnych podzespołów, przekłada się na niską emisję ciepła – nie jest wymagane dodatkowe chłodzenie.

Wydajność prądowa

Nowe zasilacze SATEL dysponują również dużą wydajnością prądową. W odniesieniu do APS-1412 jest to 14 A (bez akumulatorów) lub 12 A (zasilanie urządzeń) i 2 A (ładowanie akumulatora), a dla modelu APS-724: 7 A lub 6 A i 1 A. Takie parametry umożliwiają włączenie do systemu elementów charakteryzujących się dużym poborem prądu. Przykładowo, instalacja CCTV wykorzystująca pojedynczy APS-1412 może obejmować do 50 kamer zasilanych prądem do 250 mA.

Stabilne parametry pracy

Wysoka sprawność energetyczna i wydajność prądowa idą w parze z bardzo dobrymi, stabilnymi parametrami pracy obu zasilaczy nawet przy dużych wahaniach napięcia. Wynika to z zastosowania filtrów przeciwzakłóceniowych (na wejściu i wyjściu) oraz aktywnego układu korekcji współczynnika mocy (nawet do 0,99). Ponadto precyzyjna regulacja napięcia, kontrola stanu naładowania akumulatora (z pomiarem rezystancji wewnętrznej), a także funkcja automatycznego odłączenia w przypadku nadmiernego rozładowania przedłużają żywotność awaryjnego źródła zasilania bez ryzyka jego uszkodzenia.
Wysoki poziom bezpieczeństwa zapewniają również zabezpieczenia: przeciwprzeciążeniowe (OCP) i przeciwzwarciowe (SCP).

Sygnalizacja LED

APS-1412 oraz APS-724 są wyposażone w cztery diody LED sygnalizujące status: wyjścia zasilania, akumulatora, zasilania AC oraz zbyt wysoką temperaturę zasilacza. Wykryte awarie są także sygnalizowane na wyjściach typu OC, którym można przypisać dodatkową funkcjonalność, np. w ramach systemu automatyki budynkowej.
Model APS-1412 umożliwia ponadto integrację z wybranymi ekspanderami, modułami komunikacyjnymi czy centralą kontroli dostępu – firmy SATEL – posiadającymi złącze APS. Mogą one odbierać od zasilacza informacje o jego stanie, a także podłączonego akumulatora.

Zgodność z normami

APS-1412 oraz ASP-724 są zgodne z normami: EN 55011 Class B, w zakresie poziomu przewodzonych i promieniowanych zakłóceń EMI, oraz EN 60950-1 (bezpieczeństwo). APS-1412 spełnia również wymagania Grade 2 z katalogu regulacji EN 50131-3.

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

Bezpieczeństwo gości w hotelach

wyzwaniem dla profesjonalistów

TEKST
Wincenty Ignatowski

Do niedawna branża hotelarska charakteryzowała się poważnymi zaniedbaniami wielu obowiązków w zakresie bezpieczeństwa, na szczęście sytuacja ta powoli się zmienia. Zagrożenia wynikające ze wzrostu przestępczości czy terrorystyczne zmuszają do podniesienia poziomu bezpieczeństwa w hotelach.

Stan bezpieczeństwa hoteli

Reputacja obiektu hotelowego często decyduje o jego sukcesie komercyjnym, a zarządzanie bezpieczeństwem obejmuje również tworzenie pozytywnego wizerunku hotelu (gościnność i opiekuńczość czy profesjonalne traktowanie gości hotelowych przez pracowników ochrony). W dużej mierze zależy to od dobrego kontaktu gości m.in. z pracownikiem ochrony lub kierownikiem ds. bezpieczeństwa. Ich wzajemne relacje stanowią istotny element decydujący o tym, czy gość będzie chętniej wracał do hotelu, w którym czuje się bezpiecznie i komfortowo, albo będzie to jego ostatnia wizyta, jeżeli doświadczy braku poczucia bezpieczeństwa.

Zdarzenia przestępcze mające miejsce w hotelu często decydują o tym, że gość rezygnuje z jego usług, a za utratę mienia gości lub aktywów hotelu są obwiniane osoby zarządzające bezpieczeństwem. Nawet jeśli stratę można odzyskać, ofiary nadal odczuwają niezadowolenie, obwiniając security menedżerów o nieefektywność. Dlatego obowiązkiem menedżera ds. bezpieczeństwa jest szkolenie swojego personelu nie tylko w zakresie umiejętności detektywistycznych, ale również umiejętności współczucia i słuchania gości, ponieważ tego wymagają, szczególnie gdy dochodzi do zdarzeń o charakterze przestępczym. W celu zminimalizowania wystąpienia takich zdarzeń musi zaangażować się w działania mające na celu uzyskanie informacji nt. przestępczości. Bardzo ważne są też dobre relacje ze służbami policyjnymi pomagające w lepszym rozeznaniu w statystykach przestępczości wokół obiektu hotelowego, a także w przypadku wystąpienia przestępstw na terenie obiektu hotelowego.

Menedżerowie ds. bezpieczeństwa muszą być osobami innowacyjnymi, znać bieżące trendy i rozwiązania prawne, technologiczne i taktyczne w zakresie zapewnienia bezpieczeństwa i zarządzania nim. Lektura fachowej prasy, uczestnictwo w profesjonalnych stowarzyszeniach, kontakty z innymi kierownikami ds. bezpieczeństwa, którzy napotykają podobne problemy w swoich hotelach, powinny być nieustannie praktykowane. Kładąc nacisk na najlepsze praktyki w zarządzaniu bezpieczeństwem, menedżer ds. bezpieczeństwa odgrywa kluczową rolę w obiekcie hotelowym.

Znaczenie środków bezpieczeństwa w hotelach

Jeszcze nie tak dawno hotele nie były projektowane z myślą o zapewnieniu wysokiego poziomu bezpieczeństwa (nie mówimy tu o bezpieczeństwie pożarowym). Ich właściciele uważali, że ludziom, którzy często podróżują, wystarczy zapewnić w miarę komfortowe warunki. W dobie rosnących zagrożeń zrozumiano, że ochrona majątku hotelu i gości nabrała fundamentalnego znaczenia. Stało się też oczywiste, że coraz bardziej brutalne i bezwzględne działania przestępców (terrorystów) są zagrożeniem dla prowadzonej działalności hotelarskiej. Terroryści skupili się na planowaniu taktycznym ukierunkowanym na hotele sklasyfikowane przez siebie jako „miękkie cele". Goście hotelowi o wysokim statusie społecznym lub ekonomicznym, dyplomaci, politycy czy zamożni biznesmeni stają się łatwym celem terrorystów. Tymczasem firmy ochroniarskie świadczące usługi ochrony w branży hotelarskiej borykają się z problemami braku profesjonalizmu, gdyż edukacja i wdrażanie technik zarządzania bezpieczeństwem są tu ograniczone. Wysoki wskaźnik rotacji pracowników, nieprowadzenie szkoleń pracowników ochrony prywatnej powodują, że poziom bezpieczeństwa w hotelach jest minimalny lub ochrona jest nieefektywna.

Zadowolenie gościa i poczucie bezpieczeństwa osiągnie się tylko wtedy, gdy hotel zapewni zindywidualizowane rozwiązania w zakresie ochrony, a personel ochrony będzie dobrze przygotowany do pełnienia swoich funkcji. Najważniejsze, aby polityka bezpieczeństwa w obiekcie była dostosowana do warunków i okoliczności, w jakich ich właścicielom przyszło prowadzić biznes hotelarski, w przeciwnym razie funkcje bezpieczeństwa okażą się klapą.

Nieefektywność funkcji bezpieczeństwa w hotelach

Niestety należy stwierdzić, że zarządzanie bezpieczeństwem w hotelach często nie odpowiada wymogom bezpieczeństwa. W rezultacie pracownicy ochrony pracują nieefektywnie, a zarządzający, mając do dyspozycji ograniczoną liczbę osób, nie są w stanie ocenić zagrożeń ani prowadzić programów uświadamiających w zakresie bezpieczeństwa. Efektem jest spadek wiarygodności i szacunku dla pracy wykonywanej przez pracowników ochrony.

Nie ma dedykowanego dla branży hotelarskiej elektronicznego rejestru zdarzeń, które pozwolą na analizę ryzyka, na podstawie którego są określane środki służące zabezpieczeniu technicznemu. Ocena ryzyka związanego z bezpieczeństwem jest rzadko przeprowadzana, ponieważ właściciel hotelu uznał, że jego obiekt jest bezpieczny, mimo że zdarzenia przestępcze nadal się zdarzają, a zagrożenie terroryzmem będzie w przyszłości rosło. Dlatego bardzo ważnym zadaniem jest prowadzenie mądrej polityki bezpieczeństwa, wzorowanej na systemie zarządzania inteligentnym budynkiem, który integruje, monitoruje i optymalizuje działanie systemów: kontroli dostępu, włamania i napadu, dozoru wizyjnego oraz systemu przeciwpożarowego. System kontroli dostępu powinien zarządzać prawami dostępu – dla gości i pracowników – do określonych pomieszczeń na terenie hotelu (pokoi, parkingu, części rekreacyjnej).

> Zadowolenie i poczucie bezpieczeństwa gościa osiągnie się tylko wtedy, gdy hotel zapewni zindywidualizowane rozwiązania, a personel ochrony będzie dobrze przygotowany do pełnienia swoich funkcji

System monitoringu wizyjnego z kolei powinien umożliwiać wykrywanie i wizyjną weryfikację wszelkich zagrożeń na obrazie z kamer. Stanowi wsparcie dla służb ochrony hotelu w sytuacjach kryzysowych, natychmiast potwierdzając incydent i co za tym idzie, przyśpieszając reakcję na zagrożenie życia i mienia. System monitoringu może być zintegrowany z systemem kontroli dostępu oraz systemem kasowym w recepcji, umożliwiając weryfikację wizyjną zdarzeń (np. danych dotyczących transakcji).

Z kolei zadaniami systemu sygnalizacji pożarowej (SSP) oraz dźwiękowego systemu ostrzegawczego (DSO) jest szybkie wykrycie źródła pożaru, podjęcie błyskawicznych działań gaśniczych i powiadomienie odpowiednich służb oraz przeprowadzenie ewakuacji ludzi z zagrożonego obszaru.

Uzupełnieniem zintegrowanego systemu bezpieczeństwa powinien być system alarmowy włamania i napadu, sygnalizujący próby włamania zwłaszcza do pomieszczeń szczególnie chronionych (magazynu, pomieszczeń biurowych, serwerowni, sali i pokoi ze sprzętem wysokiej wartości, pomieszczeń sejfów hotelowych czy przechowalni bagażu gości). Elementem tego podsystemu są przyciski przyzywowe pozwalające obsłudze szybko wezwać pomoc grupy interwencyjnej w sytuacji zagrożenia bezpośredniego. Przyciski mogą być wykorzystywane w pokojach dla niepełnosprawnych w celu wezwania pomocy.

Dobór zabezpieczeń powinien zostać poprzedzony starannie wykonaną analizą zagrożeń, z uwzględnieniem szacowania ryzyka ich wystąpienia. Wdrożenie odpowiednich zabezpieczeń nie oznacza osiągnięcia zaplanowanego poziomu bezpieczeństwa. Zadania, które muszą być realizowane ciągle, to monitorowanie aktualnego stanu bezpieczeństwa, doskonalenie i adaptacja systemów oraz dostosowanie do zmieniającego się otoczenia. Ważnym elementem w tym zakresie są również szkolenia i podnoszenie świadomości pracowników ochrony.

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*.

Bezpieczeństwo gościa hotelowego

Podróże są częścią naszego życia, a noclegi w hotelach nieodzownym elementem wyjazdów biznesowych i udanych wakacji. O tym, jak zadbać o bezpieczeństwo gości, ze specjalistami grupy Accor Hotels Andrzejem Bereckim, Security Managerem odpowiadającym za bezpieczeństwo hoteli w Polsce, Rumunii, Czechach, na Węgrzech, Słowacji i Litwie (w środku), i Hubertem Żakiem, Safety Expertem (po lewej), rozmawia Jan T. Grusznic.

Jaką politykę bezpieczeństwa prowadzi sieć hoteli Accor?

ANDRZEJ BERECKI (A.B.): Posiadamy ujednoliconą politykę bezpieczeństwa, zawierającą się głównie w procedurach, które w skrócie nazywamy APACHE. To akronim od nazwy *Accor Process to Act in Crisis Hazard and Emergencies.* Dotyczą one zasad postępowania w różnego typu sytuacjach kryzysowych, np. w razie poważnych awarii czy podejrzenia wykorzystywania seksualnego nieletnich. W dużym skrócie najważniejsze jest bezpieczeństwo własne, bezpieczeństwo gości i powiadomienie odpowiednich służb. Każde zdarzenie jest ewidencjonowane oraz analizowane, dlatego wpływa na poprawę skuteczności polityki bezpieczeństwa w naszych obiektach. Algorytmy postępowania opieramy na wieloletnim doświadczeniu.

Czy różni się ona w zależności od klasy hotelu?

A.B.: Kluczowa jest lokalizacja hotelu, a nie jego klasa.

HUBERT ŻAK (H.Ż.): W naszych hotelach mamy różnych klientów, ale zagrożenia, które z tego wynikają, są takie same. To położenie obiektu definiuje sytuacje, które mogą się wydarzyć. Inne zagrożenia będą np. w hotelu usytuowanym w pobliżu klubu piłkarskiego, do którego po meczu przychodzą kibice, a inne, gdy hotel jest zlokalizowany na przedmieściach.

A.B.: Gdy okoliczne lokale gastronomiczne zostają zamknięte, intruzów przyciągają jasno oświetlone hotelowe drzwi obracające się 24 godziny na dobę przez 365 dni w roku.
W latach 2017–2018 najwięcej zanotowanych zdarzeń stanowiły wizyty osób niebędących gośćmi, a chcących dostać się do hotelu, aby sprawdzić, czy np. można zobaczyć panoramę miasta z dachu. Niestety często osoby takie są pod wpływem różnego rodzaju środków odurzających. Borykamy się głównie z zagrożeniami tego typu.

Jak udaje się wam godzić wymogi bezpieczeństwa z oczekiwaną przez klientów hoteli gościnnością?

A.B.: Goście oczywiście oczekują bezpieczeństwa. Większość z nas czuje się bezpieczniej, wiedząc, że ktoś czuwa i reaguje. Przykładowo ja, jako gość hotelu, chciałbym mieć pewność, że drzwi prawidłowo się za mną zamknęły po opuszczeniu pokoju, a nie tylko domknęły – nawiązując do bezpieczeństwa technicznego. Zdarzają się sytuacje, kiedy złodziej, nie będąc gościem i nie posiadając karty, wchodzi razem z innymi gośćmi do windy i wysiada razem z nimi. Sprawdza potem pokoje, łapiąc po prostu za klamki, i pokój z niedomkniętymi drzwiami może stać się łatwy do spenetrowania.
Czy będzie nietaktem zapytanie takiej podejrzanie zachowującej się osoby czy jest gościem i poproszenie o okazanie karty gościnnej? A co, jeśli się okaże, że przypadkowo wzięliśmy gościa za złodzieja? Chciałbym też np., aby w sytuacji, gdy zablokuję sejf w pokoju, pracownik, który przyjdzie go odblokować, zweryfikuje, czy jestem osobą zameldowaną (używając poprzedniego nazewnictwa) w pokoju. Ja o to się nie pogniewam, jednak nie każdy gość może być wyrozumiały w tej kwestii.
Naszą rolą jest także m.in. sprawdzanie, czy osoby, zwłaszcza młode, które przebywają w hotelu, nie znajdują się w nim wbrew swojej woli.
Zdajemy sobie sprawę, że w tych i innych przypadkach odpowiednie procesy muszą odbywać się zgodnie z procedurami, ale istotą rzeczy jest, aby przeprowadzić to w sposób grzeczny, kulturalny i z wyczuciem, gdyż nie każda nietypowa sytuacja musi być równoważna z przestępstwem.

H.Ż.: Z drugiej strony my sprzedajemy określony produkt. Informujemy gości, że tu jest pracownik ochrony, tu są kamery, takie mamy procedury. To już wybór klienta, czy chce u nas zostać, czy też mu to nie odpowiada.
Utrzymanie poczucia bezpieczeństwa naszych gości traktujemy jak wyścig, w którym staramy się być zawsze o pół kroku z przodu. Czy to jest możliwe? Nie wiem. A czy ma sens? Zawsze, ponieważ pozwala nam w znacznej części – korzystając z tych obszarów wiedzy, techniki, umiejętności i obserwacji – również sprzedawać poczucie bezpieczeństwa. Na rynku przez wiele lat panowało przekonanie, że bezpieczeństwo to koszt. Ja się z tym nie zgadzam. Uważam, że na bezpieczeństwie da się w pewien sposób zarabiać, ponieważ ono wraca w postaci zadowolonego gościa, który skorzysta ponownie z usług tego hotelu, jeśli był zadowolony z pobytu.

Obowiązek informacyjny jest jednym z wymogów RODO. Jak dostosowujecie się do przepisów?

A.B.: Zgodnie z przepisami informujemy gości, że obiekt jest monitorowany i kto jest administratorem danych osobowych. Tabliczki są rozmieszczone w widocznych miejscach. Właściwe informacje znajdują się są też na stronie internetowej. Z każdym hotelem gość może skontaktować się bezpośrednio i poinformować o swoich wątpliwościach lub przekazać pytania. Nie spotkałem się jeszcze z sytuacją powoływania się na przepis bycia zapomnianym, jednak i taką sytuację wnikliwie rozpatrzymy, jeśli się pojawi.

Jakie systemy zabezpieczeń stosujecie w hotelach?

H.Ż.: Mamy dwa wyznaczniki, jeśli chodzi o technologie. Po pierwsze nie sięgamy po rozwiązania, które nie są przetestowane. Moje wieloletnie doświadczenie podpowiada jedno: nie ufaj kartom katalogowym. Rzeczywistość jest taka, że test sprzętu w warunkach laboratoryjnych nie jest miarodajny. Hotel jest instytucją, która pracuje przez 24/7. Nie możemy sobie pozwolić na eksperymenty i w danym obszarze zrezygnować ze starych rozwiązań, by wprowadzić nową technologię. Większość testów przeprowadzamy sami. W pilotażowych systemach CCTV instalujemy kamery w miejscach, gdzie te urządzenia będą musiały się sprawdzić: w lobby, na recepcji, na parkingu. Oczywiście systemy te działają równolegle z innymi już pracującymi w hotelu.
Stosujemy urządzenia z szerokiego spektrum zabezpieczeń, począwszy od zamków hotelowych z kartami pozwalającymi gościom na dostęp do poszczególnych stref, poprzez systemy kontroli dostępu umożliwiające na bieżąco kontrolowanie ruchu pracowników. Zdarza się tak, że w jednym obszarze mamy zainstalowane dwa rozwiązania, korzystamy wtedy np. z kart dualnych.
Mamy też dużo systemów, które zostały opracowane dla poszczególnych obiek-

tów. Proces instalacji urządzeń nie zaczyna się u nas od przetargu, ale od etapu zbierania danych operacyjnych związanych z analizą zagrożeń, ryzykiem ich wystąpienia oraz innych informacji z tego obszaru. Na ich podstawie staramy się wybrać odpowiednie narzędzia. Inne dobieramy do hotelu mieszczącego się w centrum miasta, a inne do obiektu typowo wakacyjnego. Istotą stworzenia profilu bezpieczeństwa hotelu jest analiza obiektu i jego audyt na różnych płaszczyznach. Wiele budynków hotelowych to obiekty historyczne, będące częścią kultury miasta. To też determinuje grupę klientów korzystających z naszych usług.

Po drugie w swoich rozwiązaniach postawiliśmy na profesjonalną i bardzo dobrze wykonaną architekturę sieci, czyli na profesjonalne serwerownie, porządne urządzenia aktywne i certyfikowane okablowanie. Często sięgamy po technologie światłowodowe. Stosujemy taką politykę, że danych z systemów bezpieczeństwa nie wypuszczamy na zewnątrz. Każdy obiekt jest jednostką autonomiczną. Rozwiązaniem online'owym jest u nas tylko system rezerwacji pokoi.

Wdrożenie interesującej nas analityki jest utrudnione prawnie. Chętnie widzielibyśmy możliwość przetwarzania wizerunku przestępcy z ogólnej bazy danych, aby kamera mogła go zidentyfikować już na wejściu do hotelu. Ale na to nie pozwalają przepisy i ustawa. Nie możemy nawet udostępnić wizerunku złodzieja, który okradał nasz hotel, i przesłać go do innej naszej placówki. Zatem kupowanie rozwiązania, z którego tak naprawdę nie możemy skorzystać, jest – z naszego punktu widzenia – bezsensowne.

Innym problemem jest kompletne niezrozumienie potrzeb hotelu przez dostawców i producentów rozwiązań. Weźmy pod uwagę np. recepcję hotelu, w której przemieszcza się kilkadziesiąt osób. To z taką liczbą naraz musiałaby poradzić sobie analityka. Co innego, gdy w obiekcie jest jedna czy dwie osoby, a co innego u nas.

Który z zastosowanych systemów jest kluczowy dla działania hotelu?

H.Ż.: W systemie bezpieczeństwa kluczowym elementem nie są kamery ani system kontroli dostępu. Nadrzędny jest system sygnalizacji pożarowej, ponieważ uruchamia procedurę ewakuacji hotelu w każdej sytuacji kryzysowej. Z naszego punktu widzenia to system sygnalizacji pożarowej jest bardzo istotny dla właściwego funkcjonowania hotelu. Pozostałe systemy traktujemy jako wsparcie – nie są kluczowe, ale jednocześnie w bardzo dużym stopniu mają to bezpieczeństwo wspierać.

Czy ewakuacja hotelu jest uciążliwa dla gości?

A.B.: Robimy wszystko, aby tak nie było, ale oczywiście może się to wiązać z pewnymi uciążliwościami. Współpracujemy z kompetentnymi podmiotami zewnętrznymi mającymi uprawnienia, aby takie próbne ewakuacje co najmniej raz w roku w każdym hotelu przeprowadzać. Zazwyczaj wybierane są takie terminy, gdy obłożenie hotelu jest niewielkie i nie są zaplanowane żadne imprezy konferencyjno-bankietowe. O przeprowadzanych ćwiczeniach goście są informowani z wyprzedzeniem. Oprócz przećwiczenia algorytmów postępowania, ewakuacje takie mają na celu sprawdzenie prawidłowości działania urządzeń i systemów ochrony pożarowej zainstalowanych w hotelu.

A czy systemy zabezpieczeń mogą pomóc w ustaleniu liczby ewakuowanych gości?

H.Ż.: Na świecie jest trzech, może czterech czołowych producentów zamków hotelowych. I są to rozwiązania offline'owe. Bardzo rzadko, ze względu na cyberzagrożenia, stosuje się rozwiązania pracujące w sieci. Jednak nawet gdyby system miał informację, że zamek jest w trybie „zamknięty", nie byłoby 100-procentowej gwarancji, że gość z pokoju wyszedł. Trzeba by było zastosować dodatkowo detekcję obecności osób w pokoju. A to jest bardzo drogie i na świecie jest tylko kilka hoteli, które ją stosuje. W Polsce – żaden.

Nie ukrywam, że testowaliśmy i takie rozwiązania. Staramy się być na bieżąco z nowościami na rynku, ale dzisiaj w naszej ocenie są one jeszcze zbyt zawodne. To zależy, jak pojmujemy integrację. Bo jeśli myślimy jak o inteligentnym budynku, to hotel na dzień dzisiejszy takim budynkiem może być, ale tak naprawdę tylko w obszarach technicznych. Wskazania np. przez systemy CCTV i kontroli dostępu stanowią pewien zbiór informacji, który muszą być przetworzone przez kompetentną, przeszkoloną osobę bazującą na naszych procedurach APACHE czy instrukcjach kryzysowych.

Dziś branża elektronicznych systemów zabezpieczeń oferuje słabą integrację dla obiektów hotelowych. Jeśli już, to korzystamy z integracji opartej na rozwiązaniach BMS. 20- czy 30-letnie doświadczenie tych firm, które zaczynały od wizualizacji temperatury w kotłach, przekonuje nas bardziej, ponieważ rynek systemów zarządzania budynkami bardzo się rozwinął. I właśnie z tymi systemami integrujemy np. kamery czy kontrolę dostępu. Jednocześnie wykonujemy bardzo dużo instalacji pilotażowych, testujemy rozwiązania różnych producentów. Jest to i dla nas, i dla wytwórców korzystne, ponieważ my oferujemy obiekty „żywe" z bardzo dużym natężeniem ruchu trwającym 24 godziny, 7 dni w tygodniu. To idealne pole doświadczalne do usprawniania ich rozwiązań na bazie naszych doświadczeń i sugestii.

Na świecie są organizacje zrzeszające grupy hotelowe, które standaryzują procesy bezpieczeństwa i udostępniają wyniki analiz incydentów. Czy z nich korzystacie?

H.Ż.: Tak, korzystamy z doświadczeń i wiedzy innych. Jeśli w hotelu w Szwajcarii miało miejsce włamanie (do systemu komputerowego zarządzającego zamkami pracującymi w trybie online – przyp. red.), analizujemy ten przypadek pod kątem naszych zabezpieczeń. Problem z czerpania doświadczeń, chociażby amerykańskich, sprowadza się do tego, że to kompletnie inny kraj, inny rynek i inne zagrożenia. My dywersyfikujemy bezpieczeństwo w obszarach lokalizacji hotelu w kraju.

