

TEMAT NUMERU

Inteligentne miasto
musi być przede wszystkim
bezpieczne. Jakie są miasta
przyszłości?
str. 16

Smart CITY Safe CITY

TELEWIZJA DOZOROWA

Kamery w mieście

Monitoring miejski jest częścią *smart city*. Takie zastosowanie jest możliwe dzięki *big data* i rozwiązaniom ICT.

str. 38

INTERNET RZECZY

Czy IoT w security jest bezpieczny?

Security coraz częściej idzie w parze z IoT. Jednak typowe dla Internetu Rzeczy luki w zabezpieczeniach są wykorzystywane do cyberataków.

str. 75

INTELIгентNY DOM

Trendy na rok 2017

Na naszych oczach rośnie rynek *smart home*. O dominację walczą globalni giganci. Co nam przyniesie ich pojedynek?

str. 88



NR 1 NA ŚWIECIE



innowacyjna firma



jedna z najbardziej
wartościowych
marek na świecie

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

Drodzy Czytelnicy

Przyszłość, trendy, kierunki rozwoju – te tematy najbardziej dziś interesują wszystkie branże technologiczne. Nie inaczej jest z branżą security. Sztuczna inteligencja, *deep learning*, Internet Rzeczy czy *big data* stanowią obecnie słowa-klu-
cze również naszej branżowej rzeczywistości. Wszystkie one jak w soczewce skupiają się w miastach, które coraz szybciej prą ku przyszłości, tworząc tzw. **smart cities**. Te naszpikowane nowoczesnymi technologiami organizmy mają ułatwiać mieszkańcom funkcjonowanie w coraz większych systemach, a władzom miasta i jego instytucjom – zarządzanie tymi systemami. W tym wydaniu *a&s Polska* opisujemy historię powstania i filozofię działania miasta przyszłości (s. 16), wskazując przy tym **Singapur – modelowe smart city** (s. 20) oraz **Dubaj – inteligentną metropolię w sercu pustyni** (s. 26).

Każde inteligentne miasto musi być jednocześnie bezpieczne. Dlatego w kontekście *smart city* piszemy także o **safe city**. Wyzwaniem jest zapewnienie bezpieczeństwa nie tylko mieszkańcom, ale także miejskim systemom – miasto inteligentne jest bowiem dla potencjalnych napastników celem samym w sobie (s. 30). W aspekcie bezpiecznego miasta zwracamy uwagę na systemowe zależności w **zarządzaniu systemami monitoringu wizyjnego** (s. 33) oraz rolę **kamer dozorowych w miastach** (s. 38).

Branża security coraz częściej interesuje się **rozwiązaniem IoT**. Jednak musi pamiętać o szczególnych środkach ochrony, ponieważ typowe dla Internetu Rzeczy luki w zabezpieczeniach są wykorzystywane do cyberataków (s. 75). O konsekwencjach stosowania rozwiązań IoT w urządzeniach zabezpieczeń technicznych opowiedział nam **szeef ONVIF** (s. 78). A jest się czego obawiać – routery i sieciowy sprzęt wideo to jedno z **najczęściej atakowanych urządzeń IoT** (s. 80). Wyzwania cyberbezpieczeństwa opisuje raport Orange Polska – warto zapoznać się ze statystykami **najczęstszych ataków w polskiej cyberprzestrzeni** (s. 82).

IoT i cyberbezpieczeństwo to tematy szczególnie istotne dla tzw. **inteligentnego domu**, w którym urządzenia są wzajemnie połączone (komunikują się ze sobą) w sieci. Ten rynek wymaga jeszcze wielu unormowań i wypracowania jednolitych standardów, ale już wi-
dać, że w najbliższej przyszłości będzie się rozwijał dynamicznie (s. 86). Jak bardzo *smart home* jest istotny i rojący na przyszłość może świadczyć rozpoczęta właśnie wojna czterech globalnych gigantów: Amazon, Apple, Google i Microsoft – będzie się działo... (s. 88).

Pierwszy kwartał roku był dla naszego zespołu niezwykle pracowity, nie tylko za sprawą wprowadzenia na rynek nowego tytułu *a&s Polska*, co z dumą uznajemy za sukces! Podczas naszego kolejnego **śniadania ekspertów** przedstawiciele rynku security i użytkownicy końcowi mogli swobodnie porozmawiać o bezpieczeństwie infrastruktury krytycznej (s. 8). Uczestniczyliśmy też w dziesiątkach szkoleń, konferencji i spotkań branżowych – w tym także zagranicznych na Tajwanie i w Dubaju (s. 112 i 116). Cieszymy się, że możemy **aktywnie uczestniczyć w globalnym rynku security** i opisywać go na naszych łamach.

Okazją do rozmów o światowych trendach i kierunkach rozwoju security będzie organizowany przez nas **Warsaw Security Summit**. Ta pierwsza tego typu międzynarodowa konferencja naszej branży odbędzie się 9 czerwca. Mamy nadzieję, że podobnie jak śniadania ekspertów, na stałe wpisze się w kalendarz naszej branży.

Marta Dynakowska
redaktor naczelna

Mariusz Kucharski
dyrektor zarządzający

a&s POLSKA | ŻŁOTY PARTNER



a&s POLSKA | SREBRNY PARTNER



Wydawca

a&s Polska Sp. z o.o.

Adres wydawcy i redakcji

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

Dyrektor zarządzający

Mariusz Kucharski

Redaktor naczelna

Marta Dynakowska

Dział reportażu

Andrzej Popielski

Dział marketingu i reklamy

Iwona Krawiec

Kolegium redakcyjne

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

Korekta

Jolanta Kucharska

Projekt graficzny

Sylwester Dmowski

Skład

Dorota Cybulska
Sylwester Dmowski

Prenumerata

www.aspolska.pl/prenumerata

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

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

© Copyright by a&s Polska



BOSCH
Technologia bliżej nas

Oni widzą doskonałą usługę

Zdalny Dostęp

Ty widzisz łatwy i efektywny sposób zarządzania wszystkimi zainstalowanymi systemami.