Czy oprócz elektronicznych systemów zabezpieczeń stosujecie ochronę fizyczną?

A.B.: Tak współpracujemy z zewnętrznymi agencjami ochrony, których pracowników szkolimy, wspieramy, stosujemy instrukcje ochrony bazujące na APACHE-u, specjalnie dla nich zmodyfikowane. Pracownik ma inne niż recepcja zadania, np. w razie podejrzenia wykorzystywania seksualnego. Przeprowadzamy szkolenia pracowników hotelu oraz ochrony m.in. w zakresie świadomości bezpieczeństwa, tak aby wszyscy wiedzieli, na jakie nietypowe zachowania lub zdarzenia zwracać uwagę i w jaki sposób reagować. Osobiście posiadam prawie 20-letnie doświadczenie w pracy oraz zarządzaniu w Działach Ochrony warszawskich 5-gwiazdkowców. Czy zdarzały się sytuacje kryzysowe, siłowe? Tak, jednak 95% przypadków udało się rozwiązać za pomocą argumentów słownych. To jest kierunek, w którym zmierza branża security, zapewniając bezpieczeństwo nie tylko w hotelach.

Z jakimi incydentami spotykacie się najczęściej w hotelach w Polsce? A jakie są w hotelach europejskich?

A.B.: Incydentów kryzysowych nie mamy zbyt wiele. Zależą one głównie od lokalizacji. Jak wspomniałem wcześniej, najwięcej jest tych związanych z osobami postronnymi niebędącymi naszymi gośćmi. Obserwujemy stosunkowo niewielką liczbę alarmów pożarowych, które niejednokrotnie spowodowane są paleniem papierosów w pomieszczeniach hotelu. Zdarzały się ewakuacje spowodowane odebraniem informacji o podłożeniu ładunku wybuchowego.

W skali Europy też jest spokojnie. W Budapeszcie, gdzie mamy 16 hoteli, naszymi gośćmi są głównie turyści, a miasto jest pełne patroli policji. Statystycznie najwięcej incydentów występuje w Polsce, szczególnie w Warszawie. Związane jest to przede wszystkim z większą liczbą gości hotelowych i z lokalizacją. Jednym z niedawnych wydarzeń w stolicy była akcja pracownika hotelu i ochrony, którzy wspólnie podjęli reanimację gościa i za pomocą defibrylatora przywrócili mu czynności życiowe. Dodam, że w każdym z naszych hoteli znajduje się defibrylator.

Czy w przyszłości trendem będzie automatyzacja, hotele bezobsługowe?

H.Ż.: Mamy już takie hotele we Francji: Formuła 1, są przeznaczone dla innego typu klienta. W Polsce też robiliśmy pilotaże rozwiązania automatycznej recepcji, czyli takiego, w którym gość rejestrujący się online rezerwujący pokój dostaje od nas elektroniczny klucz i może bez pośrednictwa recepcji, po przyjeździe do hotelu udać się bezpośrednio do pokoju. Z naszych obserwacji wynika, że na to rozwiązanie nasz rynek nie jest jeszcze gotowy. Przyczyny tego są trzy: większość z nas korzysta z telefonu jako źródła informacji i oczywiście urządzenia do rozmów. Jednak część nie chce lub nie potrafi pobrać i obsługiwać właściwej aplikacji. Druga sprawa to liczba błędów, które te systemy generują. Trzecia wynika z tego, że my nie eksperymentujemy, ale stosujemy rozwiązania sprawdzone, wychodząc z założenia, że bezpieczeństwo jest najważniejsze.

Ryzyko związane z wprowadzeniem niesprawdzonego rozwiązania jest dla nas zbyt kosztowne. Dlatego w naszych obiektach zawsze dywersyfikujemy rozwiązania ochronne. Przykładowo awaria kamery nie powoduje braku podglądu z danego obszaru, gdyż ten sam obszar jest objęty dozorem przez inną kamerę.

Nie mam wątpliwości, że hotele bezobsługowe są przyszłością hotelarstwa. Jestem zdania, że rozwój ich przyspieszy, gdy na rynku pojawi się rozwiązanie, które połączy wykorzystywane technologie, takie jak rezerwację i płatności online, analitykę, systemy dozoru wizyjnego, kontroli dostępu i sygnalizacji pożarowej w jedno zintegrowane rozwiązanie. Już teraz mamy na rynku kilku integratorów, ale naszym zdaniem ich rozwiązania nie są jeszcze gotowe, by spełniać nasze potrzeby. Trzeba czasu na dopracowanie szczegółów.

Dziękuję za rozmowę.

Hikvision w hotelach

Zastosowanie systemów monitoringu wizyjnego w obiektach hotelowych to już standard. Poprawiają jakość funkcjonowania obiektu, podnoszą poziom bezpieczeństwa gości hotelowych i personelu, pozwalają uniknąć obecności niepowołanych osób na terenie obiektu. Monitorują i sprawują kontrolę nad pracą obsługi hotelowej, co znacząco wpływa na wzrost wydajności i rzetelności ich pracy. Zarejestrowane nagrania mogą też stanowić cenny materiał dowodowy.

Kolejną korzyścią wynikającą z zastosowania systemu monitoringu wizyjnego jest spadek liczby kradzieży i większa dbałość o mienie hotelu i jego klientów. Obiekty hotelowe ze względu na swoją specyfikę są miejscami szczególnie narażonymi na różne sporne sytuacje. Zapisy z monitoringu mogą być więc cennym materiałem dowodowym dla policji w przypadku kradzieży czy pobicia, przydatnym także w kontrowersyjnych sytuacjach zaistniałych na terenie hotelu. Dlatego szczególnie ważne jest odpowiednie zabezpieczenie zarejestrowanego materiału. Jedną z funkcji umożliwiającą ochronę nagrań w rejestratorach Hikvision jest tryb *Hot Spare* – możliwość podłączenia rejestratora nadmiarowego (uruchamianego w przypadku awarii).

Dodatkowe zabezpieczenie oferują kamery z kartami Micro SD, które w połączeniu z rejestratorem umożliwiają skonfigurowanie funkcji zabezpieczenia rejestrowanego materiału o nazwie ANR. Nagrania na karcie SD są zapisywane tylko w przypadku problemów z łącznością pomiędzy kamerą a rejestratorem, po usunięciu awarii są automatycznie synchronizowane i dopisywane do rejestratora.

Skuteczność systemu monitoringu wizyjnego przede wszystkim zależy jednak od parametrów technicznych użytych kamer, ich prawidłowego rozmieszczenia i montażu. Newralgicznymi punktami w obiektach hotelowych są: wejścia i wyjścia w budynku, recepcja, korytarze hotelowe, parkingi oraz obszar przed budynkiem. Ich obserwacja daje właścicielom/zarządzającym ogólny wgląd na przestrzeń użytkową, pozwala na łatwe kontrolowanie sytuacji w obiekcie, a dzięki inteligentnym funkcjom usprawnia pracę całego obiektu.

W dozorze przestrzeni hotelowej świetnie sprawdzają się kamery i rejestratory z serii Easy IP 4.0. Są to urządzenia o wysokiej rozdzielczości (do 4K) wyposażone w oszczędny algorytm kompresji H.265+, znacznie wydłużający czas archiwizacji danych, a także sprzętowy WDR 120 dB, co jest szczególnie istotne w przypadku obserwacji scen o dużym kontraście oświetlenia: wejść do budynku, przeszklonych przejść. Dzięki wykorzystaniu technologii głębokiego uczenia kamery znacząco zwiększają dokładność wskazania miejsc wystąpienia alarmów, umożliwiając łatwiejsze i przede wszystkim skuteczniejsze przeszukiwanie nagrań wideo. Dzięki precyzyjnemu rozpoznawaniu obiektów system może odfiltrować do 90% zdarzeń wywołujących fałszywe alarmy, co znacząco obniża koszty pracy.

Funkcjonalność hotelu znacznie poprawia zaawansowana analiza obrazu oferowana przez kamery Hikvision, np. odczyt tablic rejestracyjnych czy inteligentne porównywanie obrazów twarzy osób znajdujących się w polu widzenia kamer z bazą uprzednio zapisanych zdjęć. Ze względu na oryginalność wykończenia wnętrz obiektów hotelowych w ofercie Hikvision znajdują się także kamery umożliwiające dyskretny montaż.

Jednym z przykładów systemu dozoru wizyjnego zrealizowanego z wykorzystaniem urządzeń Hikvision jest luksusowy hotel Sofitel w Paryżu, zlokalizowany w okolicy Łuku Triumfalnego i Place de l'Etoile, zaledwie 15 minut spacerem od słynnych Pól Elizejskich. Liczni goście paryskiego hotelu cenią sobie prywatność i luksus, a także poczucie bezpieczeństwa, zapewniane przez urządzenia Hikvision. Zainstalowany w hotelu system monitoringu wizyjnego składający się z wandaloodpornych kamer IP oraz rejestratorów sieciowych skutecznie monitoruje przestrzeń obiektu, w tym główny hol hotelowy, wyjścia ewakuacyjne oraz korytarze prowadzące do pokoi gości. Kamery o odpowiednich, wysokich parametrach technicznych umożliwiają uzyskanie obrazu o wysokiej rozdzielczości, a solidna, wytrzymała konstrukcja obudowy chroni przed potencjalnymi wandalami. □

Hikvision Poland

ul. Żwirki i Wigury 16B,
02-092 Warszawa
tel. 22 460 01 50,
faks 22 464 32 11
e-mail: info.pl@hikvision.com

Największe wyzwania stojące przed security menedżerami

w obiektach instytucji finansowych

Kluczowym celem działalności instytucji finansowej jest świadczenie na rzecz klienta usług finansowych. Klienci powierzają tam swoje oszczędności, są to zatem instytucje zaufania publicznego. Aby zapewnić właściwy poziom bezpieczeństwa, budzący jednocześnie zaufanie klientów, instytucje finansowe stale dokonują analiz ryzyka i możliwych zakłóceń bezpieczeństwa w wielu obszarach prowadzonej działalności i procesów biznesowych.

TEKST
Marcin Kamieniorz

PYTANIE FUNDAMENTALNE – CZYM JEST ZARZĄDZANIE RYZYKIEM I DLACZEGO JEST ONO TAK SZCZEGÓLNIE ISTOTNE W BANKU?

Termin ryzyko wywodzi się z języka włoskiego (*risico*), oznaczając przede wszystkim przedsięwzięcie, którego wynik jest nieznany albo niepewny. Ryzyko jest związane z wszelką działalnością człowieka, a każdy, dokonując codziennych wyborów życiowych, podświadomie i świadomie zarządza ryzykiem. Jedna z najprostszych definicji określa zarządzanie ryzykiem jako podejmowanie działań mających na celu rozpoznanie, ocenę i sterowanie ryzykiem oraz kontrolę podjętych działań. A celem zarządzania jest ograniczanie ryzyka oraz zabezpieczanie się przed jego skutkami. Bank, jako instytucja finansowa, zarządza ryzykiem na wielu płaszczyznach - kredytowym, rynkowym i operacyjnym zgodnie z zasadami określonymi w normach polskiego prawa, regulacjami Komisji Nadzoru Finansowego oraz innych uprawnionych organów.

Jako że ryzyko jest terminem bardzo obszernym, wyróżnia się wiele jego podziałów. Są one przydatne z praktycznego punktu widzenia, gdyż pomagają odpowiedzieć na kluczowe pytania – w jaki sposób, kiedy i jak ujawnia się ryzyko. Rodzaje ryzyka wynikają z różnych źródeł i można je sklasyfikować wg różnych kryteriów. W banku proces zarządzania ryzykiem można podzielić na dwa główne obszary: ryzyka finansowego oraz niefinansowego. Cechą charakterystyczną ryzyka finansowego jest jego mierzalność, np. możliwość bezpośredniego uchwycenia jego wpływu na wynik finansowy. W artykule przyjrzymy się bliżej ryzyku niefinansowemu, które dużo trudniej opisać w jednym zdaniu.

Ryzyko niefinansowe obejmuje funkcje zarządzania ryzykiem operacyjnym i ryzykiem braku zgodności (*compliance*). Ryzyko operacyjne jest rozumiane jako możliwość wystąpienia bezpośredniej lub pośredniej straty wynikającej z niedostosowania lub zawodności wewnętrznych procesów, ludzi i systemów lub ze zdarzeń zewnętrznych. Podstawowym celem w zarządzaniu ryzykiem operacyjnym jest ciągła poprawa bezpieczeństwa banku i jego klientów. Kluczem do efektywnego zarządzania obszarem ryzyka niefinansowego jest dogłębne poznanie i rozumienie tego obszaru, pozwalające zidentyfikować procesy, a następnie ryzyka, które im towarzyszą.

Skuteczne zarządzanie ryzykiem operacyjnym wymaga podziału zadań i odpowiedzialności. Najczęściej cały obszar można podzielić na minimum dwie linie obrony:
- jednostki wykonawcze (1LO),
- jednostki nadzorujące (2LO).

Dla instytucji finansowej istotnym obszarem ryzyka jest bezpieczeństwo fizyczne. Uzyskuje się je poprzez kombinację środków zabezpieczeń: pasywnych i aktywnych. Należy ono do 1LO (linii obrony), a jego zadaniem jest zapewnienie ochrony pomieszczeń, sprzętów, infrastruktury i personelu przed bezpośrednim działaniem czynników fizycznych oraz zdarzeń, takich jak:
- zagrożenia środowiskowe: pożar, powódź,
- kradzież, wandalizm, terroryzm.

JAKĄ ROLĘ PEŁNI SECURITY MANAGER W OBSZARZE BEZPIECZEŃSTWA?

Obrazowo działania w obszarze bezpieczeństwa fizycznego pierwszej linii obrony (1LO) można porównać do linii frontu, a security menedżer jest tu dowódcą. Jego rolą jest organizacja skutecznej pracy jednostki. On odpowiada za strategię procesu zapewnienia bezpieczeństwa oraz jego realizację. W zakresie jego obowiązków jest odpowiedzialność za bezpieczeństwo oraz organizacja współpracy z biznesem wewnątrz instytucji i na zewnątrz, z szeroko rozumianymi organami ścigania.

JAKIE SĄ CECHY DOBREGO I SKUTECZNEGO SECURITY MENEDŻERA?

To osoba bardzo dojrzała emocjonalnie, pewnie radząca sobie w sytuacji kryzysowej i potrafiąca bezzwłocznie ją rozwiązywać. Ze względu na złożoność działań powinna mieć dużą łatwość komunikacji werbalnej by precyzyjnie obrazować i uzasadniać ryzyko, co wiąże się również z dużą świadomością w obszarze technologicznym.

Jednak jedną z głównych cech jest zdolność kierowania zespołem i licznymi projektami jednocześnie – często pod presją czasu. Niezastąpiona jest umiejętność autorefleksji, gdyż jedynie częsta analiza wniosków może prowadzić do ulepszania procesów bezpieczeństwa.

W JAKI SPOSÓB SECURITY MENEDŻER W INSTYTUCJI FINANSOWEJ POWINIEN PODEJŚĆ DO ZBUDOWANIA STRATEGII BEZPIECZEŃSTWA I JEJ WDROŻENIA?

Istnieje wiele standardów zarządzania ryzykiem. Do najpopularniejszych należą FERMA, COSO. Szczegóły ich dotyczące można znaleźć w wielu publikacjach i materiałach źródłowych, tym niemniej trudno w tym miejscu pominąć ich etapy:

- zidentyfikowanie i opisanie wszystkich procesów bezpieczeństwa w kontekście procesów biznesowych,
- ocena ryzyka wszystkich zidentyfikowanych procesów bezpieczeństwa,
- ewaluacja ryzyka – wypracowanie decyzji, czy wartość oceny ryzyka jest akceptowalna, czy nie,
- mitygacja ryzyka – postępowanie wobec ryzyka, skutkujące jego zmniejszeniem (obniżeniem) do poziomu akceptowalnego – zgodnego z zaakceptowanym „apetytem" na ryzyko,
- raportowanie ryzyka,
- monitorowanie ryzyka.

Aby zminimalizować skutki dynamiki procesów biznesowych oraz zagrożeń, konieczne są następujące działania:
- okresowy (generyczny) przegląd procesów biznesowych i ryzyka już zidentyfikowanego,
- bieżące reagowanie na incydenty/zdarzenia mogące być skutkiem nowego źródła ryzyka.

Na ocenę ryzyka składają się: analiza ryzyka, identyfikacja ryzyka, opis ryzyka, pomiar ryzyka.

CZYM JEST MAPOWANIE PROCESÓW I JAKI JEST JEGO CEL W ASPEKCIE BEZPIECZEŃSTWA BANKOWEGO?

Działania w obszarze bezpieczeństwa z czasem komplikują się i rozbudowują. Dlatego ich fundamentem jest stworzenie przejrzystej mapy, która zobrazuje podstawowe założenia, prowadzone działania i wszystkie zależności. Mapowanie procesu to metoda identyfikacji nieprawidłowego działania procesu oraz zrozumienia, co należy poprawić. Jednocześnie uzmysławia uczestnikom procesu, że powinny zostać wdrożone działania naprawcze, aby w przyszłości działał on lepiej i sprawniej.
Oczywiście nigdy nie mamy i nie będziemy mieli pewności, że cały proces został „zmapowany" w kontekście oceny ryzyka. Co więcej, w dowolnym czasie, każdego dnia, pojawiają się nowe zagrożenia i tego nie zmienimy.

Wyzwania w zakresie nowych technologii

Istotnym wyzwaniem jest stałe poszukiwanie nowych, skutecznych środków hamowania, tj. mitygacji ryzyka. Specyficznym wyzwaniem w tym obszarze jest zderzenie tradycyjnego podejścia uznającego ochronę czynną (fizyczną) za jedyny skuteczny środek mitygacji ryzyka, z podejściem nowoczesnym, polegającym na technicznej ochronie obiektów. W tym obszarze widać nadal „twarde"

Stałym wyzwaniem dla security menedżera jest utrzymanie świadomości personelu w zakresie bezpieczeństwa – konieczne są bieżące szkolenia i zmiana niewłaściwych nawyków

decyzje i warunki stawiane przez policję w procesie uzgadniania planów ochrony.
Realizacja „twardego" podejścia do ochrony czynnej w obiektach nie wyklucza oczywiście stosowania nowoczesnych technologii w tym obszarze. Co więcej, można zdecydowanie podnieść skuteczność takiej ochrony, stosując odpowiednie interfejsy prezentacji/obrazowania oraz sterowania dla pracowników ochrony.
Trzeba podkreślić, że nowoczesne rozwiązania techniczne polegają przede wszystkim na maksymalnej automatyzacji procesów, w tym procesów bezpieczeństwa. A szeroko rozumiana automatyzacja pozwala na ograniczenie błędów ludzkich, przez to wymuszając poprawny proces, w tym zachowania osób chronionych i chroniących. Uzyskanie tego wymaga zdigitalizowania procesów bezpieczeństwa, cyfryzacji systemów i ich integracji.
Na drodze w kierunku nowoczesnej technologii w obszarze bezpieczeństwa istotnym wyzwaniem są skutki tej rewolucji technologicznej w obszarze ryzyka fizycznego.

Wyzwania te można pogrupować na dwie kategorie:

1. Kompetencje personelu

Mając na uwadze technologie komputerowe stosowane w nowoczesnych zintegrowanych systemach bezpieczeństwa, istotnym wyzwaniem jest pozyskanie osób z nowymi kompetencjami, a w szczególności obszerną wiedzą z obszaru IT. Na początku tego procesu jest analiza realnych kompetencji wewnątrz oraz na zewnątrz organizacji (firmy).

Kolejnym istotnym wyzwaniem jest analiza i decyzja, czy nowe „kompetencje" powinno się budować w organizacji, czy też pozyskać z zewnątrz. W ten sposób dochodzi się do kolejnych wyzwań:
- jaki zakres procesu lub czynności można bezpiecznie dla organizacji „outsorcować"?
- jakie są dodatkowe ryzyka związane z outsourcingiem procesu lub czynności w procesie?

Gdy znajdziemy odpowiedzi na powyższe pytania, pojawiają się kolejne wyzwania:
- zakres i jakość usług oferowanych przez zewnętrznych dostawców,
- jak skutecznie ocenić potencjalną jakość usług?
- czy wystarczą prezentacje, wizytacje?
- jakie audyty należy przeprowadzić, aby mieć pewność, że jakość usług jest na akceptowalnym poziomie?
- jak zapewnić długofalowe relacje z partnerem outsourcingowym,
- jakie parametry kontroli jakości usługi należy uzgodnić?

Na to nakłada się kwestia zakresu usług, czyli na ile aktualne doświadczenie i kompetencje wykonawcy pokrywają się z oczekiwaniami kupującego usługę. Każda organizacja (firma) ma różne procesy, wobec tego doświadczenia stron są zawsze inne. Konieczna jest precyzyjna analiza procesów i usług wykonawcy w celu wykrycia różnic. Następnie należy precyzyjnie uzgodnić sposób ich realizacji.

2. „Kompetencje sprzętu" rozumiane jako jakość sprzętu i aplikacji (systemów)

Dużym wyzwaniem jest znalezienie systemu spełniającego oczekiwane funkcjonalności oraz parametry użytkowe. Mając na uwadze oczekiwaną integrację wielu systemów, nie jest to łatwe. Obecnie, mimo dużego już rozwoju rozwiązań technologii IT w obszarze systemów zabezpieczeń, znalezienie kompletnie zintegrowanego systemu, który będziemy potrafili sprawnie zastosować z wykorzystaniem istniejących już rozwiązań technicznych w zajmowanych budynkach, jest bardzo trudne, a nawet – zaryzykuję stwierdzenie – prawie niemożliwe.
Skutecznym rozwiązaniem może być integracja istniejących już technicznych systemów na wyższej warstwie, z wykorzystaniem dostępnych API komunikacyjnych systemów lub urządzeń i przenosząc istotną logikę biznesową na ten poziom architektury systemu. Alternatywą jest zakup zintegrowanego systemu z dużą kastomizacją do posiadanych lokalnych systemów i urządzeń oraz procesów.
Budowanie własnego systemu lub duża kastomizacja istniejącego, dzięki jego unikalności wnosi istotną wartość w postaci poufności tego konkretnego rozwiązania. Jest to niezmiernie istotne w kontekście bezpieczeństwa całego systemu. Ponadto ważne jest sprawdzenie i zapewnienie właściwych parametrów wydajnościowych tych systemów, w szczególności w kontekście technologii dopuszczonej w danej organizacji (firmie).

Mając na uwadze szeroko rozumiany obszar technologii IT, naturalnym kolejnym wyzwaniem jest zapewnienie bezpieczeństwa systemowi bezpieczeństwa, tj.: odporności na włamania, integralności, poufności oraz dostępności. Zakładając, że sobie poradzimy z powyższym, nie zapominajmy o wymogach związanych z elastycznością wybranego rozwiązania. Musimy pamiętać, że wyboru dokonujemy na podstawie aktualnej wiedzy, doświadczenia i bieżących procesów. Jednak dynamika biznesu wymaga sprawnego reagowania na zmiany procesów biznesowych i nowe ryzyka.
Nie można oczywiście pominąć konieczności stałego podnoszenia świadomości nowych zagrożeń, skutków niewłaściwego zachowania oraz zastosowanych środków technicznych.
Zintegrowany system bezpieczeństwa gromadzi centralnie olbrzymią ilość danych, przede wszystkim nt. aktywności personelu, procesów biznesowych, zdarzeń bezpieczeństwa oraz zdarzeń technicznych. Trudno ten potencjał przecenić. Daje on ogromne możliwości przekształcenia na wiedzę i wartość biznesową.

Podsumowując:

W sektorze bankowym kluczową kwestią jest bezpieczeństwo środków i danych klientów oraz partnerów, na które należy zwracać szczególną uwagę w codziennych działaniach. Na bieżąco trzeba obserwować zagrożenia i analizować ich wpływ na infrastrukturę teleinformatyczną (aplikacje, systemy, sieci), a także procesy biznesowe oraz ich potencjalny wpływ na klientów. Na tej podstawie należy projektować i wdrażać odpowiednie rozwiązania organizacyjne i techniczne, z naciskiem na systemy cyberbezpieczeństwa. Stałym wyzwaniem dla security menedżera jest utrzymanie świadomości personelu w zakresie bezpieczeństwa – konieczne są bieżące szkolenia i zmiana niewłaściwych nawyków.
Instytucje finansowe, ze względu na realizowane procesy przetwarzania środków pieniężnych, są instytucjami zaufania publicznego. Ich reputacja jest podstawą zaufania klientów.
Security menedżer jest odpowiedzialny za realizację wszystkich podstawowych „liniowych" procesów w obszarze ryzyka niefinansowego. Jego działania i sukcesy lub zaniechania i porażki mają bezpośredni wpływ na reputację instytucji. ▫

BIO

Marcin Kamieniorz

Ponad 21-letnie doświadczenie w pracy w ING Banku Śląskim, z czego 18 lat w Ryzyku Operacyjnym.
Przez 6 lat pełnił funkcję menedżera w obszarze bezpieczeństwa fizycznego, od 3 lat w IT na stanowisku architekta IT.