Bosch umożliwia budowanie bezpieczniejszego świata. Dzięki usłudze zdalnego dostępu oferuje trzy przełomowe rozwiązania. Doświadcz lepszej łączności, stałej dostępności na dowolnym poziomie, oraz pełnej ciągłości działania w każdym miejscu na świecie.



TEMAT NUMERU

RAPORT
STR. 16
Smart CITY
Safe CITY

SPOTKANIE
BRANŻOWE
STR. 8

ŚNIADANIE
EKSPERTÓW

INTERNET
RZECZY
STR. 75
Bezpieczeństwo IoT
– zagrożenia
i przeciwdziałanie

SPOTKANIE BRANŻOWE

- 8 Śniadanie ekspertów
- 10 Produkty numeru

SMART CITY SAFE CITY

- 16 Smart city – w poszukiwaniu miasta przyszłości
Bartosz Dominiak
- 20 Singapur – lew inteligentny
William Pao, a&s International
- 26 Spacer po smart city – Charles Trybus, Comarch
- 28 Miasta, które myślą... To naprawdę możliwe
APA
- 30 Analiza krytycznych systemów w smart city
Jerzy Mikulik
- 33 Zarządzanie systemowe w miejskim systemie monitoringu – Paweł Wittich
- 38 Kamery w miastach – Jan T. Grusznicki
- 44 Wpływ zastosowania kamer sieciowych na poprawę komfortu życia w inteligentnym mieście
Andrea Sorri, Axis Communications
- 46 IndigoVision – praktyczny system monitoringu miejskiego – Miwi Urmet
- 48 Bezpieczne miasta i obiekty biurowe
Marcin Ruciński, Hanwha Techwin Europe
- 50 AxxonSoft – VMS dla smart cities
Michał Przybylski, AxxonSoft Polska
- 52 Miasto w panoramie
Dominika Majsterek, Hikvision Poland
- 53 Nie tylko bezpieczeństwo. Monitoring miasta Karpacz
Dagmara Dąbrowska, CBC Poland
- 54 BCS Manager – wszystko w jednym
Marcin Morzyk, BCS
- 56 QVR Pro – profesjonalny system dozoru wizyjnego na serwerze NAS
QNAP
- 58 Sztuczna inteligencja na usługach systemów zabezpieczeń
Mateusz Zapotoczny, Dahua Technology Poland
- 59 Modelowe zarządzanie kryzysowe
Marek Okularczyk, IBM
- 60 Parkuj inteligentnie w erze IoT
William Pao, a&s International
- 64 Głos branży – bezpieczne miasto

BEZPIECZNE OBIEKTY BIUROWE

- 68 Bezpieczeństwo pożarowe obiektów biurowych
Grzegorz Cwiek, Schrack Seconet Polska
- 70 Ciągłość zasilania urządzeń ppoż. w zapewnieniu bezpieczeństwa pożarowego obiektów biurowych – Edward Skiepcio

INTERNET RZECZY

- 75 Bezpieczeństwo IoT – zagrożenia i przeciwdziałanie im
SMAhome, a&s International
- 78 Internet Rzeczy i jego konsekwencje dla branży zabezpieczeń technicznych
Rozmowa z Perem Björkdahlem, przewodniczącym ONVIF
- 80 Routery i sieciowy sprzęt wideo najczęściej atakowanymi urządzeniami IoT – Fortinet
- 82 Cyberbezpieczeństwo – wyzwania i zagrożenia w 2017 roku – Orange Polska
- 86 Boom na rynku IoT i inteligentnego domu – potrzeba standaryzacji – a&s International
- 88 Inteligentny dom – trendy w 2017 roku
a&s International

BEZPIECZEŃSTWO BIZNESU

- 94 Nasze dane; e-społeczność a problem ochrony danych wrażliwych. Rozwój przestępczości w obszarze danych osobowych cz. 3
Marek Blim
- 98 Nie daj się podsłuchać
Sebastian Błażkiewicz
- 100 Incydenty wybuchowe w obszarach miejskich
Tomasz Goleniowski

OCHRONA INFORMACJI
NIEJAWNYCH

- 102 Spóźniona nowelizacja – Marek Ryszkowski

FORUM/OPINIE

- 106 Polskie Normy po polsku – Jerzy W. Sobstel
- 109 Monitoring wizyjny w szkołach: potrzebne są lepsze regulacje – Paweł Wittich

SERWIS INFORMACYJNY

- 112 20. edycja targów: Secutech Taipei 2017
- 115 Premiera systemu NAZCA na największych targach przemysłowych na świecie – APA

FELIETON O BEZPIECZEŃSTWIE

- 123 Estetyczny faraon, czyli renesans murów
Andrzej Popielski

RAPORT

INTERNET
RZECZY
STR. 86

Boom na rynku IoT
i inteligentnego domu
niezbędna standaryzacja

SMART/SAFE
CITY
STR. 60

Parkuj inteligentnie
W ERZE INTERNETU RZECZY

SERWIS
INFORMACYJNY
STR. 112

Secutech
Taipei 2017

ŚNIADANIE EKSPERTÓW

Bezpieczeństwo infrastruktury krytycznej

W obliczu przemian społeczno-politycznych i zagrożeń terrorystycznych to temat niezwykle istotny. O problemach związanych z zabezpieczaniem obiektów infrastruktury krytycznej rozmawiali uczestnicy drugiego śniadania ekspertów „a&s Polska”.

Spotkanie odbyło się tradycyjnie w piątkowy poranek (12 maja) w warszawskim hotelu Westin. Dyskusję przy wspólnym stole prowadzili przedstawiciele producentów i dystrybutorów firm z rynku security oraz specjaliści i security managerowie firm i instytucji – operatorów infrastruktury krytycznej. To już drugie tego typu spotkanie w branży zabezpieczeń – kolejny raz spotkało się z entuzjastycznym przyjęciem uczestników, o czym może świadczyć duża frekwencja oraz burzliwa i inspirująca dyskusja.