MATERIAŁY ŹRÓDŁOWE:

Zintegrowany Raport Roczny ING Banku Śląskiego 2018

RODO w monitoringu wizyjnym

SYSTEM MONITORINGU WIZYJNEGO JEST CORAZ BARDZIEJ POWSZECHNĄ FORMĄ OCHRONY OSÓB I MIENIA ZARÓWNO W INSTYTUCJACH, JAK I DOMACH PRYWATNYCH. WRAZ Z ROSNĄCYMI WYMAGANIAMI DOTYCZĄCYMI OCHRONY PRYWATNOŚCI I ZWIĘKSZAJĄCĄ SIĘ POPULARNOŚCIĄ KAMER DOZOROWYCH NALEŻY ZADBAĆ O SZEREG SPRAW.

TEKST
Piotr Powązka

Organizacje, firmy dostarczające i projektujące tego typu rozwiązania, a także osoby prywatne powinny bacznie przyjrzeć się wymogom w zakresie wykorzystania monitoringu, np. w aspekcie regulacji RODO. Osoby prywatne często są przekonane, iż przepisy RODO w tym zakresie ich nie dotyczą. Otóż nie zawsze, na co wskazują organy nadzorcze. RODO nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach działalności osobistej lub domowej, czyli bez związku z działalnością zawodową lub handlową.

W kontekście monitoringu wizyjnego działalność osobista lub domowa może polegać na monitorowaniu terenu własnej posesji. Ten aspekt przysparza trudności, gdyż niejednokrotnie kamera zasięgiem widzenia obejmuje również przestrzeń publiczną, np. chodnik czy dom sąsiada. W takich sytuacjach, zgodnie z dotychczasową praktyką, trudno mówić o typowo domowym użytku. Monitoring nie może naruszać prawa osób trzecich, a ponadto nie może dochodzić do rozpowszechniania nagrań.

Monitoring wizyjny i jego stosowanie nie jest wbrew pozorom sprawą prostą ze względu na brak jednolitych przepisów. Należy pamiętać zarówno o przepisach RODO, ustawy o ochronie danych osobowych, ustawy tzw. wprowadzającej RODO, jak i ustawach branżowych.

Europejska Rada Ochrony Danych (EROD) wydała opinię w zakresie wymogów, jakie należy spełniać przy stosowaniu i projektowaniu systemu monitoringu wizyjnego. Do 9 września 2019 r. można było składać do niej uwagi, gdyż podlegała konsultacjom. W opinii można przeczytać, iż utrwalanie wizerunku w celu zabezpieczenia nieruchomości kończy się na granicy tej nieruchomości.

Zwrócono w niej również uwagę na kamery stosowane w samochodzie. Jeśli są one zaprogramowane w sposób uniemożliwiający identyfikację osób (maskowanie numerów rejestracyjnych na nagraniu), wówczas można mówić o domowym użytku i korzystać z wyłączenia. Ciekawe, czy w dłuższej perspektywie opinia ta wywoła burzliwe dyskusje w tym temacie. O ile kamery cofania raczej nie rejestrują obrazu, o tyle bardzo popularne już wideorejestratory samochodowe, w celu choćby udowodnienia wykroczenia, rejestrują wszystko, łącznie z tablicami rejestracyjnymi. W niektórych krajach, np. w Austrii, stosowanie wideorejestratorów w samochodzie jest zabronione.

Przepisy są niespójne, więc przyjdzie nam zapewne jeszcze poczekać. Z premedytacją w tym artykule nie będziemy rozstrzygali, czy numery rejestracyjne nadal są daną osobową, gdyż kontrowersje nie milkną.

Wytyczne EROD wskazują, iż zarejestrowany materiał wizyjny przedstawiający osobę, której dane dotyczą, w okularach lub na wózku inwalidzkim poruszającym się np. przy budynku, nie jest uważany za przetwarzanie danych osobowych szczególnych kategorii. Jednakże na podstawie zdjęć przedstawiających możliwe do zidentyfikowania osoby biorące udział w proteście, strajku czy manifestacji można już wywnioskować ich poglądy polityczne. To implikuje zastosowanie art. 9 RODO.

Ponadto zarówno EROD, jak i Urząd Ochrony Danych Osobowych (UODO) wskazują na zasady, jakimi należy się kierować w przypadku stosowania systemu monitoringu wizyjnego.

ROZWAŻAJĄC INSTALACJĘ KAMER MONITORINGU, NALEŻY PAMIĘTAĆ O ZASADACH WPROWADZONYCH PRZEZ RODO:

Jak te zasady przekładają się na podmioty stosujące system monitoringu wizyjnego?

• NIEZBĘDNOŚĆ, PROPORCJONALNOŚĆ I LEGALNOŚĆ (art. 5 RODO)

Innymi słowy chodzi o cel, do jakiego monitoring wizyjny jest niezbędny. Badania NIK-u prowadzone w latach 2010–2013 dobitnie wskazały, iż podmioty mają problemy z uzasadnieniem niezbędności (zasadnością) stosowania monitoringu. Mimo że upłynęło kilka lat, nadal widać trudności w określeniu zasadności stosowania tego rozwiązania technicznego. Organy EROD czy PUODO stoją na stanowisku, iż system monitoringu wizyjnego powinien być stosowany wtedy, gdy nie ma alternatywnych metod (np. dodatkowe patrole ochrony w celu zapewnienia bezpieczeństwa). Podobnie jest z proporcjonalnością, gdyż musimy określić wiele różnych elementów systemu takich jak:

- rodzaj kamer oraz jakość obrazu (analogowe, IP itp.),
- rozwiązania statyczne czy mobilne, z kamerami PTZ śledzącymi ruch obiektu lub bez,
- pole widzenia oraz zasięg kamer,
- sposoby rejestracji oraz funkcjonalności (algorytmy) dotyczące analizy obrazu,
- jakie kategorie danych osobowych jesteśmy w stanie pozyskać, stosując kamery monitoringu,
- czy jesteśmy w stanie skorelować już posiadane dane osobowe z pozyskanymi z systemu monitoringu,
- jak długo przechowywać nagrania.

• OBOWIĄZEK INFORMACYJNY

Wobec osób objętych monitoringiem wizyjnym należy realizować obowiązek informacyjny (art. 12 i art. 13 RODO). Nieruchomości i obiekty budowlane objęte dozorem kamer oznacza się w sposób widoczny i czytelny informacją o monitoringu za pomocą odpowiednich znaków. Obowiązek informacyjny powstaje niezależnie od konieczności zapewnienia odpowiedniej podstawy do przetwarzania danych osobowych.

Obowiązki informacyjne można realizować w formie pisemnej:

- ulotki w miejscu obserwacji, np. podczas imprezy plenerowej,
- obwieszczenia w miejscu obserwacji,
- informacja na stronie internetowej, np. w związku z wydarzeniem (m.in. sesja rady gminy),

oraz formie dźwiękowej:

- ogłoszenia przekazywane za pośrednictwem systemów nagłaśniających (np. w zakładach pracy, szkołach, na dworcach czy w centrach handlowych),
- przekazywanie informacji przez operatora kamery, np. nasobnej lub umieszczonej w pojeździe.

Obowiązek informacyjny o obecności kamer można i należy realizować w sposób warstwowy. Trzeba wydzielić pewien zakres kluczowych informacji i udostępnić je przed wejściem w obszar monitorowany, przekazując maksymalną ilość najważniejszych informacji – szczegółowe dane na temat celów przetwarzania, kto jest administratorem danych osobowych oraz możliwości kontaktu z nim, praw przysługujących osobie, której dane dotyczą, oraz najistotniejszych skutków przetwarzania. Należy poinformować o inspektorze ochrony danych osobowych (jeśli został powołany) oraz udzielić informacji, gdzie można zapoznać się z pełną klauzulą informacyjną.

Z niektórych przepisów wynika maksymalny 3-miesięczny okres przechowywania nagrań. PUODO sugeruje przyjmować krótsze terminy, chyba że przepisy wskazują inaczej (np. 3 lata według ustawy o grach hazardowych). Taki czas retencji trzeba każdorazowo analizować, jak wskazano wcześniej.

• REALIZACJA UPRAWNIEŃ PODMIOTÓW DANYCH

Należy rozważyć, jakie prawa wymagane w art. 15–22 RODO jesteśmy w stanie zrealizować wobec osób objętych monitoringiem. Nie wszystkie systemy umożliwiają np. anonimizację, tym samym mogą wystąpić problemy z udzielaniem dostępu do danych osób (kopii danych), których te dane dotyczą. Trudno bowiem wydać kopię danych (wizerunku) osobie, na której będą również dane innych osób. Realizacja uprawnień osoby obserwowanej niejednokrotnie wiąże się z wymogiem przedstawienia przez

UWAGA: piktogramy „UWAGA! TEREN MONITOROWANY" nie są wystarczające.
Niewłaściwe są również oznaczenia w postaci:

Źródło: opracowanie Piotr Powązka

Obowiązek informacyjny o obecności kamer należy realizować w sposób warstwowy: trzeba wydzielić zakres kluczowych informacji i udostępnić je, przekazując maks. ilość najważniejszych informacji

nią informacji o sytuacjach, w których mogła znaleźć się w obszarze działania systemu monitoringu. Na ogół mówimy o prawie dostępu do danych, żądaniu usunięcia danych, prawie do sprzeciwu.

• NARUSZENIA OCHRONY DANYCH I NOTYFIKACJA

Wymagania w tym zakresie wskazano w art. 33 i art. 34 RODO. W jaki sposób określimy czas przechowywania nagrań (deklarowany)? W jaki sposób należy go skonfigurować, biorąc pod uwagę nadpisywanie starszych nagrań, gdy brakuje miejsca na nagrania? Uwzględniając przepisy art. 32 ust. 1 lit. c) RODO „zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego", jakie są procedury w przypadku awarii nośnika danych? To tylko niektóre pytania i problemy do rozważenia.

• ANALIZA RYZYKA I DPIA

Administratorzy mają do spełnienia szereg obowiązków w zakresie RODO. Jednym z nich jest analiza ryzyka (art. 24 i art. 32 RODO), w tym tzw. DPIA (Ocena Skutków dla Ochrony Danych). Warto podkreślić, że mówimy o ryzyku naruszenia praw i wolności osób fizycznych. Nie sposób pominąć też zagrożeń i ryzyka dla organizacji. Jeżeli dana metoda przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele może z dużym prawdopodobieństwem powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (DPIA) oraz konsultuje się z inspektorem ochrony danych (jeżeli został wyznaczony). Ocena taka jest obligatoryjna:

- jeżeli systematyczna, kompleksowa ocena czynników osobowych odnoszących się do osób fizycznych opiera się na zautomatyzowanym przetwarzaniu (w tym profilowaniu) i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną,
- w przypadku przetwarzania na dużą skalę danych, o których mowa w art. 9 lub art. 10 RODO,
- w przypadku systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie,
- UODO wydaje też wykaz operacji, które wymagają DPIA. Ostatni ukazał się w lipcu 2019 r.

• Systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdą się w monitorowanej przestrzeni.

Do tej grupy nie zalicza się systemów monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku konieczności analizy incydentów naruszenia prawa. Firma projektująca system monitoringu wizyjnego może wesprzeć administratora w tej kwestii, nawet gdy obowiązek spoczywa na samym administratorze danych osobowych.

• MONITORING – REJESTROWANIE A PODGLĄD

Jeżeli kamera monitoringu służy jedynie do podglądu danej sceny (danego obszaru), a nagranie nie jest rejestrowane na dysku twardym czy innym nośniku,

wówczas trudno mówić o przetwarzaniu danych osobowych. Z danymi osobowymi mamy do czynienia wówczas, gdy obraz z kamery zawiera wizerunki osób i został utrwalony w systemie monitoringu na nośnikach danych. Już samo gromadzenie, a nie tylko identyfikowanie osób, jest przetwarzaniem. Zatem systemy wizyjne umożliwiające podgląd „na żywo" wyłącznie na zasadzie wizjera nie podlegają reżimowi RODO.

• PRZEPISY A MONITORING MIEJSC

Nie ma jednolitych przepisów regulujących kwestie podejścia do monitoringu wizyjnego. Należy rozważyć nie tylko przepisy RODO, ale także regulacje branżowe, m.in.:

a) Kodeks Pracy:
- pracodawca może stosować monitoring wizyjny, gdy jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia bądź kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę;

b) ustawa z 8 marca 1990 r. o samorządzie gminnym, ustawę z 5 czerwca 1998 r. o samorządzie powiatowym:
- zapewnienie porządku publicznego i bezpieczeństwa obywateli;
- zapewnienie ochrony przeciwpożarowej i przeciwpowodziowej;
- zapewnienie ochrony mienia komunalnego;

c) ustawa z 5 czerwca 1998 r. o samorządzie województwa
- zapewnienie ochrony mienia województwa;

d) ustawa z 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym:
- zapewnienie ochrony mienia państwowego.

Zasadniczo monitoringiem wizyjnym nie obejmuje się pomieszczeń udostępnianych zakładowej organizacji związkowej, pomieszczeń sanitarnych, szatni, przebieralni, sali do zajęć dydaktycznych czy wychowawczych i opiekuńczych, sali pomocy psychologicznej i pedagogicznej, stołówek oraz palarni, pomieszczeń przeznaczonych do odpoczynku i rekreacji pracowników, pomieszczeń sanitarno-higienicznych, gabinetu profilaktyki zdrowotnej. Nie powinien on stanowić środka nadzoru nad jakością pracy wykonywanej przez pracowników. Kamer nie stosujemy tam, gdzie możliwy jest inny nadzór.

• PRZEPISY A MONITORING UKRYTY I DŹWIĘK

Nie stosujemy ukrytych kamer i nagrywania dźwięku. W zakresie swoich kompetencji tylko uprawnione służby mogą rejestrować również dźwięk.
Są wyjątki przy stosowaniu nagrywania dźwięku, jednak należy je konsultować ze specjalistami i mieć podstawy prawne (np. ustawa o grach hazardowych). Warto odnotować wyrok Wielkiej Izby Europejskiego Trybunału Praw Człowieka (ETPC) z 17 października 2019 r. w sprawie Lopez i inni przeciwko Hiszpanii dotyczący ukrytych kamer. Pracownicy w sposób zorganizowany okradali pracodawcę (hiszpański supermarket). Hiszpański pracodawca zastosował ukryte kamery, gdy zorientował się, jak duża jest skala kradzieży. Nagrania stanowiły dowód w sprawie o bezpodstawne rozwiązanie umowy o pracę. Zwolnieni pracownicy złożyli pozew ze względu na zastosowanie ukrytego monitoringu. W tym jednak przypadku interes pracodawcy okazał się ważniejszy niż prawo do prywatności, choć ETPC częściej opowiadała się po stronie pracowników. Wcześniej ETPC była zdecydowanie przeciwna takim formom nadzoru. W każdej takiej sprawie proporcjonalność środków dozoru bada się odrębnie. Ostrzegam zatem przed pochopnym podejmowaniem decyzji w zakresie stosowania takiego monitoringu u pracodawców.

• STOSOWANIE ATRAP

Stanowisko Prezesa UODO jest w tej kwestii niezmienne – stosowanie atrap kamer powinno być zakazane. Z jednej strony wprowadzają one u potencjalnie monitorowanych poczucie ingerencji w sferę prywatności, z drugiej – dają mylne wrażenie większego bezpieczeństwa.

• UWZGLĘDNIENIE OCHRONY DANYCH OSOBOWYCH W FAZIE PROJEKTOWANIA (PRIVACY BY DESIGN ORAZ PRIVACY BY DEFAULT)

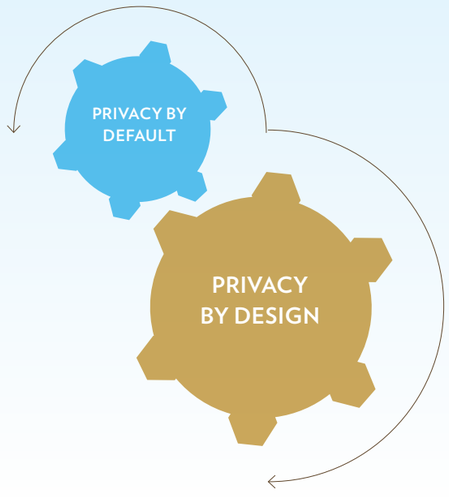
Domyślne projektowanie prywatności idzie w parze z szacowaniem ryzyka, o którym wspomniano wcześniej. RODO nie odnosi się wprost do procesu zarządzania ryzykiem i nie wskazuje konkretnej metody przeprowadzania oceny w tym zakresie.

Odnosząc te zasady do kontekstu monitoringu wizyjnego, należy uwzględnić stosowane rozwiązania techniczne zarówno sprzętowe, jak i oprogramowania, np. maskowanie obiektów (statyczne i dynamiczne), pikselizacja wykorzystywana do anonimizacji, zawężanie obszarów, selektywne wybory śledzonego obiektu – kamery śledzące czy wykrywające ruch, rozpoznające nietypowe zachowania w monitorowanym obszarze, zabezpieczenia oraz kontrola dostępu osób postronnych, kontrola dostępu do oprogramowania i funkcjonalności (np. identyfikacja na podstawie cech biometrycznych), termowizja, sposoby montażu itp. (stołówka, prywatna posesja i dom sąsiada). Wiele systemów może nie spełniać tych wymagań. Należy również pamiętać, iż systemy nagłośnieniowe powiązane z systemem monitoringu wizyjnego mają mikrofon służący do kalibracji tych urządzeń. Zatem istnieje ryzyko nieautoryzowanego podsłuchiwania.

Jak zatem mają postępować organizacje?

Niektóre kraje, np. Francja, rozważają zastosowanie algorytmów rozpoznawania twarzy. Z tego względu zainteresowanie organów nadzorczych, w tym Europejskiego Inspektora Ochrony Danych, systemami monitoringu wizyjnego rośnie. Należy zatem indywidualnie analizować przypadki, by rozwiązania mające służyć ochronie mienia i naszego bezpieczeństwa starać się godzić z prawem do prywatności, również projektując system dla osób prywatnych. Warto, aby temu zagadnieniu poświęcili nieco czasu zarówno administratorzy danych, jak i firmy profesjonalnie projektujące tego typu rozwiązania dla administratorów danych osobowych. Może się np. okazać, iż zleceniodawca będzie chciał przenieść ryzyko zgodności z wymogami prawa – w sposób umowny – na wykonawcę. Można to jednak rozpatrywać raczej jako formę możliwości zbudowania wartości dodanej do realizowanej usługi, pomagając klientowi postępować zgodnie z regulacjami. □

ERATRUST
ul. Postępu 10/34, 02-676 Warszawa
biuro@eratrust.pl



Ustawienia domyślne danego systemu powinny przewidywać możliwe najdalej posunięte zabezpieczenia danych osobowych. Ustawienia aplikacji czy serwisów społecznościowych domyślne powinny udostępniać minimalną ilość informacji o użytkowiku.

Już podczas projektowania systemu ochrony danych osobowych należy wdrażać takie środki, by od początku chronić przetwarzane dane oraz prywatność osób, których one dotyczą.

Źródło: opracowanie Piotr Powązka

BIO

Piotr Powązka

Absolwent Uniwersytetu Ekonomicznego we Wrocławiu. Posiada kilkunastoletnie doświadczenie korporacyjne w sektorach finansowym i technologicznym.
Zaangażowany w przekształcanie prywatności i praktyk handlowych poprzez budowanie zrównoważonej wartości biznesowej, propaguje nowe standardy w umowach oraz kulturę ery zaufania i współpracy. Promuje strategiczne zmiany w sposobie prowadzenia biznesu i zarządzania relacjami. Wspiera organizacje w zakresie transformacji cyfrowej, ochrony danych osobowych i prywatności, zarządzania kontraktami, zgodności i kontroli wewnętrznej oraz modelowania procesów biznesowych.
Jego publikacje obejmowały takie obszary, jak ceny transferowe, kryptowaluty, *smart contracts*, ochrona danych osobowych czy zarządzanie umowami *(contract management)*.
Członek the International Association of Privacy Professionals (IAPP) oraz Członek Rady the International Association for Contract & Commercial Management.

Ewakuacja z obiektów hotelowych

Rola dźwiękowego systemu ostrzegawczego (DSO) i oznakowania dróg ewakuacyjnych

LICZBA HOTELI W POLSCE Z ROKU NA ROK ROŚNIE. HOTELE SĄ ZALICZANE DO OBIEKTÓW SZCZEGÓLNIE NARAŻONYCH NA WYSTĘPOWANIE POŻARU. PRZEPISY W ZAKRESIE ZABEZPIECZANIA PPOŻ. SĄ ZAOSTRZANE, A MIMO TO LICZBA POŻARÓW W TYCH OBIEKTACH ROŚNIE.

T E K S T
Monika Kołodziejczyk

Zapewnienie bezpieczeństwa osób przebywających w obiektach hotelowych wymaga specjalnego podejścia na wszystkich etapach – opracowania koncepcji ochrony, przygotowania instrukcji bezpieczeństwa, doboru urządzeń ppoż. i oznakowania dróg ewakuacji. Wszystkie te elementy powinny uwzględniać sposób funkcjonowania obiektu w jego normalnych warunkach oraz fakt, że przebywają tu osoby, które na co dzień nie są jego stałymi użytkownikami. Goście mają różne cele podróży – biznesowe lub turystyczne, mogą w hotelu spędzić jedną noc albo przebywać w nim tydzień lub dłużej. Czasami są tylko uczestnikami konferencji lub innych imprez organizowanych w hotelu. Cechą wspólną wszystkich gości jest to, że z reguły nie są zaznajomieni z ciągami komunikacyjnymi i procedurami ewakuacyjnymi hotelu, a tym bardziej z układem dróg ewakuacyjnych. W momencie wybuchu pożaru osoby mogą spać, co stanowi duże utrudnienie dla sprawnie przeprowadzonej ewakuacji.

Zadaniem personelu hotelowego jest zadbanie o to, aby wszyscy użytkownicy zostali skutecznie poinformowani o alarmie, oraz zapewnienie odpowiednich warunków ewakuacji, by szybko i bezpiecznie opuścili strefę zagrożoną lub objętą pożarem. Do alarmowania i ewakuacji osób w obiektach hotelowych są wykorzystywane systemy sygnalizacji pożarowej i dźwiękowe systemy ostrzegawcze. Przepisy określają, które obiekty hotelowe podlegają obowiązkowi ich instalacji:

- systemy sygnalizacji pożarowej należy stosować w obiektach hotelowych powyżej 50 miejsc noclegowych (§ 28.1 Rozporządzenia MSWiA z 7 czerwca 2010 r. w sprawie ochrony ppoż. budynków, innych obiektów budowlanych i terenów – Dz.U. 2010, nr 109, poz. 719);
- zgodnie z § 29.1 cytowanego rozporządzenia w obiektach hotelowych, w których liczba miejsc noclegowych przekracza 200 lub budynek jest zaklasyfikowany jako wysoki lub wysokościowy (powyżej 25 m) albo ma więcej niż 9 kondygnacji naziemnych – należy stosować dźwiękowe systemy ostrzegawcze. [1]

W hotelach poniżej 200 miejsc noclegowych do powiadomienia o pożarze stosuje się przede wszystkim sygnalizatory akustyczne lub akustyczno-głosowe uzupełniane o sygnalizatory optyczne. Te ostatnie stosuje się w obszarach, w których mogą przebywać osoby niesłyszące lub niedosłyszące, a także w pomieszczeniach, w których ze względu na sposób użytkowania sygnalizatory akustyczne byłyby nieskuteczne. Można w tym celu zastosować np. specjalne poduszki wibracyjne, uaktywniane w momencie ogłoszenia alarmu, które obudzą osobę znajdującą się w miejscu zagrożenia. Sygnalizatory akustyczno-głosowe mogą dodatkowo wspierać ewakuację dzięki wgranym komunikatom ewakuacyjnym. Wszystkie urządzenia ppoż. muszą działać zgodnie z opracowanym scenariuszem pożarowym. Obsługa hotelu musi go znać, podobnie jak cały obiekt i drogi ewakuacyjne.

Niedoceniona rola DSO

W obiektach hotelowych powyżej 200 miejsc noclegowych wymagany jest dźwiękowy system ostrzegawczy (DSO). Jego zadaniem jest m.in. zapewnienie możliwości rozgłaszania sygnałów ostrzegawczych i komunikatów głosowych. System ten odgrywa bardzo ważną rolę w procesie alarmowania ludzi o zagrożeniu (nie tylko pożarowym) i procesie ewakuacji. Właściwe informacje przekazywane w komunikatach decydują o prawidłowym zachowaniu się osób przebywających w obiekcie. Komunikaty muszą zawierać istotne wytyczne, wskazujące konkretne postępowanie. Pozwala to uniknąć paniki i niepożądanych reakcji, a tym samym usprawnia i przyśpiesza ewakuację.
Klasycznym przykładem może być komunikat informujący, żeby nie kierować się do wind, ponieważ w trakcie pożaru są wyłączone (większość gości hotelowych po usłyszeniu alarmu w pierwszym odruchu kieruje się właśnie do windy). Przykłady można by mnożyć. Najważniejsze jednak, aby komunikat był zrozumiały, zwięzły, jasny i dostosowany dla konkretnej lokalizacji.
Dźwiękowe systemy ostrzegawcze umożliwiają przekazywanie komunikatów zarówno na żywo, przez ratowników przeprowadzających akcję ratunkową (lub inną wyznaczoną osobę), jak i gotowych komunikatów, nagrywanych w pamięci centrali DSO. Które z komunikatów alarmowych przedstawionych w tabeli są bardziej odpowiednie? Z badań wynika jednoznacznie, że ludzie reagują najszybciej, gdy słyszą komunikaty alarmowe nadawane na żywo. Czas reakcji na sygnały nadawane dźwiękowo lub na komunikaty automatyczne jest zbliżony.

Tabela 1. Czas reakcji ludzi w zależności od rodzaju ostrzeżenia [2]

Rodzaj obiektu budowlanego	Czas reakcji		
	na sygnał dźwiękowy	na nagrany komunikat głosowy	na komunikat głosowy nadawany na żywo
Hotele: budynki zamieszkania zbiorowego (ludzie przeważnie niezaznajomieni z obiektem)	>4 min	4 min	<2 min

W opinii ekspertów stosowanie DSO, szczególnie w dużych obiektach (w tym hotelowych), wpływa pozytywnie na skrócenie czasu ewakuacji ludzi z zagrożonej strefy pożarowej, a także umożliwia poinformowanie osób przebywających w innych strefach o tym, co powinni robić. Potwierdzają to również wyniki badań ankietowych:

- w ocenie 91% badanych DSO usprawnia proces ewakuacji z obiektu budowlanego podczas pożaru lub innego zagrożenia,
- 89% ankietowanych przyznaje, że zastosowanie DSO znacznie skraca czas ewakuacji.

Co ciekawe, zdaniem większości respondentów (76%) dźwiękowe systemy ostrzegawcze nie są właściwie wykorzystywane podczas akcji ratowniczych. Czynnikami, które mogą na to wpływać, są głównie:

- brak zaufania do systemu ze strony użytkowników (np. komunikaty automatyczne głosowe nie są traktowane poważnie),
- nieznajomość obsługi systemu przez osoby odpowiedzialne za ewakuację,
- niska zrozumiałość mowy DSO,
- słaba dostępność i słabe oznaczenie mikrofonu strażaka,
- brak zaufania do systemu ze strony obsługi (strażaka),
- brak cyklicznych ćwiczeń,
- uszkodzenia systemu (fałszywe alarmy),
- panika użytkowników obiektu podczas alarmu. [3]

Najczęściej w trakcie ewakuacji z obiektów (nie tylko hotelowych) korzysta się z komunikatów alarmowych automatycznych, mimo że ewakuacja prowadzona przez służby ratownicze jest szybsza – strażacy najczęściej nie mają możliwości użycia mikrofonu strażaka, by przekazać komunikaty na żywo. Obiekt zazwyczaj musi zostać opuszczony przez wszystkich użytkowników, nawet tych, którzy nie są narażeni na bezpośrednie oddziaływanie pożaru. [3]

Scenariusz ewakuacji i instrukcje bezpieczeństwa

Zapanowanie nad zachowaniem ludzi, zwłaszcza w momencie zagrożenia ich życia, jest bardzo trudne, ale możliwe, o ile został przyjęty optymalny scenariusz zadziałania urządzeń przeciwpożarowych.

Przyjęte zasady mają wskazywać osobom przebywającym w hotelu bezpieczną drogę ewakuacji. Kluczową rolę odgrywa również współdziałanie systemów sygnalizacji pożarowej, DSO, systemów wentylacji pożarowej oraz stałych urządzeń gaśniczych. Nie ma gotowych scenariuszy pożarowych. Są one specyficzne dla każdego obiektu i powinny stanowić element instrukcji bezpieczeństwa pożarowego w tym obiekcie. Istotnym zadaniem takiej instrukcji jest zapoznanie personelu z:

- warunkami ochrony ppoż. w obiekcie, sposobami działania urządzeń ppoż.,
- obsługą oraz zasadami postępowania w przypadku ogłoszenia ewakuacji,
- drogami ewakuacyjnymi, kierunkami ewakuacji, lokalizacją wyjść ewakuacyjnych.

Bardzo pomocne są również ewakuacje próbne, które powinno się przeprowadzać co najmniej raz w roku. Pozwalają one sprawdzić w praktyce scenariusz i instrukcję bez obciążania stresem, który w przypadku realnego zagrożenia ma wpływ na sprawność ewakuacji. Ewakuacje próbne raz w roku mogą nie być wystarczające chociażby ze względu na rotujący personel hotelowy.

Oznakowanie dróg ewakuacyjnych

Drogi ewakuacyjne, urządzenia sygnalizacji pożarowej, sprzęt pożarniczy i do ręcznego sterowania oraz środki ograniczające rozwój pożaru wymagają odpowiedniego sposobu znakowania oraz rozmieszczenia znaków bezpieczeństwa. Na drogach ewakuacji największą trudność w dotarciu do bezpiecznej strefy może stanowić zadymienie, które znacznie utrudnia (a czasem wręcz uniemożliwia) szybkie opuszczenie budynku. Dobre oznakowanie może być kluczem w odnalezieniu bezpiecznej drogi ewakuacyjnej. O właściwym kierunku drogi ewakuacyjnej informują użytkowników budynku odpowiednie znaki ewakuacyjne. Aby spełniały one swoją funkcję, muszą być jednoznaczne, rozmieszczone w sposób umożliwiający ich poprawny odczyt oraz stosowane zgodnie z obowiązującymi wymaganiami. Można się spotkać z następującymi oznakowaniami:

ZNAK BEZPIECZEŃSTWA – ogólny komunikat bezpieczeństwa uzyskany przez połączenie koloru i kształtu geometrycznego, który poprzez dodanie symbolu graficznego nadaje szczególnego znaczenia komunikatowi bezpieczeństwa (tł. ISO 7010:2011),

ZNAK DODATKOWY – uzupełnia inny znak; jego głównym celem jest zapewnienie dodatkowego wyjaśnienia (tł. ISO 7010:2011),

DROGA EWAKUACYJNA – cały odcinek drogi poziomej i pionowej do przebycia z dowolnego punktu budynku do wyjścia na otwartą przestrzeń lub do innej (bezpiecznej). Należy dokonać analizy danego obiektu, określając liczbę użytkowników oraz stopień zagrożenia. [5]

Przy obecnym stanie formalnoprawnym możliwe jest zastosowanie znaków bezpieczeństwa zgodnych z normą:
- PN-N-01256-01 (znaki – ochrona przeciwpożarowa),
- PN-N01256-02 (znaki – ewakuacja) ,
- PN EN-ISO 7010 (znaki – ochrona przeciwpożarowa, znaki – ewakuacja). [4]

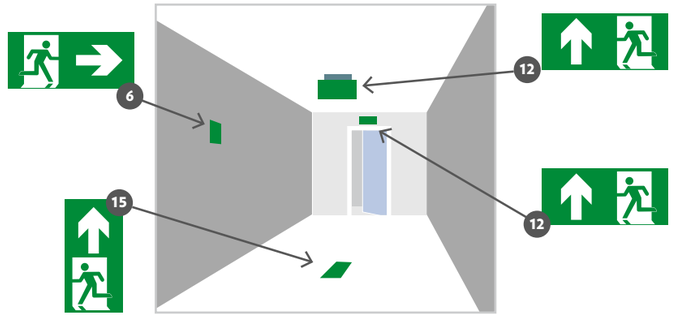
Obiekty hotelowe często są odwiedzane przez obcokrajowców, w związku z tym rekomenduje się stosowanie znaków bezpieczeństwa wg normy międzynarodowej PN-EN ISO 7010. Ich przesłanie jest bardziej zrozumiałe dla cudzoziemców i lepiej spełniają swoje funkcje w przypadku wystąpienia zagrożenia w obiekcie. Znaki na drogach ewakuacyjnych muszą być widoczne z każdego miejsca, w którym może zajść niejednoznaczność co do kierunku przebiegu drogi ewakuacyjnej.
Rozmieszczając znaki ewakuacyjne, należy zwrócić uwagę na pobliskie źródła światła. W miejscach, gdzie występuje oświetlenie dzienne bądź sztuczne, stosujemy znaki wykonane z materiałów fotoluminescencyjnych. Natomiast znaki podświetlane można stosować wszędzie tam, gdzie nie ma oświetlenia dziennego lub sztucznego oraz gdy oświetlenie sztuczne nie gwarantuje znakom niezbędnej energii świetlnej przez wymagany czas. Zależność między wymiarami znaków bezpieczeństwa a odległością obserwacji – największą odległością, z której znak bezpieczeństwa jest widoczny – wyraża się następującym wzorem:

$$h = l/Z \quad [1]$$

gdzie:
h – wysokość znaku,
l – odległość obserwacji,
Z – współczynnik odległości ($Z = 1/\tan_{\omega}$)

Wartości h i l są podawane w jednakowych jednostkach. [5]

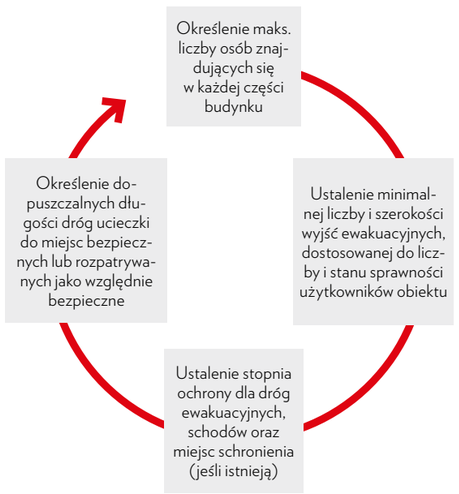
Zasadnicze wytyczne dotyczące rozmieszczania znaków zostały przedstawione w normach BS 5499-4:2013 oraz ISO 16069:2017.
W pomieszczeniu przedstawionym na rys. 1 zastosowano trzy znaki o różnych grafikach (różnej konfiguracji „człowiek – strzałka"), wskazujących ten sam kierunek ewakuacji (wiersze 6, 12 i 15). Ten sam znak (o tej samej grafice i układzie) może podawać, w zależności od sposobu jego rozmieszczenia, odmienną informację o kierunku ewakuacji.
Oto kilka ogólnych zasad i wskazówek dotyczących umiejscowienia znaków ewakuacyjnych wprowadzonych normą BS 5499-4 w obiektach:
- z dowolnego miejsca w każdym pomieszczeniu powinna być widoczna co najmniej jedna droga ewakuacyjna lub przejście prowadzące do drogi ewakuacyjnej: jeżeli droga ta nie jest widoczna lub użytkownik obiektu może zostać wprowadzony w błąd, trasa powinna być oznaczona znakiem;
- w miejscu, w którym bezpośredni widok drogi ewakuacyjnej lub znaku wskazującego drogę ewakuacyjną jest zasłonięty, należy umieścić jeden lub więcej znaków pośrednich;
- drzwi lub przejścia, które można mylić z drogami prowadzącymi do wyznaczonej drogi ewakuacyjnej, powinny być wyraźnie oznaczone;
- znaki dróg ewakuacyjnych powinny mieć pierwszeństwo przed wszystkimi innymi znakami;
- wszelkie zmiany kierunku w korytarzach, na schodach i otwartych przestrzeniach stanowiących część drogi ewakuacyjnej powinny być oznaczone znakami pośrednimi;
- każde drzwi przejściowe lub skrzyżowanie powinny być podobnie oznakowane;
- jeżeli linia widoczności do następnego znaku przekroczyłaby zalecaną maksymalną odległość widzenia dla wybranego rozmiaru znaku, należy umieścić dodatkowe znaki;
- każda wyznaczona droga ewakuacyjna powinna prowadzić do bezpiecznej lokalizacji. [5] □



Rys. 1. Przykład oznakowania drogi ewakuacyjnej korytarz [5]

Komunikat nadawany przez DSO musi być zrozumiały, zwięzły, jasny i dostosowany do konkretnej lokalizacji

Podstawowe zasady określenia warunków ewakuacji



Określenie innych niezbędnych środków dla zapewnienia bezpiecznej ewakuacji:
- wykrycie pożaru,
- zaalarmowanie użytkowników,
- zabezpieczenie przed zadymieniem,
- oświetlenie ewakuacyjne,
- znaki bezpieczeństwa,
- wysterowanie kontroli dostępu.

BIO

Monika Kołodziejczyk

Z branżą zabezpieczeń związana od 2000 r. Obecnie prezes firmy C-AIM. Ma bogate doświadczenie w zakresie projektowania i wdrażania rozwiązań z zakresu systemów sygnalizacji pożarowej.

Źródło:

[1] Rozporządzenia MSWiA z 7 czerwca 2010 r. w sprawie ochrony ppoż. budynków, innych obiektów budowlanych i terenów (Dz.U. 2010, nr 109, poz. 719).
[2] Elektroakustische Alarmierungseinrichtungen – Erläuterungen und Ergänzungen zu Normen, rechtlichen Grundlagen und technischen Regeln, ZVEI, 2010, s. 12.
[3] T. Popielarczyk: Ewakuacja ludzi w wykorzystaniem dźwiękowych systemów ewakuacyjnych. Wyd. CNBOP-PIB
[4] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 27 kwietnia 2010 r. zmieniającego rozporządzenie w sprawie wykazu wyrobów służących zapewnieniu bezpieczeństwa publicznego lub ochronie zdrowia i życia oraz mienia, a także zasad wydawania dopuszczenia tych wyrobów do użytkowania (Dz.U. nr 143, poz. 1002 z późn. zm.)
[5] Wytyczne CNBOP-PIB W-0005:2019 „Stosowanie znaków bezpieczeństwa zgodnych z normą PN-EN-ISO 7010"

Systemy bezpieczeństwa pożarowego znajdujące się w ofercie Schrack Seconet Polska Sp. z o.o., do których należy m.in. dźwiękowy system ostrzegawczy (DSO) APS®-APROSYS produkowany przez g+m elektronik ag, dają wiele możliwości w zakresie stosowania rozwiązań zwiększających poziom bezpieczeństwa w obiekcie, a także pozwalają na podniesienie komfortu obsługi. W niniejszym artykule zostaną opisane wybrane funkcje, których cechą wspólną jest optymalizacja zasobów systemowych i innowacyjność w podejściu do bezpieczeństwa obiektu budowlanego.

ROZWIĄZANIA SPECJALNE W INSTALACJACH DSO NA PRZYKŁADZIE APS®-APROSYS

TEKST
Rafał Kowal
Schrack Seconet Polska

Rozwiązania te dotyczą elementów wykonawczych systemu DSO (jakimi są np. wzmacniacze mocy czy linie głośnikowe rozprowadzone w obiekcie) oraz specjalnych cech funkcjonalnych systemu, m.in. związanych ze współdziałaniem z systemem integrującym urządzenia przeciwpożarowe SIS-FIRE. Umożliwiają również integrację z systemem budynkowym BMS, wykorzystywanym np. do celów komercyjnych, niezwiązanych z alarmowaniem.

Do takich funkcji specjalnych należą sposoby i możliwości rozgłaszania komunikatów „na żywo" w sytuacjach szczególnych zagrożeń mogących wystąpić w obiektach, takich jak akty terroryzmu, anomalne zachowania osób przebywających w obiekcie, wtargnięcia osób nieuprawionych do stref chronionych itp. Poniżej przedstawiono przykłady zastosowań specjalnych z wykorzystaniem systemu APS®-APROSYS.

Pierwsza funkcja dotyczy efektywnego (optymalnego) wykorzystania mocy wzmacniaczy systemowych. W oferowanych na rynku rozwiązaniach mamy do czynienia z systemami, w których występują ograniczenia liczby linii głośnikowych lub stref nagłośnieniowych obsługiwanych przez pojedynczą końcówkę mocy wzmacniacza operacyjnego. Skutkuje to często przewymiarowaniem systemu – dostarczana przez wzmacniacze moc jest dużo większa niż faktycznie wymagana do nagłośnienia stref. W projektach występują większe rezerwy mocy, które w przyszłości nie będą wykorzystywane, np. zapotrzebowanie mocy na klatkach schodowych – brak możliwości zmian architektonicznych czy aranżacji w tego typu przestrzeniach, jak ma to miejsce np. w przestrzeniach biurowych.

System APS®-APROSYS, wykorzystując kontrolery linii głośnikowych z selektorami stref APS-178.1-XX-EV, pozwala na uniknięcie takiego przewymiarowania systemu w zakresie liczby i mocy sumarycznej wzmacniaczy w stosunku do faktycznego zapotrzebowania wynikającego z bilansu mocy linii głośnikowych. Nie ma ograniczeń co do liczby obsługiwanych linii głośnikowych przez pojedynczą końcówkę wzmacniacza. Takie rozwiązanie przekłada się na aspekt ekonomiczny wynikający z finalnego zapotrzebowania mocy elektrycznej, jaką musimy dostarczyć do systemu.

Z kolei gdy wymagane jest zastosowanie rozwiązania pozwalającego na zwiększenie bezpieczeństwa w zakresie nagłaśnianych przestrzeni, np. na wypadek wystąpienia zwarcia w jednej z dwóch projektowanych linii głośnikowych obsługujących daną przestrzeń, należy wdrożyć rozwiązania specjalne, które umożliwiają spełnienie takich wymagań.

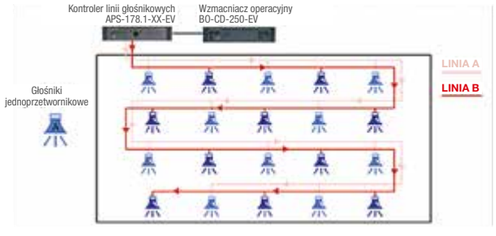
W tradycyjnych rozwiązaniach projektowych w przypadku nagłaśniania stref stosuje się co najmniej po dwie linie głośnikowe (*rys. 1*). To rozwiązanie jest podyktowane wymaganiami normatywnymi, z których wynika, że w przypadku uszkodzenia pojedynczej linii głośnikowej nie powinno dojść do pełnej utraty nagłośnienia w danej strefie, co w przypadku symetrycznego rozmieszczenia głośników będzie skutkowało utratą nagłośnienia na poziomie 50% (*rys. 3*).

Odnośnie do systemu APS®-APROSYS spełnienie powyższych wymagań stawianych przez projektanta czy inwestora nie stanowi problemu dzięki zastosowaniu certyfikowanego modułu pętlowego APS-180-LOOP wraz z dedykowanymi izolatorami zwarć. Zasada jego działania jest zbliżona do działania pętlowych linii dozorowych stosowanych w systemach sygnalizacji pożarowej. W takim przypadku zamiast tradycyjnych linii promieniowych, jak to przedstawiono powyżej, instalowana jest pętla głośnikowa wraz z dwustronnymi izolatorami zwarć, które dodatkowo zabezpieczają instalację głośnikową, zwiększając poziom bezpieczeństwa nagłaśnianych powierzchni.

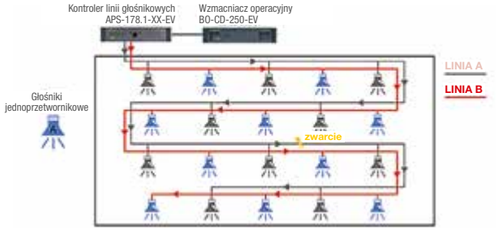
W momencie np. wystąpienia pojedynczego zwarcia w pętli głośnikowej moduł APS-180-LOOP wykrywa ten stan i automatycznie izoluje odcinek pomiędzy izolatorami, na którym powstało to uszkodzenie. Taka funkcjonalność pozwala na zachowanie nawet 100% pracujących głośników pomimo powstałej usterki w pętli głośnikowej (*rys. 4*).

Opisane rozwiązanie z powodzeniem zostało już wdrożone w kilku obiektach w Polsce. Warto też podkreślić, że zostało również docenione przez Kapitułę konkursu MTP podczas Międzynarodowych Targów Zabezpieczeń SECUREX 2018 i nagrodzone złotym medalem (więcej na ten temat można przeczytać na stronie Schrack Seconet Polska: (https://www.schrack-seconet.com/pl/company/news_events/index.html?id=0000020&kind=news).

Kolejnym z rozwiązań specjalnych stosowanym w instalacjach DSO z wykorzystaniem APS®-APROSYS, jest możliwość integracji z systemem sygnalizacji pożarowej Integral IP oraz certyfi-



Rys. 1. Przykład tradycyjnej instalacji DSO z wykorzystaniem linii głośnikowych typu A/B



Rys. 2. Przykład tradycyjnej instalacji DSO z wykorzystaniem linii głośnikowych typu A/B – usterka jednej linii

kowanym systemem integrującym urządzenia przeciwpożarowe (SIUP) SIS-FIRE. W dużych obiektach wyposażonych w bogatą gamę systemów bezpieczeństwa pożarowego możliwość sterowania nadrzędnego oraz monitorowania DSO z poziomu SIUP jest bardzo pomocna, szczególnie w zakresie szybkiego i skutecznego podejmowania decyzji oraz nadrzędnego zarządzania i sterowania w sytuacjach zagrożenia.

System APS®-APROSYS skomunikowany cyfrowo z SIS-FIRE pozwala użytkownikowi na rozgłaszanie komunikatów głosowych w trybie rzeczywistym do wybranych grup lub stref nagłośnieniowych oraz stałe monitorowanie szczegółowych stanów pracy systemu, np. w zakresie stanu zasilania podstawowego, rezerwowego czy połączenia CDSO z pulpitami mikrofonowymi, łącznie z monitorowaniem usterek poszczególnych linii głośnikowych poprowadzonych w obiekcie.

Integracja cyfrowa systemów bezpieczeństwa pożarowego dzięki ścisłemu współdziałaniu zintegrowanych systemów i uzyskaniu dodatkowych ww. funkcji pozwala na zwiększenie komfortu obsługi oraz podwyższenie bezpieczeństwa zabezpieczanego obiektu. Jest to szczególnie polecane przez firmę Schrack Seconet Polska.

Kolejną godną uwagi funkcjonalnością systemu APS®-APROSYS jest możliwość zdalnego rozgłaszania komunikatów głosowych „na żywo” dzięki dedykowanemu modułowi komunikacji z CDSO za pomocą wydzielonego łącza telefonicznego. Przeszkolony personel obiektu w sytuacji specjalnej, nietypowej, ale również wtedy, gdy nie ma możliwości dostępu do pomieszczenia, w którym jest zlokalizowany pulpit mikrofonowy, może z dowolnego miejsca np. przez telefon komórkowy nadać komunikat głosowy do uprzednio zaprogramowanych stref nagłośnieniowych, „dodzwaniając” się do DSO.

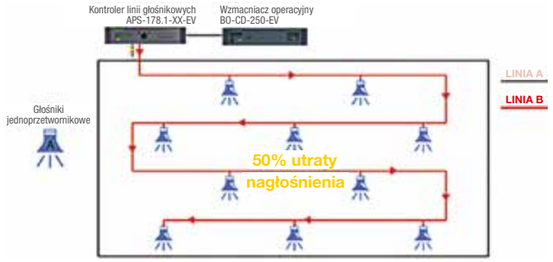
Taka funkcjonalność może być bardzo przydatna do wykorzystania w obiektach strategicznych, takich jak porty lotnicze, dworce kolejowe, obiekty szpitalne lub wszędzie tam, gdzie czasowo może przebywać bardzo duża liczba osób, np. w obiektach widowiskowo-sportowych. W tego typu obiektach mogą wystąpić zagrożenia związane nie tylko z pożarem, ale także aktami wandalizmu, atakami terrorystycznymi lub nieracjonalnym zachowaniem się osób, np. pacjentów izby przyjęć w placówce szpitalnej.

Szczegółowe informacje dotyczące systemu APS®-APROSYS i jego możliwości można uzyskać na stronie internetowej Schrack Seconet (www.schrack-seconet.com) oraz podczas cyklicznie organizowanych szkoleń projektowych dla projektantów dźwiękowych systemów ostrzegawczych.