Film ze spotkania na:
www.aspolska.pl/śniadanie-ik



Witold Skomra
Rządowe Centrum
Bezpieczeństwa

Trzeba przyznać organizatorom, że świetnie trafili z tematyką i składem dzisiejszego spotkania. To była bardzo rzadka okazja do wymiany doświadczeń – co najnowszego dzieje się w zakresie techniki, co się dzieje w przepisach prawa, w którą stronę idziemy i jak bezpieczeństwo będzie postrzegane za kilka miesięcy czy za kilka lat. Rzadko mamy taką możliwość.



Jest wiele do zrobienia – zmienia się otaczający nas świat, więc musimy nadążać za tymi zmianami. To, co jest dobre w dziedzinie bezpieczeństwa dzisiaj, nie musi być odpowiednie w przyszłości. To jest ciągły proces, a my musimy się wciąż doskonalić i dotrzymywać tempa tym zmianom.

Janusz Syrówka
innogy Polska



Harald Dingemans
Linc Polska



Jestem bardzo zadowolony ze spotkania. Tym razem weszliśmy znacznie głębiej w temat, było też więcej dyskusji i interakcji. Wychodzimy ze śniadania z cennymi refleksjami – zarówno my, dystrybutorzy i producenci, jak i użytkownicy końcowi czy strona rządowa.

Grzegorz Ćwiek
Schrack Seconet Polska



Cieszę się, że mieliśmy do czynienia z jeszcze większym gronem ekspertów, interdyscyplinarnymi wypowiedziami i zainteresowaniami. To poszerza horyzonty i buduje całą sieć powiązań, dobrych pomysłów na rozwój systemów bezpieczeństwa. Dobry kierunek!



Jacek Grzechowiak
Securitas Polska

Świetne spotkanie i duża wartość merytoryczna... Bardzo ciekawa dyskusja ze specjalistami branżowymi i przedstawicielami Rządowego Centrum Bezpieczeństwa. Bezpieczeństwo jest częścią zarządzania ryzykiem i w większości podmiotów to wyraźnie widać, zwłaszcza tam, gdzie są dobrzy security lub risk menedżerowie.



Mateusz Zapotoczny
Dahua Technology
Poland

Podczas spotkania padło zdanie, że stworzymy systemy na miarę Formuły 1, a sadzamy za kierownicą osobę z kartą rowerową. Też to zaobserwowaliśmy, dlatego przygotowujemy aktualnie kurs kierowcy F1 dla wszystkich zainteresowanych.



Jan Grusznicki
Axis
Communications

Rewelacyjna dyskusja. Wyciągnięcie wniosków po pierwszym spotkaniu zaowocowało bardzo ciekawą dyskusją dającą mi osobiście bardzo dużą wiedzę o oczekiwaniach klientów końcowych. Zdecydowanie polecam! Widać bardzo dobre kontakty i pole do współpracy.

Dzięki tej formie spotkania uczestnicy wypowiadają się w sposób mniej skrepowany, więcej można się dowiedzieć – mówią swobodnie o rzeczach ważnych, o których wcześniej być może słyszeliśmy, ale nie tak szczerze i życiowo jak tutaj.

Tomasz Goljaszewski
Hikvision Poland

Spotkanie bardzo dobitnie pokazało różne spojrzenia na problemy związane z bezpieczeństwem w infrastrukturze krytycznej – nie tylko w zakresie produktów, systemów czy rozwiązań, ale także procedur zarządzania ryzykiem czy innych kwestii, które nam, producentom, często umykają. Przekonaliśmy się jednak, że są one kluczowe dla klientów końcowych.

Michał Borzucki
Bosch Security Systems



Kolejny raz miałem możliwość wzięcia udziału w spotkaniu, podczas którego grupa ludzi rozmawia o bezpieczeństwie z różnych perspektyw: producenta, integratora i użytkownika. I kolejny raz przekonałem się o tym, że takie spotkania są niezbędne.

Sławomir Szlufik
Hanwha Techwin



Krzysztof Pohorecki
Polski Holding Obronny

Największym wyzwaniem jest niewystarczająca wiedza na poziomie decyzyjnym – zarządu, rady nadzorczej, osób decyzyjnych. Nad właściwym ułożeniem struktur bezpieczeństwa jest jeszcze ogromna praca do wykonania – temu służą m.in. takie spotkania.



Jacek Wójcik
Optex Security



Seria AXIS P13 - znakomity obraz 4K i 5 Mpix w dowolnych warunkach oświetleniowych



Axis Communications
www.axis.com/pl

Kamery sieciowe AXIS P1367 (do zastosowań wewnętrznych) oraz AXIS P1367-E i AXIS P1368-E (do zastosowań zewnętrznych) uzupełniają uznaną serię kamer stałopozycyjnych AXIS P13. Doskonale sprawdzą się w miejskim monitoringu wizyjnym, transporcie i sektorze handlu detalicznego. Dzięki lepszej czułości i jakości obrazu oraz wyższej częstotliwości odświeżania kamery dostarczają obraz 4K również z rozległych, otwartych przestrzeni przy wymagających warunkach oświetleniowych (hale dworcowe zatłoczone centra miast, parkingi). Model AXIS P1367/E umożliwia stosowanie obiektywów z mocowaniem typu CS oraz iCS. 4K AXIS P1368-E jest natomiast dostarczana standardowo z obiektywem i-CS. Obie skonstruowano ze szczególnym uwzględnieniem zastosowań zewnętrznych. Innowacyjna platforma mechaniczna ułatwia dostęp do złączy i okablowania i zapewnia więcej miejsca na opcjonalne obiektywy. Wbudowane szyny kamer zwiększają funkcjonalność, umożliwiając instalację większych obiektywów zoom. *Nie są to po prostu kamery w obudowie. Kamery do zastosowań zewnętrznych z mocowaniem CS opracowaliśmy całkowicie od podstaw. Uzyskaliśmy funkcjonalny system, w którym można zastosować obiektywy zoom, a nawet funkcję Axis Corridor Format, gdy istnieje potrzeba uzyskania obrazu w orientacji pionowej* – ocenia Andres Vigen, Global Product Manager ds. kamer stałopozycyjnych w Axis Communications. Nowe modele będą dostępne do końca czerwca. ■■

Rejestrator BCS-P-NVR12816-4KR wyświetlanie na 14 monitorach



BCS
www.bscctv.pl

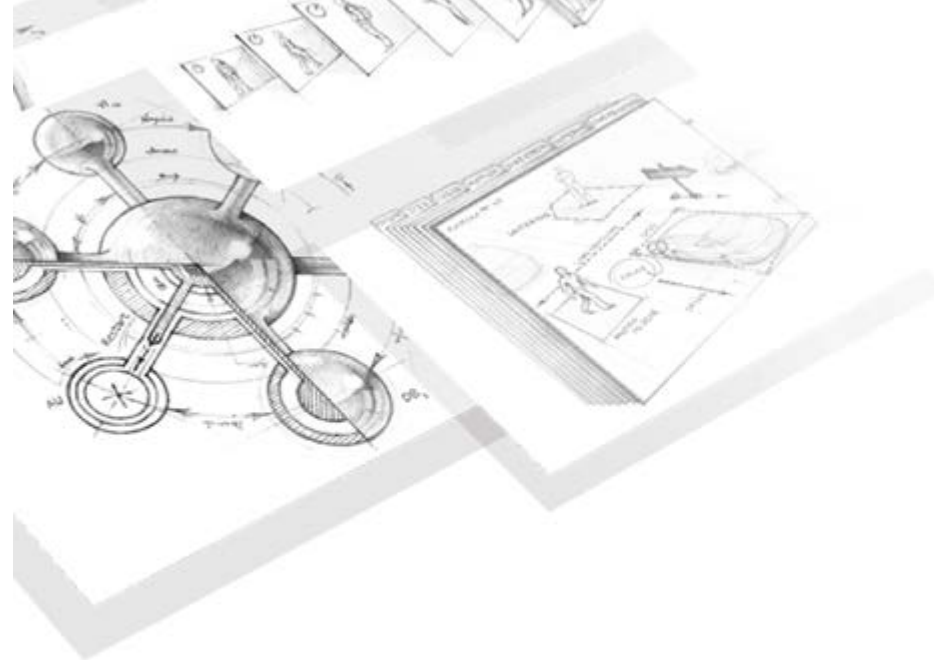
BCS-NVR-P-12816-4KR jest najnowszym modelem w szerokiej gamie rejestratorów. Może zapisywać strumień ze 128 kamer jednocześnie, gdzie *bitrate* wejściowy dla rejestratora wynosi 384 Mb/s, a maksymalna rozdzielczość kamer to 12 Mpix. Strumienie te zapisywane są na 16 dyskach montowanych w rejestratorze, które instaluje się poprzez zdejmowany przedni panel. Podczas pracy urządzenia przestrzeń dyskową można przeorganizować tak, aby dyski pracowały w RAID 1 lub RAID 5, co zwiększa bezpieczeństwo archiwum. Jeżeli któryś z dysków w rejestratorze ulegnie awarii, kontroler *Hot Swap* pozwoli wymienić dysk, nie wyłączając całego urządzenia. Rejestrator BCS-P-NVR12816-4KR może również znaleźć zastosowanie w rozbudowie istniejących instalacji. Można do niego podłączyć zdalne kanały z istniejących urządzeń BCS (również analogowych i HDCVI) tak, aby najważniejsze punkty kamerowe były doprowadzone do jednego miejsca. Pozwala to na oglądanie obrazów z wybranych kamer systemu dozoru z dowolnego miejsca na jednym rejestratorze NVR. Tego typu rozwiązanie umożliwia również dublowanie nagrań z niewrażliwych miejsc zabezpieczanego obiektu. Wyświetlanie wszystkich kamer możliwe jest na 14 monitorach, które można podłączyć bezpośrednio do rejestratora (dwa mogą być o rozdzielczości 4K). Każdy z monitorów może być konfigurowany osobno i na każdym mogą być wyświetlane obrazy z dowolnych kamer systemu. ■■

Kamera DH-HAC-HF3805G w standardzie HDCVI 4.0



Dahua Technology
www.dahuasecurity.com/pl

Historia miejskich systemów monitoringu wizyjnego w Polsce liczy już kilkadziesiąt lat. Mieliśmy okazję obserwować rozwój magnetowidów i ich odejście do lamusa, bezprecedensowy rozwój kamer analogowych, następnie szybkie rozpowszechnienie systemów sieciowych, które były jedynym wyborem, gdy konieczna była wysoka rozdzielczość obrazów. To już przeszłość. Wraz z wprowadzeniem przez Dahua Technology standardu HDCVI 4.0 sytuacja się zmieniła. Przykładem jest innowacyjna kamera DH-HAC-HF3805G wyposażona w przetwornik o rozmiarze 4/3" ze skanowaniem progresywnym o niespotykanej w systemach analogowych rozdzielczości 8 Mpix. Kolejną unikatową cechą jest system mocowania obiektywów: zdecydowano się na zastosowanie znanego od lat standardu M43. Połączenie dużego sensora, „jasnej” optyki oraz technologii Starlight zapewnia uzyskanie doskonałego obrazu nawet przy znikomym poziomie oświetlenia. Aby podobne efekty uzyskać w sytuacji mocnego i kontrastowego światła, kamera wykorzystuje funkcję Ultra WDR 140 dB. DH-HAC3805G realizuje podstawowe założenia standardu HDCVI, umożliwiając przesył przewodem koncentrycznym czterech sygnałów, tj. obrazu, dźwięku, danych i zasilania. Uzupełniając charakterystykę tego modelu o funkcje inteligentnej analizy, możliwość bezstratnej transmisji sygnału przewodem koncentrycznym na odległość do 700 m czy wykorzystanie zaawansowanych algorytmów redukcji szumów, dostajemy produkt unikatowy i w zasadzie kompletny. Przyszłość jest teraz. ■■