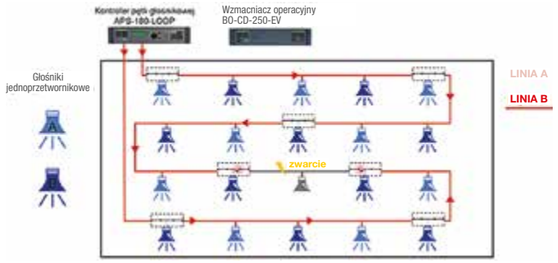
Referencje dotyczące obiektów, w których powyższe rozwiązania zostały już wdrożone, można uzyskać, kontaktując się bezpośrednio z biurem firmy Schrack Seconet Polska. □

Schrack Seconet Polska

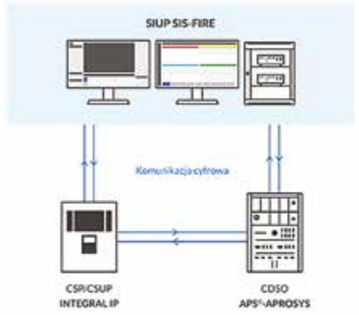
ul. A. Branickiego 15
02-972 Warszawa
www.schrack-seconet.pl



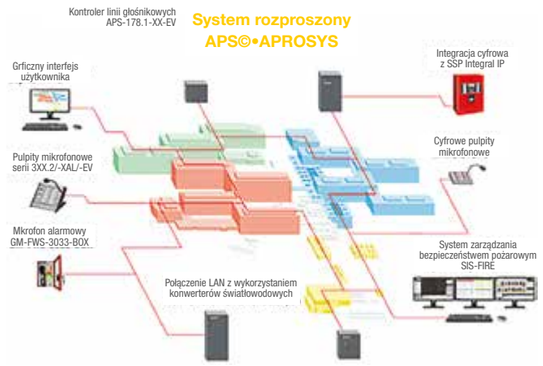
Rys. 3. Przykład tradycyjnej instalacji DSO z wykorzystaniem linii głośnikowych typu A/B – usterka jednej linii



Rys. 4. Przykład instalacji DSO z zastosowaniem pętli głośnikowych z wykorzystaniem modułu APS-180-LOOP i izolatorów zwarć

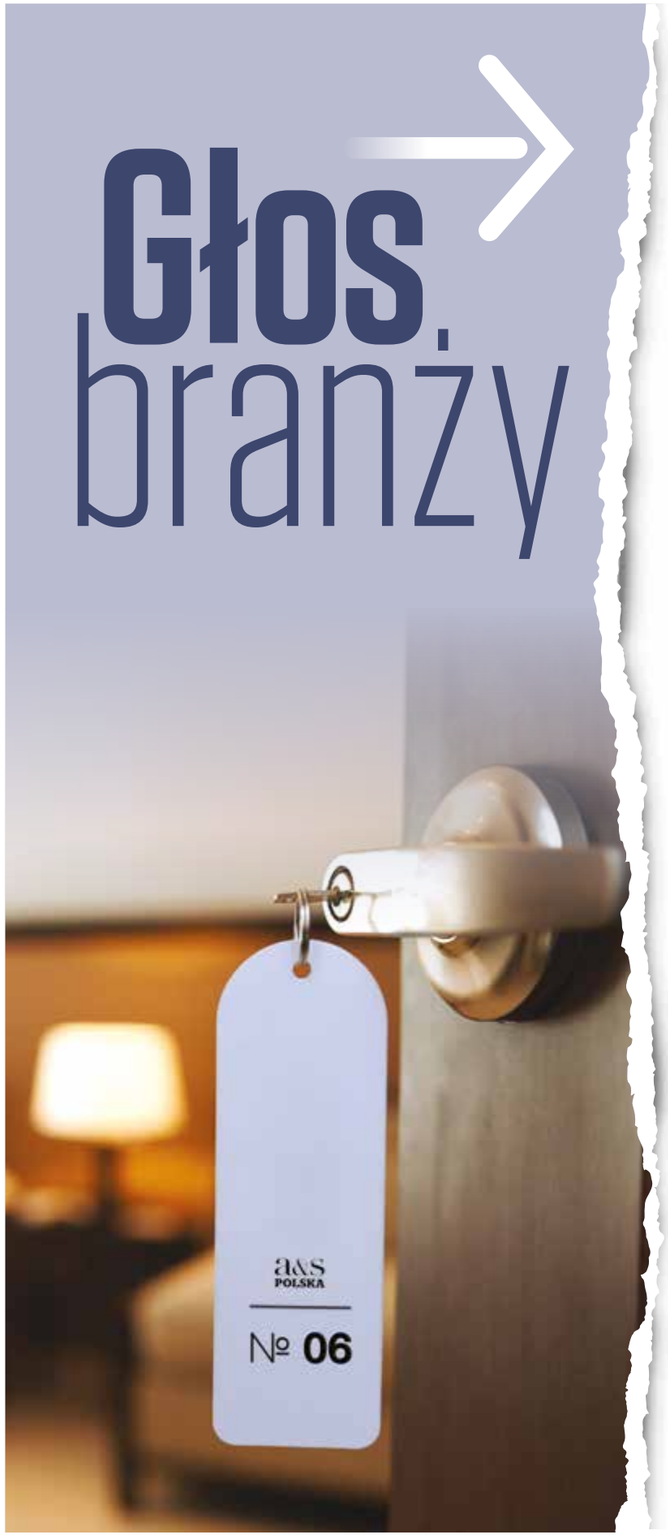


Rys. 5. Integracja cyfrowa DSO z systemem Integral IP oraz SIUP SIS-FIRE



Rys. 6. Przykład budowy systemu APS®-APROSYS w układzie zdecentralizowanym (system rozproszony)

Głos branży



HOTELE I INSTYTUCJE FINANSOWE SĄ OBIEKTAMI WYMAGAJĄCYMI SPECYFICZNEJ OCHRONY. ZARZĄDZAJĄCY NIMI MUSZĄ DBAĆ O BEZPIECZEŃSTWO ZARÓWNO GOŚCI, JAK I PRACOWNIKÓW, UWZGLĘDNIAJĄC PRZY TYM CHARAKTER ICH DZIAŁALNOŚCI. CZEGO OCZEKUJĄ OD BRANŻY SECURITY?

Adam Brzezicki

Inżynier sprzedaży
Axis Communications

Oferta dla hoteli

Każdego dnia hotele obsługują od kilku do kilku tysięcy gości. Zapewnienie im bezpieczeństwa i dbałość o ich komfort jest najwyższym priorytetem i stanowi nie lada wyzwanie. Oferta Axis skierowana do segmentu hoteli zapewnia spełnienie tych wymogów na najwyższym poziomie. Kamery Axis z serii M30 oraz M42 zagwarantują doskonałą jakość obrazu w każdych warunkach oświetleniowych. Kompaktowe wymiary oraz dostępne akcesoria pozwolą zainstalować je w sposób dyskretny.
Aby zwiększyć zadowolenie klientów z obsługi, należy odpowiednio zarządzać personelem hotelu. Można w tym celu wykorzystać oprogramowanie analityczne, np. Axis People Counter, które analizując obrazy z kamer, dostarczy informacji o liczbie osób na danej przestrzeni, lub Axis Queue Monitor, które pozwoli zarządzającemu czy operatorowi zniwelować czas oczekiwania w nielubianych kolejkach.
Odpowiednia muzyka zapewni klimat i atmosferę, w której goście będą czuli się komfortowo. Systemy audio Axis pozwolą centralnie zarządzać dźwiękiem w całym obiekcie, kierując odpowiednie treści w odpowiednie miejsca. Funkcje takie jak harmonogram pracy czy automatyczne testy urządzeń sprawiają, że cały system działa automatycznie i bezobsługowo. Wzmacniacz Axis C8210 pozwala dołączyć do systemu dowolne głośniki pasywne, zachowując wszystkie zalety systemu Axis Audio IP.
Wysoka jakość, długi czas eksploatacji oraz cyberzabezpieczenia w produktach Axis zapewnią nieprzerwaną pracę systemów na długie lata, bezpieczeństwo gości oraz optymalizację pracy całego hotelu.

Marcin Walczuk

Specjalista ds. produktu
BCS

Bezpieczny hotel

Stale rozwijająca się branża hotelarska ze względu na swoją specyfikę musi zwracać szczególną uwagę na zapewnienie możliwie najwyższego poziomu ochrony swoich klientów. Osoby korzystające z usług hotelowych oprócz oczywiście wygody oczekują, że będą czuć się komfortowo i bezpiecznie. Aby spełnić te oczekiwania, w hotelach instaluje się wysokiej klasy systemy zabezpieczeń, począwszy od systemów kontroli dostępu do pokojów gościnnych, systemów przeciwpożarowych, sygnalizacji włamania oraz telewizji dozorowej.
BCS, jako producent urządzeń VSS/CCTV, w swojej ofercie ma pełną gamę urządzeń, które sprawnie i skutecznie mogą zabezpieczyć największy tego typu obiekt. Rejestratory, nawet 128-kanałowe, sprawdzą się w systemie monitoringu średnich hoteli, natomiast przy użyciu aplikacji BCS Manager można połączyć więcej tego typu urządzeń i cały system obsługiwać z poziomu jednej stacji roboczej. W takim przypadku ograniczeniem może być tylko moc tej stacji umożliwiająca wyświetlanie obrazów z odpowiedniej liczby kanałów.
Z kolei doskonałą jakość obrazu zapewnią kamery o rozdzielczości nawet do 12 Mpix. Ze względu na zróżnicowane potrzeby wymagających klientów BCS proponuje rozwiązania, które potrafią spełnić również ich oczekiwania. Kamery specjalnego przeznaczenia, np. z funkcją rozpoznawania i identyfikacji twarzy, umożliwiają porównanie twarzy osób, które znajdą się na terenie hotelu, z bazą danych gości i wychwytywanie osób niepożądanych.
Kamery z funkcją liczenia osób pomogą sprawdzić, czy liczba osób w hotelu odpowiada liczbie osób w nim zameldowanych, a w razie ewakuacji mieć pewność, że wszyscy opuścili budynek. Najnowsza seria kamer BCS AI z zaimplementowanym algorytmem sztucznej inteligencji umożliwi systemowi reagowanie na szczególnego typu zdarzenia, takie jak przekroczenie linii, wtargnięcie lub zbyt długie przebywanie w strefie bądź monitorowanie pozostawionych (skradzionych) przedmiotów.
Z kolei przy monitorowaniu parkingów nieodzowna może się okazać kamera rozpoznająca numery tablic rejestracyjnych, która w połączeniu z aplikacją BCS Manager przyzna dostęp autom o zgłoszonych numerach rejestracyjnych gości hotelowych.

Grzegorz Długosz

Technical Support Engineer
Dahua Technology Poland

Digital Signage

Czasy się zmieniają i wszystko to, co nas otacza, również się zmienia, dostosowuje, poszerza swoją funkcjonalność i otwiera nowe możliwości, które wcześniej oglądaliśmy w filmach science fiction. Nawet nie zauważyliśmy, kiedy technologia Digital Signage wkradła się już w naszą rzeczywistość, statyczne reklamy zaczęły zmieniać się w dynamiczne obrazy wyświetlane na otaczających nas ekranach, a treści tam prezentowane są aktualizowane w czasie rzeczywistym przez centrum zarządzania rodem z filmu „Raport mniejszości". Podobny los czeka interaktywne urządzenia do obsługi klientów, które wnikają obecnie w coraz większy obszar naszego życia.
Możliwość implementacji podobnych rozwiązań ma przed sobą ogromną przyszłość

i dlatego jako częsty gość hoteli chciałem zainspirować potencjalnych projektantów i właścicieli, którzy pragną wzbogacić swoje obiekty hotelowe (i nie tylko), zgodnie z duchem czasów. W sieci już teraz można znaleźć oferty hoteli „bezobsługowych", które są wspaniałą zapowiedzią czekającej nas rzeczywistości. Jeszcze kilka lat temu podobne ciekawostki opierały się mentalności społeczeństwa, teraz są one przyciągającą gości atrakcją.
Wyobraźmy sobie sytuację, że gość wchodzący do hotelu ma wybór – czy będzie obsługiwany przez pracownika recepcji, czy też skorzysta z interaktywnego urządzenia do rejestracji, które pokaże dostępne atrakcje w danym kompleksie, przekaże informacje na temat odbywających się imprez w hotelowym klubie czy promocji na dodatkowy masaż w SPA, jeżeli zamówi pokój o odpowiednim standardzie. Będzie mógł ponadto przejrzeć galerię dostępnych pokoi, a nawet odbyć po nich wirtualny spacer, przejrzeć menu restauracji oraz repertuar pobliskich kin, teatrów, muzeów itp. Całości powinny dopełnić umieszczone w newralgicznych punktach urządzenia typu Digital Signage, które w sposób przyjazny i czytelny będą informować gości hotelowych, w której sali będzie odbywać się konferencja lub szkolenie branżowe, na które przyjechali.
Kluczową kwestią i ogromną zaletą tego typu rozwiązań jest możliwość zdalnego zarządzania wyświetlanymi treściami z jednego miejsca przez administratora systemu. Wyświetlenie nowej promocji w restauracji hotelowej, szybka zmiana szaty graficznej na świąteczną wraz z odpowiednim klimatycznym podkładem – wszystko dostępne zdalnie w przyjaznej dla obsługi platformie połączonej z dedykowaną chmurą.
Powyższe rozwiązania jeszcze kilka lat temu były albo niedostępne albo bardzo drogie w stosunku do swoich możliwości. Dzisiaj dzięki Dahua Technology ograniczenia te nie stanowią już przeszkody, możliwości personalizacji rozwiązań oraz relatywnie niskie koszty w stosunku do dostarczonej przez nie funkcjonalności otwierają nową drogę ku przyszłości.

Jedynym ograniczeniem staje się wyobraźnia projektantów i dizajnerów w kreowaniu przestrzeni hotelowych poprzez technologie przyjazne człowiekowi.

Jakub Sobek

Trener, Inżynier Wsparcia Sprzedaży Linc Polska

Łatwy cel?

Zarówno urządzenia, jak i oprogramowanie podłączone do Internetu każdego dnia są narażone na cyberataki. Osoby przeprowadzające takie ataki w największym stopniu skupiają się na wykorzystaniu najsłabszych punktów danego rozwiązania. Ich intencją jest zdobycie dostępu do krytycznych i wrażliwych danych. Coraz częściej celem ukierunkowanych cyberataków są elementy systemów zabezpieczeń, które już w większości przypadków są podłączone do sieci. Niewiele jest już urządzeń odizolowanych od świata zewnętrznego.
Czy zapewnienie bezpieczeństwa takich systemów musi być drogie? Wiadomo że nikt nie chce zbyt dużo inwestować w zabezpieczenia, jeśli nie musi, tym bardziej że świadomość takiego zagrożenia jest bardzo mała. Niestety często można zauważyć, że inwestorzy poszukujący odpowiedniego rozwiązania wizyjnego nie doceniają znaczenia niezawodności danego systemu. Trzeba pamiętać, że w dzisiejszych czasach nie płacimy tylko za sam produkt, ale także za kompleksową ochronę przed rosnący mi zagrożeniami związanymi m.in. z atakami ze strony międzynarodowych hakerów. Kiedy hakerzy atakują sieć w celu uzyskania dostępu do obrazu na żywo i/lub nagranego na serwerach czy w kamerach, to nie zawsze kamera jest ich jedynym celem.
Zdarza się też, że zdemontowana kamera trafia w niepowołane ręce wraz z kartą pamięci, na której nadal znajdują się niezaszyfrowane nagrania. Atakowane są także słabo zabezpieczone rejestratory wizyjne, które nigdy nie zostały poddane kompleksowym testom bezpieczeństwa. Niewielu producentów może pochwalić się certyfikatami poświadczającymi wysoki poziom zabezpieczeń oferowanych produktów. Do tego dochodzi także kwestia bezpieczeństwa sieci i jej odporność na ewentualne podsłuchiwanie lub manipulacje.
Istotne jest wprowadzanie rozwiązań zapewniających enkrypcję end-to-end, czyli utajnienie danych na wszystkich etapach ich wymiany. Nie można sobie pozwalać na tzw. martwe punkty, ponieważ to właśnie one stają się łatwym celem. Od źródła danych, poprzez sieć, miejsce rejestracji, aż do systemu zarządzania na komputerze użytkownika – wszędzie tam bezpieczeństwo jest istotne i takiej filozofii myślenia o systemach powinniśmy wymagać od producentów i integratorów systemów.

Mariusz Malicki

Polska Izba Hotelarstwa

Ochrona nieletnich

Największym wyzwaniem dotyczącym zapewnienia bezpieczeństwa w hotelach jest moim zdaniem ochrona dzieci i młodzieży do lat 18. Jest to istotne, ponieważ coraz częściej nagłaśniane są przestępstwa i podejrzenia przestępstw na tle seksualnym, których ofiarami padają dzieci i młodzież.
Identyfikowanie dzieci przebywających w obiektach hotelarskich pod opieką dorosłych nie znajduje uzasadnienia w obowiązujących przepisach prawa. Dzieci nie wymagają zameldowania, dlatego też trudno zagwarantować im bezpieczeństwo. Niestety w przypadku braku identyfikacji małoletnich może dojść do sytuacji zagrożenia zdrowia zarówno fizycznego, jak i psychicznego wywołanego przez obcą osobę (chodzi o uprowadzenia, rodzicielskie uprowadzenia, wykorzystywanie nieletnich).
Polska Izba Hotelarstwa już od dłuższego czasu porusza ten temat. Pisaliśmy w tej sprawie do Rzecznika Praw Dziecka. Niestety sprawa jest bardzo złożona. Polska Izba Hotelarstwa na spotkaniach branżowych uczula hotelarzy na takie sytuacje, dlatego moim zdaniem powinniśmy wszyscy wspólnie dążyć do prawnego rozwiązania tak ważnej kwestii.

Grzegorz Wensker

Głowny konstruktor i założyciel firmy Roger

Rola systemów kontroli dostępu w hotelach

Kontrola dostępu w hotelach to w zasadzie obowiązkowy element ich wyposażenia. Elektroniczna kontrola dostępu z oczywistych powodów ułatwia zarządzanie dostępem do pokoi hotelowych oraz innych pomieszczeń, ale nie tylko. Istotną korzyścią płynącą z jej zastosowania jest zwiększenie poziomu bezpieczeństwa gości hotelowych.
Przy stosowaniu tradycyjnego klucza w zasadzie nie było sposobu, aby skutecznie zabezpieczyć się przed jego zduplikowaniem, a w przypadku jego zagubienia wymagane było wymienienie całej wkładki. Wiązało się to z dodatkowymi kosztami, a nawet koniecznością czasowego wyłączenia pokoju z użytkowania.
Bez elektronicznej kontroli dostępu praktycznie nie było też możliwości zabezpieczenia dostępu do przejść wspólnych, a w szczególności wejścia do hotelu. Wszystkie te słabości wynikające z użycia tradycyjnych kluczy mechanicznych może usunąć elektroniczna kontrola dostępu.
Trzeba jednak pamiętać, że nie każdy system kontroli dostępu oferuje odpowiedni poziom bezpieczeństwa. Szczególnie krytycznym elementem, mającym zdecydowany wpływ na poziom bezpieczeństwa, jest użyta w systemie technologia identyfikacji. Dla przykładu popularne karty zbliżeniowe standardu EM 125 kHz dają się klonować sprzętem dostępnym na aukcjach internetowych. Pełną gwarancję zabezpieczenia przed duplikowaniem uzyskuje się, stosując karty z szyfrowaną transmisją danych oraz szyfrowanymi blokami pamięci, np. karty standardu MIFARE® DESFire® oraz MIFARE Plus®. Niestety starsze wersje kart MIFARE® (np. Classic) nie były odpowiednio odporne na ataki hakerskie i ich zabezpieczenia zostały złamane.
Jak się okazuje, użycie odpowiedniego sprzętu i technologii to nie wszystko. W celu zapewnienia odpowiedniego poziomu bezpieczeństwa konieczne jest również właściwe skonfigurowanie systemu i zabezpieczonych haseł do oprogramowania zarządzającego oraz danych na identyfikatorach.
W ofercie firmy Roger znajduje się system kontroli dostępu RACS 5, który z powodzeniem może sprostać oczekiwaniom w zakresie funkcjonalności oraz bezpieczeństwa w małych i średnich hotelach. Dostępna jest ponadto dedykowana seria urządzeń kontroli dostępu i automatyki przeznaczona do integracji z oprogramowaniem zarządzającym hotelem, realizującym zaawansowane funkcje sterowania automatyką pokoju hotelowego.

Marek Malczewski

Bank Millennium, Departament Bezpieczeństwa | Zespół Bezpieczeństwa Korporacyjnego

Ciągłość działania sektora bankowego

Dzisiejsze zagrożenia dla sektora bankowego, mogące zakłócić jego ciągłość działania lub skutkować wysokimi stratami, zmieniły się w stosunku zagrożeń dominujących jeszcze kilka lat temu. Większość z nich nie ma już charakteru fizycznej utraty mienia. W obszarze naszego zainteresowania wciąż pozostaje ochrona kluczowych obiektów i aktywów – infrastruktury, personelu i procesów. Jednak chciałbym zwrócić uwagę na nieco bardziej przyziemne, a często zapominane aspekty.
Jedną z najważniejszych wartości współczesnego przedsiębiorstwa jest informacja. Informacje mogą przyjmować różne formy, od „wiedzy plemiennej", know-how, przez zbiory zer i jedynek składowanych w centrach przetwarzania danych, po fizyczne kopie dokumentów i informacji wyświetlanych na ekranach komputerów.
Dzisiejszy rynek instytucji finansowych

jest ściśle regulowany, również w zakresie ochrony danych, nie tylko osobowych, oraz sankcji grożących za ich wyciek. Zbyt często, rozważając aktywa, które należy zabezpieczyć, wyłączność w ochronie informacji powierzamy jednostkom współcześnie kojarzonym z ich cyfrową postacią. Zabezpieczenie fizycznych kopii dokumentów, bezpiecznego procesu ich niszczenia czy choćby przetwarzania w codziennej pracy również powinno być przedmiotem naszej uwagi.
Warto zadać sobie pytanie, czy aranżacja przestrzeni, w której przetwarzane są dane osobowe lub tajemnice przedsiębiorstwa, sprzyja ochronie tych informacji. Czy pracownicy posiadają należytą wiedzę i zrozumienie wartości informacji, które przetwarzają? Czy zdają sobie sprawę z konsekwencji prawnych, wizerunkowych i biznesowych ich nieświadomego ujawnienia? Czasem zastosowanie prozaicznych środków, takich jak ekranowe filtry prywatyzujące czy sposób aranżacji biurek, który uniemożliwia osobom postronnym obserwację treści wyświetlanych na monitorze, pozwalają zapewnić właściwą ochronę informacji przedsiębiorstwa.
Moje obserwacje wskazują, że wyciek informacji w procesie ich archiwizacji, transportu fizycznych nośników lub ich utylizacji jest dla banków znacznie bardziej kosztowny niż większość incydentów związanych z atakami na aktywa fizyczne.

Kamil Soporek

Security Manager
Krajowa Izba Rozliczeniowa

Cyberbezpieczeństwo w obszarze zabezpieczeń technicznych

Sektor finansowy charakteryzuje się dużą dojrzałością w obszarze bezpieczeństwa informatycznego. Wiąże się to z wysoką świadomością organizacyjną i koniecznością spełniania wymagań wielu standardów bezpieczeństwa, takich jak Rekomendacja D, PCI DSS, SWIFT czy NIST Cybersecurity Framework.
Realizowane cyklicznie skany infrastruktury i prowadzone testy penetracyjne komponentów wskazują jednak na braki ze strony producentów rozwiązań z obszaru zabezpieczeń technicznych. Paradoksalnie więc narzędzia mające zapewnić bezpieczeństwo w wymiarze fizycznym niekiedy generują zagrożenia w środowisku IT. Wykrywane podatności często nie mogą być wyeliminowane na poziomie konfiguracji systemów czy urządzeń, gdyż ich oprogramowanie jest zamknięte, bez realnego wsparcia ze strony developmentu. Deklaracje producentów na temat bezpieczeństwa ich produktów mają głównie charakter marketingowy, a siła ich przekazu słabnie w świetle dowiedzionych nieprawidłowości. Jednocześnie w ostatnich latach wraz z upowszechnieniem kamer IP w monitoringu wizyjnym skala podatnych na ataki systemów diametralnie się zwiększa.
Miejmy świadomość, że każda kamera to komputer podłączony do sieci LAN, zabezpieczony lub wręcz przeciwnie – podatny na ataki. Wystawianie urządzeń tego rodzaju do sieci publicznej skutkowało dotychczas lawinowym wzrostem ich użycia w sieciach botnetowych, takich jak Mirai, które służą m.in. do prowadzonych przez grupy przestępcze ataków DDoS.
Kompensacja podatności jest oczywiście możliwa z zastosowaniem rozwiązań znanych i stosowanych w świecie bezpieczeństwa informatycznego. Izolacja sieciowa środowisk jest realizowana poprzez wydzielanie sieci wirtualnych (VLAN) oraz wykorzystanie reguł firewallowych na urządzeniach brzegowych. Dostęp do zarządzania jest zapewniamy przez systemy *Privilage Account Management* (PAM), a ochrona sieci i hostów – zarówno pasywna w postaci detekcji anomalii w ruchu sieciowym, jak i aktywna z użyciem *Intrusion Prevention System* (IPS) – jest stosowana razem z innymi mechanizmami ochrony.
Ostatecznie jednak całą pracę zabezpieczającą powinno się wykonać u źródła, lecz świadomość producentów w tym zakresie dopiero rośnie. Zadaniem użytkowników jest sygnalizowanie potrzeb. W mojej ocenie motorem rozwoju będzie sektor finansowy stawiający przed producentami i dostawcami rozwiązań zabezpieczeń technicznych najwyższe wymagania.
Wyzwanie stojące przed producentami jest niezwykle istotne, gdyż wyścig z cyberprzestępcami trwa, a przed globalnymi graczami rynku security jest jeszcze dużo pracy. Problem jest bardzo istotny, bo dotyczy nie tylko urządzeń nowych, ale także tych już zainstalowanych, które wymagają interwencji. Podjęcie wyzwania lub zaniechanie działań może znacznie wpłynąć na udziały na rynku bezpieczeństwa. □

Z PEWNYM SMUTKIEM, ALE RÓWNIEŻ POCZUCIEM DOBRZE SPEŁNIONEGO ZADANIA DZIELIMY SIĘ Z PAŃSTWEM OSTATNIM JUŻ FRAGMENTEM NASZEJ OPOWIEŚCI O MIEJSKIEJ DŻUNGLI. INSPIRACJĄ CYKLU BYŁA KSIĄŻKA JACKA PAŁKIEWICZA „DŻUNGLA MIASTA – KLUCZ DO BEZPIECZEŃSTWA". W TRAKCIE NASZYCH PIĘCIU SPOTKAŃ NA GOŚCINNYCH ŁAMACH „A&S POLSKA" NIE CHCIELIŚMY STRESZCZAĆ KSIĄŻKI, KTÓRA W SPOSÓB ZWIĘZŁY, PORADNIKOWY, ALE I NIEZWYKLE KOMPLEKSOWY PRZEPROWADZA CZYTELNIKA PRZEZ RÓŻNE ASPEKTY BEZPIECZEŃSTWA ŻYCIA W MIEŚCIE.

Jeśli naprawdę kochacie miasta, to dbajcie o nie lepiej niż o Amazonię!