OTWARTA PLATFORMA INTEGRUJĄCA
SYSTEMY BEZPIECZEŃSTWA

AxxonSoft Polska Sp. z o.o.
ul. Olszańska 5H
31-513 Kraków

Tel.: +48 12 393 58 01
E-mail: poland@axxonsoft.com
www.axxonsoft.com/pl

Kamera panoramiczna PanoVu 180°



Hikvision
www.hikvision.com

Wymagania klientów dotyczące uzyskania coraz bardziej szczegółowego obrazu dużego obszaru z kamer dozorowych stale rosną. Jednocześnie oczekuje się rozwiązań ekonomicznych oraz ograniczenia ilości sygnałów wizyjnych docierających do centrum dozoru i potrzebnych licencji kamerowych. Inwestorzy coraz częściej decydują się więc na stosowanie multisensorycznych rozwiązań panoramicznych. DS-2CD6A64F-IHS/NFC jest najnowszym modelem kamery panoramicznej o polu widzenia 180°. Strumień wideo o rozdzielczości 24 Mpix (8208 x 3072) jest złożony z obrazów z czterech 6-Mpix przetworników CMOS o średnicy 1/1,8". Dzięki wysokiej czułości przetworników oraz dużemu zagęszczeniu pikseli na metr kamera generuje obraz o wysokiej szczegółowości. Mimo dużego pola widzenia można odczytać tablicę rejestracyjną pojazdu nawet z odległości 20 m. Kamery wyposażono w wydajny promiennik IR o zasięgu 50 m obejmujący kąt 180°. Tak jak we wszystkich modelach z nowej linii PanoVu, zastosowano w niej superwydajną kompresję obrazu H.265+, funkcje WDR i HLC oraz zaawansowaną analizę obrazu. Zaimplementowano też wspieraną z poziomu rejestratora funkcję śledzenia obiektów, które można wyodrębnić z obrazu panoramicznego i wyświetlić w oddzielnych oknach podglądu na żywo w zadanej wielkości powiększenia cyfrowego. Oprócz wbudowanego interfejsu kamera została wyposażona w złącze światłowodowe. ■

Ochrona perymetryczna FFT Security

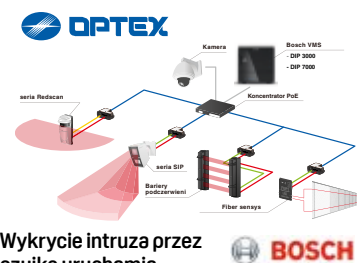


Linc Polska Sp. z o.o.
www.linc.pl

Systemy marki FFT Security zostały zaprojektowane z wykorzystaniem technologii światłowodowej. Działają doskonale o każdej porze roku, niezależnie od temperatury i warunków atmosferycznych. Odporność światłowodów na zakłócenia elektromagnetyczne, a jednocześnie czułość na drgania, hałas i ruch sprawiają, że system ochrony FFT jest niezwykle precyzyjny i skuteczny. Jego działanie polega na detekcji zakłóceń światła lasera wysyłanego z nadajnika i wykrycie zagrożenia. Przewód można zawiesić na ogrodzeniu, a także zakopać w ziemi, otaczając chroniony obszar. Systemy FFT oferują:

- daleki zasięg – ochrona perymetryczna do 80 km,
- lokalizację zdarzenia – określenie z maks. dokładnością miejsca zakłócenia/wtargnięcia,
- inteligentną analizę – rozróżnianie między faktycznym wtargnięciem a naturalnym zakłóceniem spowodowanym przez wiatr, deszcz, ruch uliczny czy pracę maszyn lub samolotów,
- niskie koszty instalacji i użytkowania – światłowód nie wymaga zasilania ani dodatkowej „elektroniki”,
- bezpieczeństwo i niezawodność – stabilne działanie, odporność na EMI, RFI i wyładowania atmosferyczne,
- integrację – oprogramowanie CAMS pozwala na integrację z urządzeniami firm trzecich. Produkty marki FFT zostały zaprojektowane z myślą o ochronie perymetrycznej rozległych terenów, takich jak granice państw, elektrownie, fabryki, lotniska itp. Ich głównym zadaniem jest ochrona przed atakami terrorystycznymi, szpiegostwem, kradzieżą czy próbami podkopów. Urządzenia zostały pozytywnie przetestowane przez światowe instytucje wojskowe, rządowe, energetyczne, transportowe, przemysłu i wiele innych. ■

Integracja czujek ruchu REDWALL-IP z rejestratorami Bosch DIP 3000 i DIP 7000



Wykrycie intruza przez czujkę uruchamia scenariusz w rejestratorze Bosch

OPTEX Security
www.optex.com.pl

Czujki zewnętrzne REDWALL-IP firmy Optex zyskały na funkcjonalności. System detektorów obejmujący zewnętrzne czujki dalekiego zasięgu REDWALL, laserowe czujki REDSCAN, napłotowy system światłowodowy RAPID REDFIBER oraz aktywne bariery podczerwieni REDBEAM można teraz wykorzystać w systemach dozoru wizyjnego IP firmy Bosch. Oprogramowanie urządzeń dozoru wizyjnego Bosch DIP 3000 i DIP 7000 oraz BVMS Professional Edition 7.0 zostało rozszerzone o protokół komunikacyjny REDWALL Event Code. Umożliwia to tworzenie scenariuszy działania, w których sygnał alarmowy TCP lub UDP z czujki kieruje kamerą do presetu lub rozpoczyna scenariusz nagrywania. Ponadto informacje o detektorze OPTEX będą przechowywane w BVMS i mogą być wykorzystane jako dane w celu łatwego odnalezienia odpowiadających im zdarzeń z zarejestrowanych materiałów wideo. Ta integracja Optex-Bosch zapewnia rozwiązanie dostosowane do potrzeb niemal każdego scenariusza naruszenia. Połączenie detekcji ruchu w kamerze z zewnętrzną czujką ruchu pozwala zmniejszyć liczbę fałszywych alarmów wywoływanych przez zmiany oświetlenia, opady atmosferyczne czy owady. Ma to znaczenie szczególnie w rozbudowanych systemach, w których operator musi reagować na sygnały z wielu źródeł. Informacje na temat czujek REDWALL-IP oraz współpracujących z nimi urządzeń Bosch można uzyskać pod adresem optex@optex.com.pl ■

My nie idziemy drogą, my ją wytyczamy



Linc

Polska Sp. z o.o.

www.linc.pl



Pracuj z najlepszymi!



Nowoczesność i bezpieczeństwo

Pyronix PCX 46 APP System alarmowy łączący tradycję z IP



Pyronix
www.pyronix.com

PCX46 APP to profesjonalny system alarmowy umożliwiający adaptację i rozbudowę systemu bezprzewodowego. Rozwiązanie zapewnia wysoki poziom zabezpieczenia, wygodę i elastyczność instalacji oraz obsługi.

Zdalne programowanie i diagnozowanie pracy systemu za pomocą oprogramowania InSite UDL za pośrednictwem firmowej chmury PyronixCloud przyczynia się do zmniejszenia liczby zgłoszeń do instalatora, redukując tym samym koszty eksploatacji. Dzięki chmurze PyronixCloud również początkowa instalacja jest bardziej efektywna i elastyczna, liczba dostępnych urządzeń peryferyjnych Pyronix natomiast umożliwia instalatorowi dostosowanie instalacji do perfekcji.

Użytkownicy mają pewność, że kupią doskonały system alarmowy, który może zaspokoić indywidualne potrzeby ochrony ich własności i łatwą rozbudowę. Wykorzystanie urządzeń przewodowych i bezprzewodowych sprawia, że system jest mniej inwazyjny podczas instalacji.

Kluczowym aspektem jest aplikacja HomeControl+, która daje użytkownikom pełną kontrolę nad systemem w dowolnym miejscu na świecie: uzbrojenie i rozbrojenie, sterowanie wyjściami automatyki, sprawdzanie stanu każdego urządzenia w systemie i wiele innych. ■

Inteligentne rozwiązania IP Schrack Seconet



Schrack Seconet Polska
www.schrack-seconet.pl

SecoLOG IP – Graficzny system wizualizacji i zarządzania, zgodnie z ON F 3003, umożliwia stosowanie wielu stacji roboczych do prostej, scentralizowanej obsługi i nadzoru systemów sygnalizacji pożarowej.

RemoteMESSAGE – Oprogramowanie przeznaczone do centralnego nadzoru i wskazywania stanów systemowych (alarmów, uszkodzeń itp.) dla jednej lub wielu instalacji sygnalizacji poż. W połączeniu z aplikacją panelu obsługi Integral VirtualMAP umożliwia wyświetlanie zdarzeń i zdalną obsługę systemu sygn. poż.

Integral ApplicationCenter IAC – Narzędzie serwisowe do programowania i konfigurowania produktów z rodziny Integral IP.

IACmobile – Mobilny panel zarządzania systemem Integral IP, który umożliwia wskazywanie stanów pracy i obsługę systemu sygnalizacji pożarowej Integral IP za pomocą smartfona lub tabletu.

Integral MAIL – System, który za pomocą wiadomości e-mail przekazuje informacje o zdarzeniach w systemie sygnalizacji pożarowej.

Internetowa platforma usługowa – Platforma internetowa umożliwiająca dostęp do systemów Integral IP z dowolnego miejsca na świecie za pomocą komputera PC lub urządzenia mobilnego. Zasyfrowane połączenie spełnia najnowsze standardy bezpieczeństwa. ■

Switch PoE IPB-5-10-S4



ATTE Power
www.atte.pl

Switch PoE do 5 kamer IP IPB-5-10-S4 został zaprojektowany jako kompletne, zintegrowane rozwiązanie zasilania niewielkich systemów telewizji dozorowej IP. Urządzenie jest gotowe do montażu zaraz po wyjęciu z pudełka, a obudowa o klasie ochrony IP55 daje swobodę montażu wewnątrz lub na zewnątrz budynku. Wysokiej jakości tworzywo sztuczne jest odporne na promieniowanie UV i niekorzystne czynniki atmosferyczne. Niezarządzalne switchy serii IPB są przeznaczone do współpracy z kamerami IP oraz innymi urządzeniami sieciowymi PoE 802.3at/af oraz PoE PASSIVE. Łatwa rozbudowa obsługi do 10 kamer poprzez dołączenie dodatkowego modułu switcha XPOE-6-11-S3.

Najważniejsze cechy i funkcje:

- niewielkie rozmiary;
- możliwość zasilania 5 odbiorników PoE 802.3at/af lub PASSIVE;
- bezpiecznik polimerowy niezależnie dla każdego kanału PoE;
- możliwość wyłączenia zasilania na wybranych portach PoE;
- wyraźna optyczna sygnalizacja stanu zasilania oraz transmisji danych;
- do 36 W mocy na portach PoE;
- łatwe i szybkie uruchomienie bez konieczności konfiguracji parametrów;
- wysoka sprawność zintegrowanego zasilacza (>90%);
- dodatkowe złącze śrubowe ułatwia „podebranie” zasilania 48 VDC do innych urządzeń;
- „wypinane” złącze zasilania AC ułatwia serwis urządzenia;
- możliwość zachowania zapasu kabli wewnątrz obudowy;
- w komplecie kabel zasilający oraz dwa uchwyty umożliwiające montaż obudowy, bez naruszania jej stopnia ochrony IP55. ■

RLS-3060 - laserowa czujka skanująca:

- Zasilanie PoE, komunikacja IP
- Możliwość pracy w pionie i w poziomie
- Łatwa integracja IP z najważniejszymi platformami VMS



POE
Power over Ethernet

Więcej informacji na www.optex-vms.com

s m a r t c i t y

w poszukiwaniu miasta przyszłości

Od kilku lat rosnącą popularnością cieszy się pojęcie *smart city* – inteligentne miasto. Choć do opisu współczesnych metropolii używa się również innych określeń (*digital city, future city, sustainable city, magnetic city, happy city*), to jednak zwrot *smart* zyskał prymat.

BIO

Bartosz Dominiak

Autor jest ekspertem ds. *smart city* oraz twórcą Smart City Blog, autorskiego projektu poświęconego inteligentnym miastom w Polsce i na świecie.

Bartosz Dominiak

Miasta nigdy w swojej historii nie doświadczały tak dynamicznych zmian, jakie obserwujemy w ostatnich kilku dekadach. Spotkały się dwa megatrendy, które – niemal na naszych oczach – zmieniają miejski krajobraz. Na trwający od ponad pół wieku proces wzrostu liczby ludności żyjącej w miastach nałożyła się cyfrowa rewolucja ostatnich kilkunastu lat. W takiej sytuacji zrodziła się koncepcja *smart city* – miasta, które ma być pomysłem na nowe wyzwania i problemy miejskiego życia.