DŻUNGLA MIASTA

Kompleksowe ujęcie różnych aspektów bezpiecznego życia pozostawiamy Czytelnikowi, który zechce po książkę pana Jacka sięgnąć. W naszych artykułach w „a&s" nieco rozszerzyliśmy i przybliżyliśmy wybrane tematy, wychodząc od zarządzania bezpieczeństwem przemysłowym oraz bezpieczeństwem infrastruktury krytycznej, przez czynniki pozornie stojące obok planowania bezpieczeństwa współczesnych miast, takie jak architektura duża i tzw. mała architektura miejska, po zagrożenia płynące z Internetu. Wszystko w aspekcie nowej metody zarządzania kryzysem, jaką jest u*rban resilience,* czyli rezyliencja.

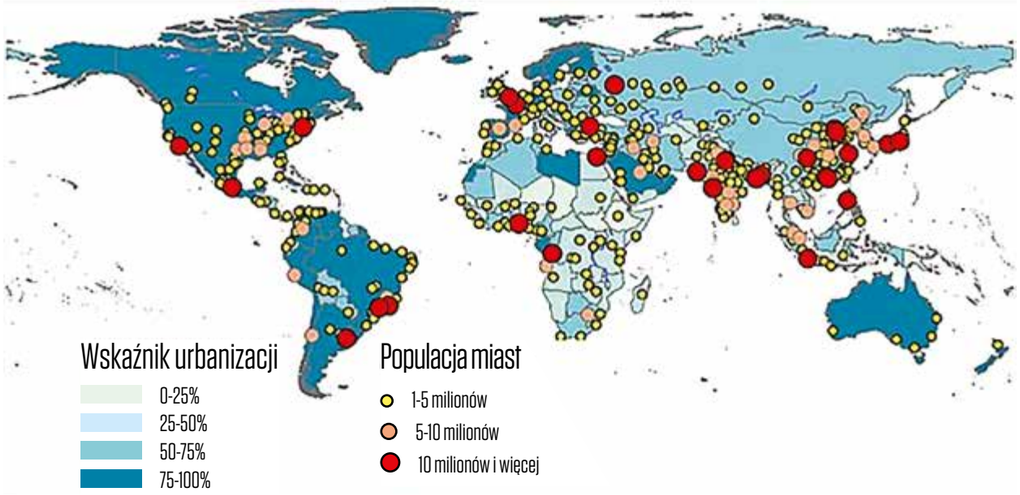
Odwoływaliśmy się do częstej w popkulturze frazy o „mieście, które jest betonową dżunglą". Frazy niezwykle ogranej, można by rzec pierwszego wyboru, jak podczas zgadywania skojarzeń w Familiadzie. Wpisując w najpopularniejszą wyszukiwarkę internetową frazę „miejska dżungla motyw w filmie w kulturze", otrzymujemy ponad 40 tys. rezultatów! Myślimy tymi kategoriami, i jest to słuszne skojarzenie. Miasto to wytworzona przez cywilizację dżungla, z której nieraz mamy ochotę się wyrwać i uciec, by zasmakować wolności. Miejska dżungla ma jeszcze jeden, ostatnio głośny aspekt: jesteśmy świadkami wielkiej tragedii, jaką są pożary lasów tropikalnych w Amazonii. Przeraża to chyba nas wszystkich, gdyż rozumiemy, że lasy w ogóle, a szczególnie te największe, jak dżungla amazońska, są niezwykle ważne dla całej cywilizacji, ważne dla naszego życia. I nie ma w tym żadnej egzaltacji czy przesady.

Przenosząc motyw dżungli w kierunku miasta jako rzeczywistości codziennego życia większości mieszkańców Ziemi, coraz częściej uświadamiamy sobie, że o miasta trzeba dbać. Trzeba o nie zabiegać, tworzyć je, przebudowywać, upiększać, czynić miejscami możliwie najlepszego i bezpiecznego życia. Teoretycznie wszystkie narzędzia potrzebne do zapewnienia mieszkańcom miast bezpieczeństwa i wysokiej jakości życia mamy w zasięgu ręki. Technologie security, a szczególnie analityka obrazu rozwijają się w niebywałym tempie. Nie ma już dzisiaj problemu z zarejestrowaniem obrazu dobrej jakości i przeanalizowaniem jego treści zarówno przez operatora, jak i dzięki algorytmom bazującym na *big data*. Rozwiązania *smart city* sprawiają, że systemy miejskie wzajemnie się uzupełniają, tworząc efekt synergii, i dostarczają danych dla zarządzających systemem. Kiedyś miasta przerażały jako siedliska zła i zepsucia, przestępczości i zbrodni. Popkultura, szczególnie kino, jest pełne obrazów miast zepsutych – Nowego Jorku, Londynu czy Tokio – jako siedlisk przestępczości. Pojawiają się obrazy miast wymyślonych, ociekających złem, jak w filmie *Sin City*. Takie obrazy wpływają na wyobraźnię.

Być może będzie to teza ryzykowna, ale czy to nie z powodu strachu i wyobraźni nakręconej przez kulturę uruchomiono wielki przemysł technicznych środków bezpieczeństwa dla miast? Wielkie ich bogactwo i różnorodność oraz stały rozwój technologii i możliwości są przedstawiane na łamach „a&s Polska" i podczas cyklicznych spotkań z branżą security. Systemy monitoringu wizyjnego – mobilne (np. na dronach) oraz klasyczne, zintegrowane centra monitoringu i analizy danych. Rozwinięte programy zapewnienia bezpieczeństwa obiektom infrastruktury krytycznej, w przeważającej części stanowiącej tkankę miasta. Bezpieczeństwo przestrzeni publicznych, obiektów handlowych, bezpieczeństwo imprez masowych, w tym bezpieczeństwo pożarowe. Są to dziedziny o sporym dorobku dzięki wytężonej i kreatywnej pracy zaangażowanych w nie menedżerów i specjalistów technicznych.

Powołany przez Fundację Rockefellera projekt „100 Resilient Cities"[1] co roku raportuje znaczący wzrost liczby

1) http://www.100resilientcities.org/about-us/



miast, które dzięki uczestnictwu w projekcie zbadały swoją rezyliencję, czyli odporność na sytuacje trudne, kryzysowe i różnego rodzaju ryzyko. Ciągle na tej liście nie ma żadnego polskiego miasta, a z regionu Europy Środkowo-Wschodniej tylko Belgrad uczestniczył w projekcie. Inna organizacja wywodząca się ze struktur Unii Europejskiej, EFUS[2], konsekwentnie tworzy w ostatnich latach wiele inicjatyw ukierunkowanych na rozwój jakościowy rozumienia różnych aspektów bezpieczeństwa miast. Uruchomiła nawet studia podyplomowe z zakresu zarządzania bezpieczeństwem miast. Dość znamienne jest to, że utknęły one w martwym punkcie po trzeciej edycji – nie udało się zebrać w skali Europy 40 chętnych na taki kierunek. Koszt nie był mały, ale też nie zaporowy – około 2 tys. euro.

Ciekawą ofertę ma Instytut Badań Przestrzeni Publicznej w Warszawie. Uruchomione tu kilka lat temu podyplomowe studia miejskie co prawda dość oszczędnie nawiązują do problematyki bezpieczeństwa, ale za to bardzo obszernie rysują piękno i skomplikowaną strukturę idei miasta i miejskiego życia w różnych aspektach. Studia są prowadzone w obiektach warszawskiej ASP, więc artystycznym klimatem są przesiąknięte, co tylko podnosi ich atrakcyjność[3].
Dopełnieniem obrazu globalnych aktywności na rzecz bezpieczeństwa przestrzeni miejskich jest UN Habitat będący agendą ONZ[4], który swoje działania koncentruje w krajach rozwijających się oraz ubogich.

Od kilku już lat żyjemy w świecie miast. Ludność zamieszkująca miasta przekroczyła liczebnie ludność obszarów wiejskich i niezurbanizowanych. To jest proces nieodwracalny w warunkach w miarę pokojowego rozwoju sytuacji na świecie. Nawet futurolodzy oraz twórcy sztuki i popkultury zazwyczaj karmią nas wizjami życia w koszmarnych ogromnych miastach nawet w epoce wielkiego i bliżej niezidentyfikowanego postkryzysu.

Globalne trendy wskazują na rosnącą liczbę mieszkańców wielkich metropolii. Lista megapolis, czyli miast powyżej 10 mln mieszkańców, liczy już ponad 40 pozycji. Zdecydowana większość nowych wielkich metropolii jest zlokalizowana poza Europą i Ameryką Północną.

Żyjemy w świecie całkowitego przedefiniowania pojęcia „miasto". Na przykład Tokio (metropolia tokijska), mające 37,5 mln mieszkańców, byłoby siódmym co do wielkości państwem Unii Europejskiej. Pod względem potencjału ekonomicznego zajęłoby czwartą lub piątą pozycję. Taka jest skala miast globalnych. W Polsce nawet nie myślimy o takich liczbach, ale dyskusja o tworzeniu metropolii jest żywa, choć nie znajduje się w czołówce dyskursu politycznego nawet przed wyborami samorządowymi. Widocznie nie ma takiej potrzeby, natomiast bezwzględnie jest potrzebna dbałość o bezpieczeństwo miast. Wiele się w tej sprawie dzieje. Polska policja od czasu do czasu ogłasza programy „Bezpieczne miasto", które angażują głównie policjantów. Wspólnoty mieszkańców i NGO (*non-government organization*) uruchamiają różne inicjatywy obywatelskie w trosce o bezpieczeństwo obywateli. Biznes również robi swoje, dbając o bezpieczeństwo swoich firm, terenów oraz osób przebywających na ich obszarze.
Temat bezpiecznego miasta często współgra z pojęciem *smart city,* chociaż wobec atrakcyjności terminu „miasto inteligentne" bezpieczeństwo tegoż miasta powoli przestaje funkcjonować jako niezależny byt, nie dlatego że jest czymś gorszym i wstydliwym, ale dlatego że staje się częścią *smart city* jako jego DNA.

Miejską dżunglą można, da się,
a przede wszystkim trzeba zarządzać.
Głównym problemem jest ciągle jeszcze
niewykrystalizowana metoda tego zarządzania

Badacze przyrody szukali i nadal poszukują systematyki praw władających dżunglami. Nie inaczej jest na szczęście z poszukiwaniem formuły zarządzania bezpieczeństwem, a ściślej ujmując – rezyliencją miejską. Brytyjskie stowarzyszenie BSI pracuje nad rozwinięciem standardu standardów, swoistym hubem z funkcją koordynującą ten obszar. W roku 2016 rozpoczęły się prace nad nowym standardem dla obszaru Urban Resilience[5], których wynikiem był wprowadzony w 2019 r. nowy standard BS 67000.

Trzymając się naszej lokalnej rzeczywistości, trzeba nawiązać do modelu zarządzania bezpieczeństwem w polskich miastach. Przeprowadzona kilka lat temu ankieta wśród mieszkańców polskich miast wskazuje jednoznacznie, że za ich bezpieczeństwo (rozumiane szerzej niż wynika to z kompetencji policji) odpowiedzialni są szefowie wydziałów bezpieczeństwa i zarządzania kryzysowego. Miasta stosują różne nazewnictwo, ale zazwyczaj ich rola orbituje wokół działań straży miejskich i policji. Nie jest naszą intencją oceniać, czy zakres ten jest wystarczający, ale warto przywołać anegdotę opowiadaną w jednym z większych polskich miast. Szefem Wydziału Bezpieczeństwa i Zarządzania Kryzysowego był emerytowany pułkownik Wojska Polskiego. Bardzo cenił on sobie zdobyte doświadczenie zawodowe i środowisko, z którego się wywodził – przez kilkanaście lat swojej działalności zajmował się głównie pielęgnowaniem sprzętu do ochrony osobistej. Po odejściu na emeryturę zdumionemu następcy pozostawił po sobie magazyn kilku tysięcy masek przeciwgazowych typu „słoń". Maski nie nadawały się do użytku, trudno było znaleźć instytucję, która chciałaby nieodpłatnie je przyjąć. Nowy szef miał co robić, żeby pracę wydziału skierować na inne tory.

Wsparciem dla szefów wydziałów bezpieczeństwa miast jest Związek Miast Polskich, a jedną z ważniejszych jego komisji jest Komisja Bezpieczeństwa i Porządku Publicznego[6].
Jej urzędnicy, pracując w reżimie ram ustawodawczych swoich funkcji, zajmują się tematami szczególnie dla nich istotnymi, np. związanymi z wypracowaniem szczegółowych rozwiązań odnoszących się do postulatu zwiększenia uprawnień samorządu w zakresie bezpieczeństwa i porządku. Komisja dostrzega konieczność wznowienia prac zmierzających do uregulowania problemów związanych z monitoringiem wizyjnym miejsc publicznych, zajmuje się także tematem zabezpieczania imprez masowych.

Miasto to dżungla. Podobnie jak dżungla jest piękne, ale bywa przerażające. Jest jednak istotna różnica między dżunglą przyrodniczą a tą miejską. Miejską dżunglą można, da się, a przede wszystkim trzeba zarządzać. Materia jest jednak bardzo skomplikowana i nawet biorąc tylko wycinek tego zarządzania, czyli bezpieczeństwo czy rezyliencję miasta, głównym problemem jest ciągle jeszcze niewykrystalizowana metoda tego zarządzania. Nie nauczyliśmy się zarządzać w sposób synergiczny. Z obserwacji wynika, że robimy to w sposób ZA BARDZO: za bardzo technologiczny, policyjny, urzędniczy, księgowy, wojskowy, antyterrorystyczny, proekologiczny, menedżerski, wolontariacki, polityczny, w lęku przed mediami. Przegięcia w kierunku „za bardzo" nie hamują rozwoju miast, one sobie poradzą. Ale źle skrojony system odporności miejskiej, mający chronić miasto i mieszkańców przed zmaterializowaniem ryzyka i zagrożeń, zawsze jest bolesny.
Szukajmy formuły sprawniejszego budowania dobrego życia w tych oazach wolności, jakimi były, są i będą miasta. Bo taka jest natura. Niemiecka sentencja jeszcze ze średniowiecza: *Stadtluft macht frei*, czyli miejskie powietrze czyni wolnym, jest świetnie pasującym podsumowaniem tematyki i uzasadnieniem, dlaczego warto budować piękne i bezpieczne miasta. Tym samym chcielibyśmy podziękować Czytelnikom naszego minicyklu „Dżungla miasta wg Jacka& Jacka" za uwagę i życzliwość. Mamy nadzieję, że zasialiśmy kilka ziaren do przemyśleń i refleksji. Polecamy się na przyszłość □

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.

2) https://efus.eu/pl/
3) http://ibpp.pl/studia_miejskie/
4) http://unhabitat.org/un-habitat-at-a-glance/
5) https://www.bsigroup.com/PageFiles/480725/Notes-on-city-resilience-workshops.pdf
6) http://www.miasta.pl/strony/komisja-bezpieczenstwa-i-porzadku-publicznego

Wpływ kosztów na usługi

– czyli co „funduje” nam wzrost płacy minimalnej i jak to wpływa na nasz biznes

***Stawka minimalna, Koszty ochrony, Budżet, Wzrost kosztów, Optymalizacja* – stawiam sto dolarów, że to hasła najczęściej wyszukiwane w przeglądarkach menedżerów odpowiedzialnych za finanse na przełomie 2019 i 2020 roku.**

TEKST
Rafał Łupkowski

Dostrzegam w tym ogromny plus dla rynku i branży usług ochrony. Paradoks polega na tym, że głównym atrybutem nie jest sam wzrost płacy minimalnej, ale wzrost kosztów. Jako branża security w tej części Europy osiągnęliśmy właśnie moment, w którym zaczynamy postrzegać rynek usług przez pryzmat następujących aspektów:

- Usługi ochrony to koszt – jaką wartość dodaną generuje?
- Bezpieczeństwo to proces – jak wspiera on organizację?
- Zmiany rynkowe – czy i w jakim stopniu wpłyną na jakość świadczonych usług?

W ostatnich miesiącach nasi klienci ze zdwojoną energią poszukują rozwiązań, które umożliwiłyby im optymalizację po stronie kosztów usług, zwłaszcza ochrony, z jednej strony rozumiejąc, iż wzrost wydatków wynika ze zmian przepisów, z drugiej – oczekując podkreślenia wartości dodanej wynikającej z usługi ochrony, aby zakup móc uzasadnić swoim zarządom. Zastanawiam się, jak długo taki stan rzeczy może mieć miejsce bez znaczących zmian na rynku.

Zewsząd słyszymy o wszechobecnej technologii, która docelowo ma zastąpić ochronę fizyczną i proste usługi dokładnie tak samo, jak w sektorze retail automaty kasjerskie miałyby zastąpić kasjerów. Technologia już wypiera człowieka, ale czy może go we wszystkim zastąpić? Moim zdaniem nie. Nie jest to bowiem uwarunkowane brakiem odpowiednich rozwiązań (technologii), lecz raczej nieprzygotowaniem rynku na ich wdrożenie. Z naszych doświadczeń wynika, że coraz częściej menedżerowie kupujący tego typu usługi dają się przekonać do pogłębionej analizy stanu faktycznego i implementacji adekwatnych, skrojonych na miarę rozwiązań. Warunek – po drugiej stronie muszą mieć partnera, który stara się zrozumieć prowadzoną przez nich działalność biznesową i realne potrzeby, a także z otwartą głową podchodzi do problemów bezpieczeństwa: kompleksowo, bez „upychania jedynych słusznych rozwiązań”.

Czy dostawcy usług i technologii są gotowi do zmiany podejścia do swoich zleceniodawców, czy chcą być partnerem stawiającym na pierwszym miejscu interes swojego klienta? O tym można się dowiedzieć na licznych konferencjach i mityngach branżowych.
Dlaczego tak trudno przekonać obie strony – kupującą i dostarczającą – do osiągania wspólnych celów biznesowych? Na polskim rynku pokutuje pewien paradygmat ujawniający się w naszej codziennej pracy polegającej na byciu kimś w rodzaju pomostu czy też mediatora pomiędzy klientem a dostawcą usługi lub rozwiązania. Problemem jest brak wzajemnego zrozumienia, a przede wszystkim zaufania, gdyż dziesiątki, jeśli nie setki przypadków potwierdzają, że obie strony „układanki” często mają określone problemy z uzyskaniem podstawowych elementów kontraktu.

Zamawiający w ramach postępowań pytają o koszt, nie określając istotnych szczegółów dotyczących usługi czy rozwiązania. Dostawcy natomiast proponują to, co już od lat lepiej lub gorzej działa, bądź „wrzucają” mniej lub bardziej określony standard. W ten sposób powiela się stare błędy, aż do czasu poważnego incydentu lub rzeczonego wpływu kosztów na zakres kontraktu.
Muszę zaznaczyć, że powyższy stan z pewnością nie dotyczy całego rynku i radykalizowanie poglądów jest krótkowzroczne, jednak liczba przykładów z codziennej pracy jednoznacznie wskazuje na reprezentatywność tych opinii, a zebrane materiały z pewnością mogą stanowić temat na bardzo długą opowieść. Zdarzają się na rynku kontrakty, które dopiero co zawarte stają przed widmem ich zakończenia z powodu braku elementarnej staranności obu stron. Wynika to także z braku odpowiednich partnerskich relacji, pokazując tym samym, jak często zakupy w zakresie usług ochrony są traktowane jako przykry obowiązek lub techniczny element, bo (cyt.) „ubezpieczyciel tego wymaga” lub „przecież ochrona zawsze była” albo „zamiast dozorcy powieśmy kamerki”. Brzmi znajomo?

> Dlaczego aż tak trudno jest przekonać obie strony (klientów i dostawców) do osiągania wspólnych celów biznesowych?

Trzeba temu zapobiegać, oczywiście możliwie jak najszybciej, mając na względzie, że:

- koszty płacy minimalnej z dużym prawdopodobieństwem wciąż będą rosły,
- statystycznie w usługach ochrony jest coraz mniej ludzi do pracy, co potwierdzają profesjonalne raporty największych firm rekrutacyjnych, które już od pewnego czasu sygnalizują problemy na rynku ochrony,
- średni wiek pracownika ochrony niebezpiecznie rośnie, a nie ma odpowiedniej zastępowalności przez młodszą kadrę,
- koszty technologii maleją i coraz bardziej wdziera się ona do naszego życia codziennego.

Coraz częściej pojawiają się wątpliwości, czy mając na uwadze przedstawione argumenty, radykalny wzrost stawki minimalnej cokolwiek poprawi, ponieważ powoduje on wzrost kosztów stałych, spadek dochodów oraz teoretycznie wyższe opłacanie ograniczonego potencjału ludzkiego.

Aby skutecznie temu przeciwdziałać, bez negatywnego oddziaływania na prowadzony biznes i działalność przedsiębiorstwa, należy:

- traktować bezpieczeństwo swojego biznesu jako proces szerszy, który nie ogranicza się tylko do pracownika ochrony czy kamery,
- okresowo analizować zmiany zachodzące w procesie bezpieczeństwa i stosować ADEKWATNE środki, korzystając z dostępnych narzędzi oceny ich wpływu na biznes oraz analizy zagrożeń i ryzyka ich wystąpienia,
- próbować poznać i rozumieć rzeczywiste potrzeby, nie ograniczać się do tego, co było, tylko bazować na stanie faktycznym (tym co jest) z nastawieniem na możliwość dokonywania uzasadnionych zmian,
- otworzyć się bardziej na czerpanie z wiedzy i doświadczeń rynkowych, w tym także konsultingu, ponieważ realizując te same lub podobne zadania przez określony czas, niejednokrotnie zatracamy naturalną zdolność do postrzegania i adaptacji.

O tym, jak duży wpływ na efektywność każdego biznesu mają rosnące koszty, przekonujemy się na co dzień, analizując, ile pracy musi włożyć dana firma, aby na konieczne koszty zarobić.
Po raz kolejny zastanówmy się wspólnie nad tym, czy stać nas i jak długo na nieefektywne usługi, które mają wspierać nasz biznes. □

BIO
Rafał Łupkowski
Business Security Advisor, Chief Operating Officer w firmie doradczej Trustman

JAK BYĆ MĄDRYM PRZED STRATĄ?

WYDAWAĆ BY SIĘ MOGŁO, ŻE W DOBIE NOWOCZESNYCH TECHNOLOGII, CORAZ SKUTECZNIEJSZYCH SYSTEMÓW MONITORINGU WIZYJNEGO, ZARZĄDZANIA DOSTĘPEM, ROZWIĄZAŃ UTRUDNIAJĄCYCH DOKONANIE NAPADU CZY WŁAMANIA TRADYCYJNE ZAGROŻENIA SĄ TEMATEM POWIEŚCI KRYMINALNYCH CZY FILMÓW PREZENTOWANYCH W KANAŁACH STREAMINGOWYCH. NIESTETY, CORAZ BARDZIEJ POWSZECHNE KRADZIEŻE PIENIĘDZY Z KONTA KLIENTA POPRZEZ FISHING CZY ZASTOSOWANIE TECHNIK MANIPULACYJNYCH W CELU WYŁUDZEŃ ZNACZNYCH KWOT NIE SPOWODOWAŁY ZANIKU TRADYCYJNYCH METOD KRADZIEŻY.

TEKST
Michał Czuma

W roku 2015 głośno było o napadzie na Hatton Garden Safe Deposit, skąd złodzieje zrabowali z rozprutych skrytek depozytowych kosztowności warte 200 mln funtów. Kradzież zauważono dopiero nad ranem, po Wielkanocy, w chwili otwarcia banku depozytowego. Oczom policjantów ukazało się potężne gruzowisko zniszczonych skrytek i skruszonego betonu w efekcie kilkumetrowego przebicia się złodziei przez grube żelbetonowe mury zabezpieczające skarbiec. Podczas wielkanocnej przerwy rabusie wykorzystali szyb windy w pobliskim budynku, dostali się do piwnic i przebili półmetrową żelbetonową ścianę do skarbca położonego w centrum dzielnicy, która od średniowiecza słynie ze sprzedaży diamentów i kosztowności. Alarm zadziałał, ale nikt na niego nie zareagował, nawet policja. Po zneutralizowaniu alarmu i rozpruciu 18-calowych metalowych drzwi opróżniono blisko 70 skrytek z kosztownościami. Podejrzani w wieku od 48 do 76 lat zostali zatrzymani w wyniku zmasowanych przeszukiwań przeprowadzonych przez ponad 200 funkcjonariuszy policji.

Do tej pory najpoważniejszego w Wlk. Brytanii przestępstwa o charakterze zaboru majątku dokonano w lutym 2006 r. w mieście Tonbridge, na południowy wschód od Londynu. Po sterroryzowaniu szefa i pracowników składnicy gotówki firmy Securitas gangsterzy zabrali z niej 53 mln funtów w banknotach. Akcja policji doprowadziła do rychłego aresztowania większości sprawców i odzyskania blisko 20 mln funtów, ale uważany za główną postać w tej sprawie Keyinde Patterson nadal ukrywa się przed wymiarem sprawiedliwości ze znaczną częścią łupu. To też był bardzo ciekawy pod względem *modus operandi* napad, starannie przygotowany i wykonany przez sprawców, z których część występowała w mundurach policjantów. Novum w przeprowadzonym napadzie i głównym elementem zuchwałej kradzieży połączonej z napadem było uprowadzenie kierownika magazynu i jego rodziny przez dwie osobne grupy przestępcze. Przebrani za policjantów napastnicy, jadąc na sygnale nieoznakowanym wozem policyjnym, zatrzymali samochód, którym podróżował kierownik skarbca. Nakazali mu przesiąść się do ich pojazdu. Ten podporządkował się poleceniu w przekonaniu, iż ma do czynienia z prawdziwymi policjantami, po czym w domniemanym policyjnym samochodzie został skuty kajdankami. W tym samym czasie dwóch innych fałszywych policjantów odwiedziło jego rodzinę w domu znajdującym się w miejscowości Herne Bay, by przekazać fałszywą wiadomość, że kierownik miał wypadek drogowy, i pod tym pretekstem wyprowadzić ich z domu.
Mając rodzinę, napastnicy zaszantażowali kierownika, zmuszając go do współpracy z gangiem. Zawieziono go na teren firmy ochroniarskiej. Tam sześciu kolejnych członków gangu (zamaskowani, niektórzy uzbrojeni w broń palną) zagroziło ok. 15 pracownikom firmy. W tym czasie kolejna grupa ładowała gotówkę do przygotowanego pojazdu.
– *Nie ulega wątpliwości, że napad został szczegółowo zaplanowany w dłuższym okresie, a napastnicy musieli od kogoś mieć informacje, które pomogły im w przygotowaniu napadu* – powiedział dziennikarzom detektyw Paul Gladstone z policyjnego wydziału do walki z zorganizowaną przestępczością w hrabstwie Kent.

Dlaczego zaprezentowałem te dwa głośne napady uznane przez dziennikarzy za napady stulecia w Wlk. Brytanii? Wbrew pozorom – chociaż te napady dzielą lata oraz *modus operandi* – są pewne elementy wspólne, nad którymi warto się zatrzymać.

Najsłabszym elementem każdego systemu jest człowiek

Wiem doskonale, że to truizm, ale wiele firm jest gotowych wydać miliony na najnowocześniejsze systemy zabezpieczające, a zapomina o tym, że wystarczy w łańcuchu bezpieczeństwa umieścić niewłaściwego człowieka, a system traci na swojej odporności i skuteczności. Przestępcy zaczynają rozpoznanie systemów od ludzi zatrudnionych w firmie i do nich szukają dotarcia. A jeśli nie da się ich pozyskać, starają się ich w jakikolwiek sposób kontrolować, dążąc do „spacyfikowania". Przy napadzie na Hatton Garden Safe Deposit okazało się, że złodzieje pokpili na początku sprawę i po południu w Wielki Piątek na chwilę uruchomili alarm, jednak ochrona nie dopełniła swoich obowiązków.

– *Strażnik poinformował mnie, że włączyły się czujniki* – tłumaczył dziennikarzowi „Daily Mail" Norman Bean, który stracił kamienie warte 35 tys. funtów. – *Zszedł do piwnicy, zajrzał przez drzwi, ale niczego nie zauważył. Gdy zapytałem, dlaczego nie zszedł do skarbca, odparł, że za mało mu płacą* – żalił się mężczyzna. Część właścicieli skrytek jest przekonana, że bandytom pomógł ktoś z pracowników, ponieważ ci wiedzieli, jak wyłączyć system alarmowy. Dziennikarze byli bezlitośni dla wszystkich odpowiedzialnych za ochronę systemu – pilnie strzeżony obiekt pokonała „banda emerytów i rencistów" (najmłodszy członek grupy przestępczej miał 48 lat, natomiast najstarsze osoby – odpowiednio: 74 lata i 76 lat).

Nie tak dawno jeden z moich potencjalnych klientów wskazywał na rozpoznaną przez niego przyczynę strat swojej firmy – źle funkcjonującą firmę ochroniarską, która w jego przekonaniu nie wywiązywała się z obowiązków. Zrezygnowali z ich usług i przeprowadzili kolejny przetarg, który wygrała inna firma. Jakież było ich zdziwienie, gdy pracę w przedsiębiorstwie rozpoczęli ci sami ochroniarze, ale z innym logo na służbowych ubraniach. Przygotowując ofertę dla klienta, standardowo przeprowadziłem rekonesans i zbadałem sytuację w otoczeniu jego firmy.

Nie zdziwiło mnie, że klient boryka się z różnymi problemami, m.in. z kradzieżami, skoro zatrudnia firmy ochroniarskie, w których pracują osoby z wysoką grupą inwalidzką i bez kwalifikacji. Sama firma ochroniarska nie tylko płaciła im kiepsko, ale także jej system kontroli tolerował wiele patologicznych zachowań własnych pracowników.

Można stwierdzić, że takie sytuacje, gdy angażuje się „tanie" środki, działające raczej na zasadzie „pozoranta", który ma odstraszać, zamiast przeciwdziałać, to niestety często standard. Wiele firm ochroniarskich zatrudnia ludzi za niewielkie stawki, by utrzymać się na rynku, ponieważ klienci chcą płacić jak najmniej. Firmy ochroniarskie zmuszone do szukania oszczędności zatrudniają osoby bez merytorycznej wiedzy i doświadczenia. Efektem tego jest swoiste zderzenie dwóch fikcji: jedni udają, że są w stanie chronić klienta – a klient udaje, że czuje się chroniony.

Oszczędzanie na bezpieczeństwie nie ma racjonalnych podstaw, co powtarzam każdemu, kto chce zabezpieczyć swoje „skarby" przed kradzieżą, wyłudzeniem czy zniszczeniem. A gdy się wie, że szykujący się do kradzieży złodziej najpierw rozpoznaje sytuację, sprawdza czujność ochroniarzy oraz penetruje często dokładnie zastosowane zabezpieczenia, nie można wybierać rozwiązań dających poczucie bezpieczeństwa, kierując się zasadą – wybieramy rozwiązania najtańsze.

Każda oszczędność w tworzeniu systemu bezpieczeństwa firmy zwykle przekłada się na wysokość strat. Problem rośnie, gdy narażone jest również życie ludzkie. I wiem to z własnego doświadczenia, gdyż odpowiadałem za bezpieczeństwo kilku tysięcy ludzi pracujących w oddziałach banku i narażonych codziennie na ryzyko napadu. Dlatego chciałbym, aby moje słowa zabrzmiały dobitnie: nie można oszczędzać, angażując firmę ochroniarską, rozpoznając wszystkie możliwe zagrożenia, kupując systemy monitorujące, dobierając systemy zabezpieczeń, by później dobrać odpowiednie rozwiązania, skutecznie zabezpieczające także te najsłabsze ogniwa w firmie czy zakładzie. Bezcenne jest życie naszych pracowników oraz efekty ich ciężkiej pracy.

> Każda oszczędność w tworzeniu systemu bezpieczeństwa firmy zwykle przekłada się na wysokość strat

Najlepsze rozwiązanie, ale źle dobrane jest nieskuteczne

To również truizm. Będąc zastępcą dyrektora bezpieczeństwa Banku PKO BP SA, byłem bombardowany ofertami i wizytami przedstawicieli handlowych oferujących „najlepsze na świecie" rozwiązania bezpieczeństwa. Ale w naszym przypadku były one zupełnie nieprzydatne.

W obu przytoczonych wyżej „skokach stulecia" wszystkie obiekty były dobrze zabezpieczone. Wydano na zastosowane tam zabezpieczenia ogromne pieniądze, gdyż „chroniąc setki milionów, wydaje się miliony". A jednak zastosowane systemy zabezpieczały przed niektórymi tylko zagrożeniami, przed innymi okazały się mało skuteczne (zła procedura w centralce alarmowej). W pierwszym przypadku system alarmowy po jego załączeniu można było zablokować, lecz pracownikowi ochrony nie chciało się sprawdzić, co wzbudziło alarm, „bo mu kiepsko płacili". W drugim przypadku nie przewidziano, że wszystko może być iluzją, i nie zabezpieczono się na wypadek wrogiego przełamania zabezpieczeń. Dzisiaj, przy istniejących rozwiązaniach technicznych i analitycznych, można nawet rozpoznać, że do głowy naszego pracownika czy klienta przyłożono pistolet i zmuszono do działania na swoją niekorzyść.

Na ostatnim spotkaniu – śniadaniu A&S Polska znamienici goście podkreślali fakt, że bardzo trudno na rynku o integratora, który znając możliwości dostawców rozwiązań oraz potrzeby klientów pod kątem zabezpieczenia się, stworzy spójny, dostosowany do potrzeb klienta system bezpieczeństwa. Dużo w tym prawdy, gdyż często spotykam się z sytuacją, że osoby bez wiedzy eksperckiej wprawdzie oferują rozwiązania zapierające dech w piersiach, ale nie znają realnej sytuacji klienta. Jako doradca muszę być również „integratorem", by zaproponować klientowi rozwiązanie optymalne. Muszę przyznać, że od ponad dziesięciu lat trafiam na dostawców rozwiązań, które można zastosować do budowania złożonych, czasami unikalnych systemów bezpieczeństwa „szytych na miarę i pod kątem oczekiwań moich klientów". Postęp technologiczny jest oszałamiający.

Większość oszustów i złodziei robi wszystko, by ukryć swoją tożsamość. W maskach napadają na banki, wynoszą z magazynów kosztowne rzeczy, włamują się na posesje, ukrywając twarz. Długo czekałem na rozwiązanie, które rozpoznaje unikalne, indywidualne i niepowtarzalne cechy, a dzięki temu identyfikuje osobę. Na podstawie analizy behawioralnej sprawcy można rozpoznać człowieka po sposobie poruszania się – po jego motoryce, charakterystycznym zachowaniu się czy rozpoznaniu, unikalnych proporcjach budowy ciała. Takie skuteczne i działające rozwiązanie już jest i można je stosować bez budowania kosmicznie drogich systemów. Czytając regularnie „a&s Polska", można się przekonać, że technologicznie biznes ma już w czym wybierać, by zabezpieczyć dowolny budynek, strukturę, firmę, zakład czy człowieka przed wieloma zagrożeniami i nękającymi firmy problemami. Jedyny znak zapytania może dotyczyć kwestii wyboru rozwiązania, które należałoby zastosować, by wszystko działało skutecznie, a inwestycja w bezpieczeństwo się zwróciła.

Już dzisiaj systemy telewizji dozorowej mogą autonomicznie śledzić konkretne przedmioty i osoby, sposób, w jaki zmieniają swoje położenie, gdzie się znajdują. Nie chodzi przy tym o inwigilację, ale o ochronę. Współczesne zaawansowane systemy mogą wskazać kierunek przemieszczania się ludzi, obiektów, a nawet dokumentów, potrafią je odnaleźć, zidentyfikować i wskazać. Nie trzeba już zatrudniać wielu operatorów, by monitorować obraz z setek, a nawet tysięcy kamer, gdyż już są systemy, które nie tylko rejestrują obraz, ale także potrafią zidentyfikować konkretne, interesujące nas zdarzenia i zachowania i w reakcji na nie uruchomić alarm, wysłać do konkretnych osób lub systemów czytelną informację oraz podjąć określone, szybkie i zdecydowane działania, np. blokujące wejścia, by uniemożliwić intruzowi ucieczkę.

Systemy stosowane na stadionach są w stanie rozpoznać wśród tysięcy kibiców nie tylko osoby z zakazami stadionowymi, ale też wykrzykujące rasistowskie hasła czy poszukiwane listami gończymi. Postęp technologiczny zmierza w kierunku systemów opierających się na sztucznej inteligencji (AI), samouczących się i autonomicznych. Nieuchronnie zmierzamy w kierunku tego, iż człowiek zostanie zastąpiony przez inteligentne systemy, maszyny, roboty.

Jeszcze chwila, a ludzie przestaną być potrzebni, np. do podjęcia interwencji w przypadku zdarzeń wymagających konkretnych działań – są systemy patrolujące wskazany obszar czy teren w sposób bardziej sumienny niż zaspany ochroniarz lub strażnik. Trwają prace nad dronami – które nie muszą spać, są nieprzekupne i skuteczniej ostrzegają przed rozpoznanymi anomaliami. Jednych ta wizja przeraża, innych intryguje. Ale jeden problem pozostaje na pewno do rozwiązania – te same rozwiązania, ale nieodpowiednio zastosowane czy dobrane mogą być nieefektywne. Trzeba pamiętać, że zakup danego rozwiązania ma nie tylko zlikwidować nasze problemy, przede wszystkim musi się zwrócić.

Bezpieczeństwo to także biznes

Nim rozwinę powyższą myśl, przytoczę kilka spektakularnych akcji, które przyniosły straty, a przestępcom zapewniły sławę i pieniądze. Zacznę od wielkiego napadu na pociąg w 1963 r. Ukradziono 2,6 mln funtów (dzisiaj – 40 mln funtów) z wagonu pocztowego. Dokonał tego 8 sierpnia 1963 r. 15-osobowy gang. W trakcie napadu, gdy zatrzymano pociąg na moście w pobliżu miejscowości Mentmore w Wlk. Brytanii, nikt nie zginął. Uciepiał jedynie maszynista, którego napastnicy uderzyli w głowę. Pieniędzy nigdy nie udało się odzyskać.

Inna historia pokazuje, że czasami złodzieje mogą mieć farta. Patrick Thomas w 1990 r. napadł z nożem w ręku

na pierwszego lepszego posłańca na jednej z cichych (wtedy) uliczek Londynu. Okazało się, że przenosił on rachunki i depozyty do Banku Anglii – łącznie na kwotę 292 mln funtów. I chociaż szczęście rabusia nie trwało długo, a policja odzyskała niemal wszystkie obligacje, wiele osób ta historia doprowadziła do palpitacji serca.
W 1987 r. dokonano napadu na Knightsbridge Security Deposit Bank, w którym pieniądze i biżuterię trzymało wiele osobistości. Rabunku dokonał włoski rabuś Valerio Viccei, któremu po sterroryzowaniu obsługi wyniesiono z banku w gotówce i kosztownościach ponad 200 mln dolarów. Napad był prawie doskonały. Viccei zbiegł i ukrył się gdzieś w Ameryce Łacińskiej, ale po jakimś czasie postanowił wrócić po swoje ferrari – policja wykorzystała okazję i sprawcę zatrzymała.
18 marca 1990 r. dwóch złodziei w przebraniu policjantów wyniosło z Muzeum Isabelli Steward Gardner w Bostonie obrazy Degasa, Maneta, Rembrandta i Vermeera. Jedno płótno tego ostatniego było szacowane na 250 mln dolarów. Do dzisiaj nie wiadomo, co się stało ze zrabowanymi działami sztuki. Oto kolejne dwa przykłady. Pierwszy to napad na najsłynniejszy hotel w Cannes. W 1994 r. trzej złodzieje sterroryzowali jubilera w hotelu Carlton, jak się potem okazało, strzelając ślepymi nabojami. Udało im się w ten sposób uciec z biżuterią wartą 30 mln funtów. Kolejnym przypadkiem była słynna kradzież diamentów na lotnisku Schiphol w 2005 r. – czterem złodziejom udało się wcielić w członków konwoju, w efekcie przejmując z samolotu drogocenne diamenty.
Wszystkie przypadki uzmysławiają jedną prawdę – jeśli posiadasz coś cennego, co ma wartość dla ciebie, twoich szefów i klientów, na pewno zainteresuje to osoby nieuczciwe. Pytanie, kiedy i jak to zrobi, a czy ty będziesz na ten akt agresji przygotowany.
Większość firm doradczych, takich jak EY, Deloitte czy PWC w swoich analizach wskazuje w sposób niebudzący wątpliwości, że większość firm jest okradana albo będzie okradziona. Straty z tytułu kradzieży często idą w dziesiątki milionów dolarów czy złotych. Jeśli więc w sposób mądry profesjonalnie zbada się zagrożenia, co i jak może być skradzione – uda się stworzyć skuteczne zabezpieczenia, a zainwestowane w bezpieczeństwo pieniądze pozwolą uniknąć strat. Z mojego doświadczenia wynika, że niezależnie od wysokości przeznaczonych na bezpieczeństwo kwot są to szybko zwracające się inwestycje.
Co ważne, trzeba inwestować rozsądnie.

Najpierw rozpoznać słabe punkty w organizacji, miejsca zagrożone przestępczymi działaniami, przeprowadzić audyt firmy pod kątem bezpieczeństwa i fraudów, a następnie szacując ryzyko rozpoznanych zagrożeń, dobrać odpowiednie rozwiązania. Nic nie może być dziełem przypadku, a budowa zabezpieczeń musi opierać się na biznesowych podstawach – inwestycja w bezpieczeństwo musi się zwrócić.

Czy jesteśmy rzeczywiście zagrożeni i w jakim stopniu?

To pytanie często słyszą osoby odpowiedzialne za bezpieczeństwo. Dzisiaj każda firma posiadająca jakiś majątek, niezależnie czy to firma produkcyjna, czy świadcząca usługi, posiada coś, co ma wartość, i może zostać okradziona. Oszuści i złodzieje kradną to, co ma jakąkolwiek wartość. Jeśli więc posiadasz dane, pieniądze, produkujesz produkty szybko zbywalne albo wartościowe, dysponujesz wiedzą, którą ktoś zechce drogo kupić, bo np. da mu to dodatkowy zarobek, pozwoli oszczędzić znaczne fundusze na pokonywanie dystansu w wyścigu konkurencyjnych firm, jeśli masz coś cennego dla ciebie, co może mieć również wartość dla innych, jesteś zagrożony.
Czy jesteś producentem FMCG, dostawcą usług dla dużych klientów lub posiadasz wiedzę o klientach innych, masz cenne dane, znasz tajemnice firmy, masz pieniądze – wcześniej czy później staniesz się celem złodziei. Odczujesz to bardzo boleśnie. Ale możesz sobie tego oszczędzić, wykonując kilka działań chroniących cię przed nieuczciwymi pracownikami, kontrahentami, złodziejami czy oszustami.

Dobry gospodarz, kiedy buduje dom, przed położeniem tynków zaprasza specjalistów od alarmów i systemów zabezpieczeń, by zaplanowali optymalne rozwiązania chroniące jego dom, dobytek i najbliższych. Osoby niefrasobliwe uważają, że zdążą się zabezpieczyć, gdy już w domu zamieszkają. Najczęściej kończy się to tym, że zabezpieczają się po kradzieży. Dokonanie wyboru, które rozwiązanie okaże się tańsze i skuteczniejsze, pozostawiam czytelnikom, gdyż każdy odpowiada za spokój i bezpieczeństwo swojej działalności.

BIO

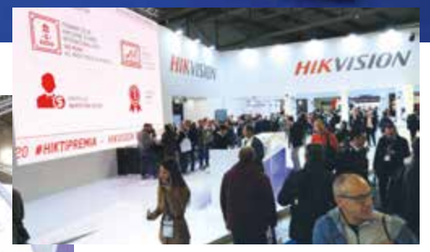
Michał Czuma

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.

Szukasz prawdziwych targów zabezpieczeń? Wybierz się do Mediolanu!

Sicurezza – targi zabezpieczeń w Mediolanie – jako nieliczne spośród organizowanych w Europie zaliczyły dwucyfrowy wzrost (w ujęciu procentowym) odwiedzających w stosunku do poprzedniej edycji. 619 wystawców z 37 krajów przedstawiło innowacje produktowe 28 629 odwiedzającym. Pod względem liczb Sicurezza przypomina nasze rodzime targi, z jednym zastrzeżeniem: wydarzenie w Mediolanie dotyczy tylko systemów zabezpieczeń. To, co niepowtarzalne, to udzielający się włoski temperament uczestników wydarzenia zachęcający do gorących dyskusji (oczywiście przy aromatycznej kawie), wymiany doświadczeń i otwartości na nowe koncepcje.

Tematem przewodnim trzech dni targowych była ewolucja systemów zabezpieczeń i automatyki budowlanej oraz aktualizacje scenariuszy bezpieczeństwa. Integracja systemów oraz AI stanowiły mocne akcenty na wielu stoiskach, ukazując stabilny, dalszy rozwój naszej branży w tym kierunku. Oprócz prezentowanych rozwiązań na styku AI + IoT + chmura coraz ważniejsze wydawały się elementy wykonawcze, takie jak zamki czy systemy sterowania napędami. Od ich sprawnego działania bowiem zależy powodzenie wykonania całego scenariusza bezpieczeństwa. Dlatego nie dziwiło, że prezentowane w Mediolanie sterowniki to skomplikowane układy zasilane technologią IoT, umożliwiającą na bieżąco zbieranie informacji o stanie zużycia poszczególnych elementów, by na czas zareagować i wymienić element przed jego usterką.



W strefie Expo dotyczącej inteligentnych miast można było podziwiać ścisłą współpracę pomiędzy ościennymi technologiami, która wyeliminowała bariery, z jakimi jeszcze niedawno musieliśmy się mierzyć na różnych rynkach wertykalnych. Systemy sterujące przepływem ludzi, automatyzacja budynków, systemy telewizji dozorowej, rozwiązania oszczędzające energię, systemy audio-wideo, platformy chmurowe i telekomunikacja (w tym przede wszystkim testowana we Włoszech technologia 5G) były ukazane jako elementy dynamicznego systemu opartego na skutecznym wykorzystaniu tzw. *big data*.

Sicurezza to też świetne miejsce do nauki i wymiany doświadczeń. Bogata oferta ponad 100 konferencji oszałamiała, tym bardziej że na większość z nich trudno było znaleźć wolne miejsce. Zainteresowanie wśród odwiedzających wzbudziła również debiutująca Cyber Arena – nowa strefa wystawiennicza, szkoleniowa i informacyjna, tak zaprojektowana, aby pomóc firmom w jak najlepszym zarządzaniu zagrożeniami IT. Wśród stoisk trudno było nie zauważyć ekspozycji firmy Hikvision, bodaj największej na targach. – *Tak duża przestrzeń umożliwiła zaprezentowanie wszystkich nowości z naszych linii biznesowych* – podkreślali przedstawiciele chińskiego producenta. Rzeczywiście, oprócz rozwiązań związanych *stricte* z telewizją, która nadal dominowała, pokazano produkty ochrony perymetrycznej w postaci barier podczerwieni, radarów, kamer termowizyjnych, jak również systemy transmisji bezprzewodowej, kontroli dostępu, włamania i napadu, wideodomofony, a także wielkopowierzchniowe ściany monitorów i rozwiązania *digital signage*.
Dahua zdecydowała się na stoisko mniejsze, ale w moim odczuciu bardziej w duchu europejskim. Zamiast prezentacji wszystkich swoich nowych produktów z wielkiego portfolio, postawiono na prezentację rozwiązań dla rynków wertykalnych: smart city, muzea czy retail. Dla odwiedzających miłym przeżyciem było na pewno doświadczenie wirtualnej rzeczywistości (VR) w trakcie obserwacji podwodnego świata.

Swoje stoiska targowe miały również m.in. polskie firmy Satel i Pulsar, obie obecne na rynku włoskim już od kilku lat. Przez ten czas wypracowały własną siatkę dystrybutorów, którzy rozwiązania wyprodukowane w Polsce bardzo sobie chwalą za staranność wykonania, innowacyjność i atrakcyjną cenę. Satel w tym roku zdecydował się na interaktywną prezentację przykładowych możliwości, jakie oferują ich rozwiązania w ramach realizacji automatyki domowej w międzynarodowym standardzie KNX. W ten sposób firma rozwija swoje portfolio produktowe w kierunku *smart home*. Obok modułów KNX wielkim zainteresowaniem cieszyła się nowa linia czujek serii SLIM LINE, przyciągająca uwagę m.in. atrakcyjnym wzornictwem.

Z kolei Pulsar zaprezentował nowe zasilacze do systemów przeciwpożarowych zgodnych z EN54. Na stoisku producenta można też było podziwiać obudowy na rejestratory wideo, które są ciekawą odpowiedzią firmy na konieczność zabezpieczania urządzenia przed niepowołanym dostępem.

Włochy to kraj producentów napędów do bram i systemów do szybkiego „zadymiania" pomieszczenia, dlatego nie dziwiła bogata oferta tych rozwiązań na Sicurezzie. Prezentacje zadziałania generatorów mgły pozostawiały trwały ślad na uczestnikach, nie tylko w postaci mgiełki unoszącej się wokół ich sylwetek krótko po opuszczeniu pomieszczenia. Skłaniała również do refleksji. Według statystyk bowiem czas trwania większości rozbojów nie przekracza 3 minut. Co prawda system alarmowy powiadamia o kradzieży, ale nie może jej zapobiec. Producenci generatorów mgły podkreślali, że jeżeli chodzi o rzeczywistą skuteczność ochrony mienia, trudno przecenić ich rozwiązania. □

Podsumowanie VIII edycji spotkań **Schrack Seconet i Partnerzy**

VIII edycja Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego Schrack Seconet i Partnerzy odbyła się 23–24 października br. w hotelu Windsor w Jachrance. Na 2-dniowe wydarzenie zarejestrowało się łącznie ponad 570 osób! Organizatorzy również w tym roku umożliwili udział w nich tym, którzy nie mogli osobiście pojawić się na miejscu – przez dwa dni była prowadzona transmisja LIVE w Internecie.

Ogromne zainteresowanie imprezą potwierdza sensowność, a nawet konieczność organizacji częstszego organizowania spotkań merytorycznych w branży systemów bezpieczeństwa. Schrack Seconet Polska, wychodząc naprzeciw oczekiwaniom rynku, każdego roku przygotowuje wiele nowości. Dotyczą one sposobu organizacji wydarzenia, komunikacji z uczestnikami (różnorodne formy przekazu), a przede wszystkim coraz głębszej, dokładniejszej analizy problemów pojawiających się w trakcie projektowania i realizacji obiektów różnego przeznaczenia.