Niebawem 2/3 ludzkości będzie mieszkać w miastach. Rośnie nie tylko liczba osób. Globalnym wyzwaniem staje się przy tym zagęszczenie ludności na stosunkowo niewielkich obszarach. Aż 1/8 wszystkich mieszkańców miast na świecie żyje w tzw. 31 megamiastach, każde o populacji ponad 10 mln. W 2030 r. takich miast będzie już 41. Coraz większa populacja mieszkańców aglomeracji miejskich jest przyczyną kumulowania się dotychczasowych i pojawiania nowych problemów. Wzrost zapotrzebowania na energię i wodę, lawinowy wzrost zanieczyszczeń ciekłych i stałych, zanieczyszczenie powietrza, brak mieszkań, utrudniony dostęp do podstawowych usług: żywności, edukacji, ochrony zdrowia, kultury. Skutkiem wzrostu liczby mieszkańców jest też rozlewanie się miast (*urban sprawl*), czyli proces poszerzania obszarów miejskich o tereny dotychczas słabiej zurbanizowane, ale coraz bardziej oddalone od centrum aglomeracji. Powoduje to coraz większe kłopoty z transportem i komunikacją. Pojawiają się dzielnice biedy, a także wzrasta przestępczość.

Nowe technologie w służbie miast

Ostatnie dwie dekady to czas rewolucji cyfrowej. Jej efektem jest powszechna dostępność nowych technologii. Niemal każde urządzenie, czy to używane na co

dzień, czy stosowane w infrastrukturze, jest pewną formą komputera, często już podłączonego do sieci tworzącej Internet Rzeczy (IoT).

Stwarza to niespotykane dotychczas możliwości wprowadzania zmian w funkcjonowaniu miast. Wszechobecne komputery i czujniki są źródłem gigantycznej ilości precyzyjnych danych (*Big Data*) nie tylko o tym, jak działa miejska infrastruktura, ale przede wszystkim o zachowaniach mieszkańców. Ta wiedza, uzupełniona o inteligentne oprogramowanie i wykorzystanie skomplikowanych algorytmów, pozwala efektywniej zarządzać zasobami. Wiele procesów może być wykonywanych automatycznie i na bieżąco. Słyszac zwrot *smart city*, oczami wyobraźni widzimy miasto naszpikowane nowoczesnymi technologiami i wszechobecnymi komputerami. Jednak takie podejście jest pewnym uproszczeniem, w rzeczywistości bowiem miasto aspirujące do bycia inteligentnym to znacznie więcej niż technologie.

Smart city niejedno ma imię

Smart city to miasto, które w sposób świadomy, kompleksowy i zaplanowany dokonuje w swoim funkcjonowaniu transformacji, związanej z możliwościami, jakich dostarcza sektor teleinformatyki (ICT – *Information and Communication Technology*). Jednak inteligentne technologie, *Big Data*, IoT i czujniki to zdecydowanie za mało. Ważny jest cel ich stosowania – zapewnienie zrównoważonego rozwoju miasta przy jednoczesnym podnoszeniu standardu życia wszystkich jego mieszkańców.

Większość miast na świecie ma aspiracje do stania się *smart* i – mniej lub bardziej świadomie – stosuje rozwiązania, które przybliżają je do tego celu. Wzorzec *smart city* jednak nie istnieje, nie ma listy cech, których spełnienie spowoduje, że dane miasto jest już *smart*. Każde ma inne problemy, oczekiwania mieszkańców, odmienne uwarunkowania i możliwości rozwoju.

Mimo że koncepcja inteligentnego miasta jest stosunkowo młoda, to przeszła sporą ewolucję. Dzisiejszy pomysł na *smart city* jest inny niż dekadę temu. Opisał to Boyd Cohen z Universidad del Desarrollo w Santiago de Chile, badacz tematyki *smart city* na świecie. Jego zdaniem mamy do czynienia z trzema generacjami inteligentnych miast:

Smart City 1.0 – to inteligentne miasta, w których technologie dominują nawet tam, gdzie niekoniecznie są potrzebne. Skrajnym przykładem są miasta, których celem było stworzenie idealnych miast przyszłości zaprojektowane jako technologiczne eksperymenty, np. Masdar w Zjednoczonych Emiratach Arabskich oraz Songdo w Korei Południowej. Dziś są raczej przedmiotem krytyki, gdyż brakuje w nich najważniejszego – życia mieszkańców. W mniej skrajnej wersji pierwsza generacja *smart city* oznacza miasta, w których inicjatorami wykorzystywania technologii są firmy sektora ICT. Ich motywacje są różne: jedne mają gotowe technologie, które chcą sprzedać władzom lokalnym, inne traktują miasto jako miejsce testowania nowych rozwiązań, które później oferują odbiorcom komercyjnym. Nie przykładają się nadmiernej wagi do tego, czy dane technologie są rzeczywiście potrzebne. Zachowanie władz miasta w tym modelu Cohen porównuje do fanów nowoczesnych gadżetów elektronicznych.

Smart City 2.0 – to dziś zdecydowanie najbardziej rozpowszechniona forma. Oznacza wdrażanie przez miasta dużej liczby projektów i programów związanych z zastosowaniem rozwiązań technologicznych: publiczne sieci Wi-Fi, inteligentne systemy sterowania ruchem, wszechobecne sensory, liczniki i korzystanie z *Big Data*. Stosowanie technologii wynika z poszukiwania rozwiązań do zdiagnozowanych problemów. Jest to świadome i selektywne korzystanie z tego, co mają do zaoferowania firmy technologiczne.

Smart City 3.0 – to forma inteligentnych miast, która pojawiła się 3–4 lata temu. Oznacza otwarcie się miejskich decydentów na aktywną postawę mieszkańców w budowaniu inteligentnych miast. Władze lokalne nie tylko inwestują w technologie, ale przede wszystkim tworzą przestrzeń do wykorzy-

stania potencjału obywateli. Ważne stają się zagadnienia związane z jakością życia: przyjazne otoczenie, zieleń, czyste powietrze, wyeliminowanie hałasu, bezpieczeństwo. Jako przykłady pionierów Smart City 3.0 Cohen wskazuje Wiedeń, Vancouver, Barcelonę, Amsterdam, Medellín czy Seul.