Podczas dwóch dni wykładów merytorycznych, paneli dyskusyjnych i pokazów działania urządzeń uczestnicy poznali aktualne zmiany prawne, wytyczne, normy i najlepsze praktyki w zakresie procesów oceny zagrożeń, tworzenia koncepcji, projektowania, realizacji i eksploatacji zintegrowanych systemów bezpieczeństwa pożarowego, technicznego i fizycznego. Studia przypadków oparte na pokazach pracy urządzeń były na bieżąco komentowane przez specjalistów branżowych. Praktyki i możliwości zastosowania najnowszych rozwiązań technicznych proponowane przez firmy partnerskie oceniali eksperci rynku.

Podczas tej edycji po raz pierwszy podjęto próbę sformułowania standardu oceny jakości wdrożenia zintegrowanego systemu bezpieczeństwa, kładąc szczególny nacisk na ocenę skuteczności stosowanych technologii i rozwiązań organizacyjnych oraz ich wpływu na skuteczność bezpiecznej ewakuacji osób z obiektów budowlanych różnego przeznaczenia.

Nowością tegorocznego spotkania były dodatkowe sale warsztatowe, w których swoje prezentacje i zajęcia poprowadzili eksperci ds. pożarowych i specjaliści od zarządzania ryzykiem – na co dzień oceniający zagrożenia i stan przygotowania budynków do minimalizacji skutków zdarzeń kryzysowych z ramienia firm ubezpieczeniowych. Poruszane kwestie obejmowały zagadnienia dotyczące odstępstw, analizy przypadków wykraczających poza ramy wytycznych i prawne oraz ocenę skutków zdarzeń kryzysowych z punktu widzenia warunków wypłaty lub wstrzymania odszkodowania za straty. W tym roku warsztaty odbywały się równolegle w 13 salach!

Organizatorzy zaskoczyli uczestników jeszcze jedną zmianą formuły: zajęcia warsztatowe, kończące oba dni wydarzenia, miały charakter sesji pytań i odpowiedzi oraz wymiany poglądów. Były to otwarte panele dyskusyjne, podczas których specjaliści z różnych dziedzin mieli jeszcze więcej możliwości uzyskania odpowiedzi na nurtujące ich kwestie z zakresu prawa, techniki oraz praktyki wykonawczej i użytkowania systemów bezpieczeństwa w obiektach komercyjnych, przemysłowych, użyteczności publicznej, muzeach itp.

W spotkaniu wzięli udział producenci najważniejszych stosowanych w obiektach budowlanych urządzeń i systemów bezpieczeństwa, takich jak SSP, DSO, SUG, BMS, SMS, CCTV (VSS), SKD, DCIM, interkomowych i powiadamiania o zagrożeniach, systemu integrującego urządzenia przeciwpożarowe (SIUP), przyzywowych i komunikacji, kontroli rozprzestrzeniania się dymu i ciepła, sterujących oddzieleniami pożarowymi i innymi instalacjami technicznymi obiektu.

Schrack Seconet Polska w imieniu swoim oraz tegorocznych Partnerów projektu składa serdeczne podziękowania wszystkim prelegentom, uczestnikom, przedstawicielom instytucji oraz uczelni technicznych, patronom merytorycznym i medialnym.

Firma Schrack Seconet Polska zaprasza do udziału w kolejnej edycji Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego 2020. Termin IX edycji zostanie podany już w grudniu 2019 r.!

Security PWNing CONFERENCE 2019

IV edycja najbardziej technicznej konferencji z zakresu bezpieczeństwa IT „Security PWNing" miała miejsce 14-15 listopada w Warszawie. W trakcie 2-dniowego spotkania wystąpiło 24 prelegentów, których prelekcji wysłuchała rekordowa liczba uczestników, rozegrano zawody liczone do klasyfikacji generalnej CTFtime, wygłoszono serię prezentacji podczas sesji lightning talks oraz stworzono nową sieć kontaktów w ramach czasu na networking i rozmowy z prelegentami.

Ponad 450 specjalistów do spraw bezpieczeństwa IT, osób odpowiedzialnych za administrowanie sieciami i systemami IT, konsultantów i ekspertów bezpieczeństwa informacji, pracowników firm dostarczających rozwiązania w zakresie bezpieczeństwa IT oraz pasjonatów tematyki wzięło udział w wydarzeniu organizowanym przez Instytut PWN. Przewodniczącym Rady Programowej i twarzą spotkania był Gynvael Coldwind, znany programista-pasjonat z zamiłowaniem do bezpieczeństwa komputerowego i niskopoziomowych aspektów informatyki, współzałożyciel zespołu Dragon Sector, pracujący w Google jako Tech. Lead / Manager w zespole bezpieczeństwa IT.

Konferencja „Security PWNing" 2019 była okazją do wysłuchania 20 wystąpień najlepszych ekspertów cyberbezpieczeństwa z Polski i Europy. Zarówno prelegenci, jak i uczestnicy podkreślali głęboko techniczny charakter konferencji, różnorodność podejmowanych zagadnień z zachowaniem spójności programu oraz najwyższy poziom merytoryczny prelekcji. Poruszane tematy spotkały się z dużym zainteresowaniem zgromadzonych, a gorące dyskusje przenosiły się z sali konferencyjnej w kuluary.
Konferencji towarzyszyły zawody zaliczane do klasyfikacji generalnej CTFtime.
Organizatorzy nie zapomnieli także o tym, aby uczestnikom konferencji zapewnić dobrą rozrywkę – w Strefie Relaksu można było zagrać w kultowe gry na sprzęcie sprzed kilkunastu, kilkudziesięciu lat od Fundacji Dawne Komputery i Gry, stworzyć własne dzieło sztuki na cyfrowej ścianie graffiti. A wieczorem wziąć udział w networkingu i zrelaksować się na after party.

Transformacja systemów bezpieczeństwa – konieczność czy szansa? Konferencja PZP Ochrona

Zmiany legislacyjne mające wpływ na zwiększenie kosztów pracy, zatrudnianie cudzoziemców w przedsiębiorstwie oraz obecna sytuacja na rynku pracy w Polsce to tylko niektóre tematy konferencji „Transformacja systemów bezpieczeństwa – konieczność czy szansa?" zorganizowanej w listopadzie przez Polski Związek Pracodawców Ochrona we współpracy z Polską Organizacją Handlu i Dystrybucji (POHiD), Federacją Przedsiębiorców Polskich (FPP) i Polską Radą Centrów Handlowych (PRCH).

Pierwszy panel konferencji dotyczył zmian legislacyjnych w obszarze kosztów pracy i ubezpieczeń społecznych. Ten temat przybliżył Marek Kowalski, przewodniczący FPP. Tomasz Chodobski, ekspert ds. polityki zatrudnienia, w drugim panelu przedstawił problemy z zatrudnianiem cudzoziemców w przedsiębiorstwie. Z kolei Ewelina Jabłońska, występująca z ramienia Grupy Pracuj.pl, przybliżyła obecną sytuację na rynku pracy w Polsce oraz podsumowała rynek firm ochrony i wnioski płynące z analiz przeprowadzonych na podstawie danych Pracuj.pl i najnowszego badania Customer Experience wydanego przez firmę eRecruiter.
Kolejny panel dotyczył rozwoju technologii w sektorze ochrony. Rafał Łupkowski, Business Security Advisor, przedstawił nową formułę ochrony traktującą bezpieczeństwo jako proces wspierający działalność zleceniodawców opartą na świadomym i adekwatnym wykorzystaniu nowoczesnych technologii.
W następnym panelu poruszono temat alternatywy dla biznesu. Paweł Grzywa z Securitas Polska omówił czynniki mające wpływ na procesy transformacji, z uwzględnieniem aspektów związanych z przemysłem 4.0. Natomiast Krzysztof Bereza z Impel Facility Services zwrócił uwagę na zagrożenia związane ze stosowaniem źle zaprojektowanych systemów kontroli dostępu. Przedstawił też nowe możliwości w zakresie stosowania systemów samoobsługi gości w nieruchomościach komercyjnych.
Remigiusz Królikowski, niezależny ekspert w zakresie property&asset management, omówił funkcje i skale rozwoju rynku centrów handlowych wynikające z tego profilu ryzyka.
Artur Nowakowski z firmy Linc Polska przedstawił praktyczne aspekty zastosowania rozwiązania dedykowanego do mobilnych systemów dozoru wizyjnego – wieży iTower.
Podczas przerw można było odwiedzić stoisko firmy EBS.

5. urodziny Hikvision Poland

W tym roku Hikvision Poland obchodzi 5-lecie swojej działalności! W Europie marka obecna jest już od dekady.

Firma z dumą spogląda na imponujący rozwój w ciągu tych lat, przy tej okazji dziękując swoim Partnerom oraz Klientom za ich wsparcie. Urodziny nie mogłyby się odbyć bez hucznej imprezy! 7 listopada podczas Urodzinowej Gali Hikvision rozdano nagrody za promowanie i wspieranie rozwoju firmy. Wcześniej odbyła się prezentacja nowego biura zlokalizowanego w kompleksie Business Garden w Warszawie.
Oprócz utworzenia 10 lat temu centrali w Holandii i 5 lat temu biura w Polsce oddziały Hikvision pojawiły się również we Włoszech, Francji, w Hiszpanii, Niemczech, Czechach, na Węgrzech i w Rumunii. Co więcej, powstały biura sprzedaży w Finlandii, Szwecji, Portugalii i Belgii.
Mijające 5 lat to znaczący kamień milowy dla Hikvision Poland. Firma rozwinęła się na polu zarówno biznesowym, jak i personalnym, pozyskując najlepszych specjalistów. Z okazji urodzin zespół wpadł na pomysł, aby to Hikvision rozdało prezenty. W Wielkiej Urodzinowej Loterii Hikvision – w puli było aż pięć samochodów, które już znalazły swoich nowych właścicieli!
Hikvision optymistycznie patrzy w przyszłość i stawia na rozwój, by dalej utrzymywać pozycję lidera, oferować jak najlepsze, kompleksowe rozwiązania dla bezpieczeństwa nas wszystkich.

Jubileusz SASMA Europe

Swoje dziesiąte urodziny SASMA EUROPE świętowała 22 listopada br. w restauracji Kamanda Lwowska w Warszawie.

Firma założona w 2009 r. na początku świadczyła proste usługi z zakresu bezpieczeństwa biznesu na terenie kraju. Na przestrzeni 10 lat rozwinęła się na tyle, by z dumą móc pochwalić się rekomendacjami od największych światowych korporacji.
Dziś SASMA reprezentuje Polskę na arenie międzynarodowej, wykonując rocznie setki projektów dla klientów z różnych branż. Bazując na swoim doświadczeniu, stworzyła specjalistyczne oprogramowanie iSASMA przeznaczone do zarządzania bezpieczeństwem biznesu, którego uroczysta premiera miała miejsce podczas obchodów X-lecia firmy.

Urządzenia umożliwiające wykorzystanie różnych inteligentnych funkcji goszczą już na rynku od pewnego czasu, zazwyczaj jednak są to kamery stałopozycyjne w różnych obudowach.

SD8A820WA-HNF
kamera PTZ z funkcjami AI

Konstrukcję kamery Dahua SD8A-820WA-HNF oparto na nieco odmiennej koncepcji, jest ona bowiem umieszczona na głowicy obrotowej o szerokich możliwościach. Ogromny przetwornik 4/3" o rozdzielczości 4K zapewnia doskonały obraz nawet w niesprzyjających warunkach oświetleniowych, natomiast obiektyw z 20-krotnym zoomem optycznym wspierany promiennikiem IR o zasięgu 500 m pozwala na dozór rozległych obszarów.

Prezentowana kamera wspiera wiele funkcji opartych na głębokim uczeniu, m.in. autotracking czy ochronę perymetryczną, pozwalającą na skuteczne filtrowanie fałszywych alarmów wywołanych przez zwierzęta czy zmiany oświetlenia. Na pokładzie znajdziemy także algorytmy rozpoznawania twarzy. W tak zaawansowanym urządzeniu nie może zabraknąć funkcji WDR, HLC, redukcji szumów czy elektronicznej stabilizacji obrazu. To bardzo ciekawa propozycja dla wysoko zaawansowanych projektów. □

Nowym prezesem firmy Hanwha Techwin został Soon-hong Ahn. Wcześniej pełnił on funkcję szefa działu sprzedaży i marketingu oraz prezesa spółki Hanwha Techwin America.

Zmiana w Hanwha Techwin

Komentując swoje nowe stanowisko, Soon-hong Ahn powiedział: - *W minionym roku firma zbudowała solidne podstawy wzrostu jakościowego, osiągając imponujące wyniki w trzech obszarach: rozwoju sprzedaży, efektywności i inwestycji w naszą przyszłość. Udało się to przy stałym wsparciu i motywacji ze strony Grupy Hanwha. Doskonałym przykładem jest tu otwarcie nowej fabryki w Wietnamie, która pozwoliła podnieść naszą ogólnoświatową konkurencyjność dzięki poprawie wydajności produkcji.*

Soon-hong Ahn - nowy prezes Hanwha Techwin

Rok 2020 to początek nowej dekady, w której będziemy pracować nad osiągnięciem pozycji wiodącego światowego dostawcy elektronicznych systemów zabezpieczeń. Przedstawimy nowe korzyści dla naszych Klientów, dostarczając różnorodne produkty i usługi oparte na nowoczesnych technologiach wideo i inteligentnych systemach zabezpieczeń. W planach na najbliższą przyszłość mamy utrzymanie stabilnego wzrostu opartego na strategii jakości i jednoczesne wdrażanie w naszych rozwiązaniach dozoru wizyjnego istotnych technologii związanych z najważniejszymi trendami, takimi jak IoT, AI i 5G, a tym samym tworzenie szans na rozwój biznesu we współpracy z integratorami i partnerami" – dodał Soon-hong Ahn. □

OPTEX: czujki dualne dla branży parkingowej

W swoim nowym produkcie firma OPTEX wykorzystała dwie technologie: mikrofalową i ultradźwiękową, tworząc linię bardzo skutecznych czujek parkingowych. Pozwalają one uniknąć prac związanych z montażem pętli indukcyjnej oraz w znacznym stopniu usprawniają zarządzanie parkingiem.

Dostępne są dwie wersje urządzeń: OVS-01GT i OVS-01CC. Głównym zastosowaniem modelu OVS-01 GT jest zautomatyzowanie podnoszenia szlabanu. Model OVS-01CC jest przeznaczony do zliczania pojazdów poruszających się z prędkością do 60 km/godz. Jednym z możliwych zastosowań tego modelu są systemy zajętości miejsc parkingowych *(rys.)*.

Zastosowanie OVS-01CC sprawia, że kierowca wjeżdżający na teren parkingu wie, w którym sektorze znajdzie wolne miejsce. Czujki są zamontowane przy pasach ruchu przeznaczonych do wjazdu i wyjazdu.

Więcej na stronie www.optex-europe.com. □

Axis przedstawia nowe kamery PTZ

Firma Axis Communications wprowadziła na rynek nową generację kamer sieciowych z serii PTZ **AXIS Q60**. Wysokowydajne kmodele AXIS Q6075 i AXIS Q6075-E PTZ wyposażone w procesory nowej generacji, wykorzystują technologię Lightfinder 2.0. Dzięki temu mają wysoką czułość, a co za tym idzie zapewniają obraz o większej ostrości obiektów w ruchu i większym nasyceniu barw nawet w trudnych warunkach oświetleniowych.

Nowe kamery PTZ są wyposażone m.in. w cyfrowo podpisane oprogramowanie sprzętowe i funkcję bezpiecznego startu, co zapobiega modyfikacji oprogramowania i chroni przed instalacją nieautoryzowanych aplikacji.

Model przeznaczony do montażu na zewnątrz budynków ma obudowę IP66/67, NEMA 4X i IK10, dzięki czemu kamera jest odporna na pył, deszcz, śnieg i wstrząsy. Zastosowana funkcja *Arctic Temperature Control* umożliwia uruchamianie i pracę urządzenia w temperaturach od -40°C do 50°C (od -40°F do 122°F).

AXIS Q60

P5655-E

Axis Communications przedstawił również **AXIS P5655-E** – nową, ekonomiczny, wysokowydajny kamerę sieciową PTZ o szerokiej gamie zastosowań. Jest wyposażona w czuły przetwornik obrazu i technologię *Forensic WDR*, która zapewnia wyraźny obraz nawet wtedy, gdy obserwowana scena obejmuje kontrastowe ciemne i jasne partie. Dzięki *Lightfinder 2.0* kamera zapewnia lepsze nasycenie kolorów na obrazach rejestrowanych w trudnych warunkach oświetleniowych, a także ostrzejszy obraz obiektów ruchomych. Z kolei funkcja elektronicznej stabilizacji obrazu minimalizuje skutki drgań i wstrząsów.

Kamera ma także większą moc obliczeniową na potrzeby zaawansowanych funkcji analitycznych oraz cztery profile sceny (wewnątrz, na zewnątrz, prace wyjaśniające i ruch drogowy). W każdym z nich kamera automatycznie optymalizuje czas ekspozycji, balans bieli, przysłonę, ostrość, kontrast i szum odpowiednio do charakteru konkretnej sceny. Podpisane cyfrowo oprogramowanie sprzętowe i funkcja bezpiecznego startu dają pewność, że wyłącznie autoryzowane, niezmodyfikowane oprogramowanie sprzętowe będzie dopuszczone do instalacji. □

Wavestore – nowa wersja oprogramowania v6.18 już dostępna

Wavestore to producent oprogramowania typu VMS. Jego najnowsza wersja v.6.18, już dostępna, wprowadza wiele innowacyjnych funkcji, w tym nowy elastyczny wybór sposobu wyświetlania obrazu, nowe funkcje audio i dodatkowe opcje przechowywania plików. Dla użytkowników, którzy chcą uzyskać maks. funkcjonalność swojego systemu dozoru wizyjnego, są to praktyczne korzyści.

Co nowego oferuje wersja Wavestore v6.18?

- Kilka stref wyświetlania wizji.
- Od teraz w systemie Wavestore można uruchamiać 4 strefy wyświetlania obrazów na jednym komputerze klienta. Dzięki temu możliwości operatorów systemu VSS znacznie się zwiększają.
- Sieciowy system plików wizyjnych.
- Mocną stroną systemu Wavestore v6.18 jest możliwość zapisu także na serwerach zewnętrznych. Połączenie może być obecnie realizowane przez sieciowy system plików NFS.
- Dźwięk – tylko urządzenia IP.
- Do tej pory Wavestore mógł obsługiwać dwukierunkowy tor audio tylko w kamerach spełniających odpowiednie wymagania. W wersji v6.18 oprogramowanie umożliwia wysyłanie komunikatów audio nie tylko przez kamery, ale także przez głośniki IP.

VMS marki Wavestore to profesjonalne i stabilne oprogramowanie przeznaczone do zarządzania kamerami i obrazem telewizyjnym. Umożliwia integrację kamer wielu producentów w funkcjonalny system. □

Więcej na ww.linc.pl

Szklane oczy kamer

Operator warszawskiego monitoringu zauważył graficiarza. Ulicznemu Michałowi Aniołowi grozi nawet więzienie, bo pomazany Pałac Branickich to zabytek. Wandalizm – nie tylko terroryzm, bandytyzm i złodziejstwo – też mieści się wśród zagrożeń dla bezpieczeństwa, choćby dotyczył tylko urody miast i wściekłych estetów. Nasi „Banksy" – artyści street art – są kiepskiej jakości, i to jest chyba główny powód mojej irytacji – sztukę na murach bym zaakceptował. Kilkanaście lat temu napisałem informację o wynalazku powstałym w stołecznym instytucie chemii. „Antygrafitti" otrzymało nawet nagrodę na światowej wystawie wynalazków. Nie był to skomplikowany system rodem z optyki, elektroniki czy IT. Potwierdza to metoda stosowania: należało pomalować mur przezroczystym impregnatem, następnie cierpliwie przeczekać atak obcej farby i podeschnięty bohomaz przetrzeć suchą szmatą – odpadał od podłoża. Produktowi wieszczyłem sukces rynkowy, bo działał, ale cisza później krzyczała. Dzisiaj jakieś takie preparaty są w internetowych wyszukiwarkach, ale kolejka chętnych do zakupów zarządców obiektów chyba za długa nie jest, patrząc na stan elewacji. Wielu z nich nadal woli walczyć z wiatrakami artystów, których ambicje zdobywania sławy są większe od twórczych możliwości.

☼

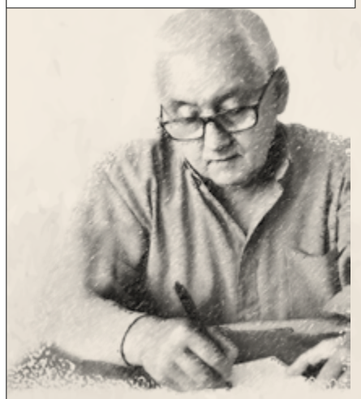
Ta informacja jest trochę zleżała – bo z końca września – i pochodzi z holenderskiego portalu „The Next Web" (własność „Financial Times"). Medium zajmuje się nowościami technologicznymi i branżowymi konferencjami. Chodzi tu o kamerę 500-megapikselową i system rozpoznawania twarzy. Jak podał chiński rządowy dziennik „Global Times" – system kamery ze sztuczną inteligencją połączonej z chmurą obliczeniową jest dziełem badaczy z Uniwersytetu Fudan w Szanghaju i Instytutu Optyki, Mechaniki Precyzyjnej i Fizyki Chińskiej Akademii Nauk w Czangczun. Powstał dla celów wojskowych i bezpieczeństwa publicznego (zadania operacyjne, strażnik na granicach, w bazach wojska i... „w bazach satelitów" (?) – w celu zapobiegania przedostania się do wewnątrz lub na zewnątrz podejrzanych osób i obiektów. W chińskich miastach – według tego serwisu – pracuje ok. 200 mln kamer, a ich liczba ma wzrosnąć w 2020 r. do ponad 620 mln (szacunek dynamiki wzrostu chyba jest mocno nierealny, ale kiedyś...). Podano, że kamera może rejestrować obraz z doskonałą dokładnością szczegółów, np. setek twarzy na stadionie, i dane przesyłać do chmury, co pozwala na natychmiastową lokalizację konkretnej osoby. Chyba znowu przesada. Chociaż technika to umożliwia, to najpierw muszą powstać bazy wizerunków twarzy do porównywania z rejestrowanymi, z biegiem czasu np. o milionowych zasobach. Przy takiej perspektywie rozwoju monitoringu widzę w innym świetle działanie internetowych przyjaznych portali społecznościowych namawiających mnie do opublikowania zdjęcia profilowego, czyli mojego portreciku z nazwiskiem.

☼

Pod koniec roku informacje się tłoczą i felieton bywa za ciasny. Kto pamięta z 2017 r. pożar 24-piętrowego budynku Grenfell Tower? Spaliło się w nim 72 mieszkańców. Koszmarnie wysoka płonąca pochodnia na tle Londynu. Teraz po audycie dochodzą informacje o błędach w akcji i systemowych zaniedbaniach, jak brak szkoleń, za mała liczba i nieprzygotowanie dyspozytorów. Pożar zaczął się od zwarcia w lodówce na czwartym piętrze. Potem było bohaterstwo strażaków, którzy próbowali się wspinać i wyciągać ludzi, i seria dużych błędów. Główny powstał przy remoncie kilkanaście miesięcy przed katastrofą, gdy ocieplono budynek materiałami łatwopalnymi. Ale nakazano także pozostać mieszkańcom w płonącym domu co najmniej o godzinę za długo, co zwiększyło liczbę ofiar. Wieżowce powinny być tak projektowane, aby ogień nie przedostawał się kolejnymi kondygnacjami. Ten budynek podobno zbudowano inaczej.

☼

Zacząłem od monitoringu wizyjnego stolicy i tematem tym skończę. Do nieistniejącego już czasopisma „Systemy Alarmowe" napisałem ponad 10 lat temu dwa duże reportaże o miejskich kamerach – Warszawa miała wtedy ponad 300 zintegrowanych w miejskiej sieci, „coś" na I linii metra, a w transporcie naziemnym ich sobie nie przypominam. Teraz w przestrzeni miasta funkcjonuje ponad 15 tys. kamer, ogromna większość w pojazdach (ok. 13 400 kamer w autobusach, tramwajach, SKM i w pociągach metra) – ponadto w infrastrukturze metra są 1084 kamery. Operatorzy zauważają rocznie ponad 7 tysięcy zdarzeń wymagających interwencji. Nie razi mnie ich zawodowe wścibstwo. □



TEKST

Andrzej Popielski

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

Kolorowy obraz w ciemności

Kamera Full-color na potrzeby systemów całodobowego dozoru

Full-color

- Przetwornik Full HD Starvis™ oraz obiektyw f/1.0 pozwalają na otrzymanie kolorowego obrazu oraz bardzo wysokiej światłoczułości, co przekłada się na lepszą jakość obrazu w każdych warunkach
- Zaawansowana technologia przetwarzania obrazu oraz filtr 3DNR redukujący szum sprawiają, że obraz jest bardziej czytelny i zajmuje mniej przestrzeni na dysku.
- Możliwość obserwacji w kolorze 24/7 znacznie ułatwia zebranie kluczowych danych dotyczących np. ludzi, pojazdów i zdarzeń.
- Doskonałe rozwiązanie do zastosowań w warunkach słabego oświetlenia, takich jak parkingi, ulice, sklepy, szkoły itp.

Polecane modele

IPC-HFW4239T-ASE

Kamera sieciowa
1080P Full-color

IPC-HDBW4239R-ASE

Kamera sieciowa
1080P Full-color

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