Inteligentni mieszkańcy

Eurocities, organizacja skupiająca ponad 100 miast europejskich, stwierdziła, że wszystkie miasta aspirujące do bycia *smart* łączą chęć włączania w ten proces mieszkańców. Nie ma inteligentnego miasta bez inteligentnych obywateli (*smart citizens*). W takiej sytuacji tracą znaczenie tradycyjne mierniki opisujące rozwój metropolii: wysokość budżetu, wartość inwestycji, PKB, średnia pensja. Pierwszoplanową rolę odgrywają trudne do zdefiniowania, zmierzania i porównania odczucia mieszkańców, czyli poczucie szczęścia, zadowolenie z życia w danym mieście, akceptacja przez otoczenie.

Dlaczego rola mieszkańców w inteligentnych miastach rośnie? Wspomniana wcześniej łatwość dostępu do nowych technologii wytworzyła ogólnoświatowy trend znany pod pojęciem *sharing economy* (ekonomia współdzielenia). Powszechny dostęp do Internetu (szczególnie w wersji mobilnej, na smartfonach), błyskawiczna wymiana informacji poprzez media społecznościowe (bez zbędnych pośredników) czy rosnące kompetencje cyfrowe mieszkańców wzmacniają pozycję klientów, będących dziś dominującą stroną w relacjach nabywca–sprzedawca.

Ten trend znajduje odzwierciedlenie również w relacjach władz miasta z mieszkańcami. Kiedyś sprowadzały się one, w uproszczeniu, do wrzucenia karty do urny wyborczej raz na cztery lata. Dziś mieszkańcy są codziennym uczestnikiem procesów decyzyjnych. Są dobrze zorganizowani, mają niemal nieograniczony dostęp do informacji, potrafią walczyć o swoje potrzeby i nagłaśniać niezadowolone z decyzji władz. Nierzadko biorą sprawy w swoje ręce, co w Polsce znalazło wyraz w tzw. ruchach miejskich aktywnie uczestniczących w wyborach lokalnych. W efekcie zmieniają się priorytety miast:

odchodzenie od spektakularnych i drogiej projektów inwestycyjnych na rzecz projektów małych i lokalnych, rozwiązujących konkretne problemy mieszkańców i podnoszących jakość życia w mieście.

Smart city na świecie

Obecnie na świecie realizuje się tysiące projektów z obszaru inteligentnego miasta. Choć zazwyczaj są one nieporównywalne, to podejmuje się próby ich klasyfikowania. W czołówce różnych rankingów pojawiają się zazwyczaj te same miasta, choć w różnej kolejności, często zależnej od kryteriów przyjętych w danym zestawieniu. Nowy Jork, Londyn, Barcelona, Vancouver, Wiedeń, Medellín, Seul – często wymienia się je jako przykłady *smart cities*.

WYBRANE RANKINGI INTELIGENTNYCH MIAST NA ŚWIECIE (za 2016 r.)

Cities in Motion Index (IESE Business School)

1. Nowy Jork
2. Londyn
3. Paryż
4. San Francisco
5. Boston

Global Smart City 2016 (Juniper Research)

1. Singapur
2. Barcelona
3. Londyn
4. San Francisco
5. Oslo

Networked Society City Index 2016 (Ericsson)

1. Sztokholm
2. Londyn
3. Singapur
4. Paryż
5. Kopenhaga

Inteligentne miasta w Polsce

Od kilku lat miasta w Polsce świadomie planują i wdrażają polityki *smart city*. Wciąż daleko im do światowych liderów, szybko natomiast nadrabiają dystans do większości miast w Europie Zachodniej

czy w USA. W rankingu *Cities in Motion Index* zostały uwzględnione dwa polskie miasta: na 74. miejscu Warszawa i na 94. Wrocław. Oba otrzymały wysokie noty w planowaniu przestrzennym, jednym z dziesięciu ocenianych obszarów – odpowiednio miejsca: 12. i 14. Wśród polskich miast aktywnych w obszarze *smart city* są zarówno duże metropolie, jak i miasta średniej i małej wielkości. W dotychczasowych dwóch edycjach konkursu organizowanego przy okazji Smart City Forum zwycięzcami były Wrocław i Łódź (w kategorii miast powyżej 500 tys. mieszkańców), Lublin i Rzeszów (od 100 do 500 tys.) czy Legnica i Jaworzno (do 100 tys.). Jakże projekty z obszaru *smart city* najczęściej realizują polskie miasta? Zdecydowanie najwięcej jest tych z zakresu transportu, a wśród nich inteligentnych systemów zarządzania ruchem. Coraz częściej pojawiają się projekty o charakterze ekologicznym: wymiana taboru komunikacji zbiorowej na zeroemisyjny, promocja alternatywnych form przemieszczania się – przykładem są popularne miejskie sieci wypożyczalni rowerów. Warszawa i Wrocław przygotowują się do uruchomienia własnych krótkoterminowych wypożyczalni aut (*carsharing*), przy czym stolica Dolnego Śląska chce, aby to były wyłącznie samochody elektryczne. Ostatniej zimy wiele miast po raz pierwszy poważnie zainteresowało się tematem smogu. Dużo projektów dotyczy jakości obsługi mieszkańców. Funkcjonują już pierwsze systemy opłat i podatków lokalnych przez Internet (Sopot, Wrocław). Coraz więcej informacji jest udostępnianych w sieci, np. dane przestrzenne naniesione na mapy interaktywne (miejscowe plany zagospodarowania przestrzennego, granice i własność działek, lokalizacje obiektów publicznych). Płatności w urzędach kartami płatniczymi lub rezerwacje wizyt przez Internet powoli stają się standardem. Dużą pomocą jest – rozwijany przez państwo, a nie władze miast – portal obywatel.gov.pl, który umożliwia załatwianie wielu spraw urzędowych bez wychodzenia z domu. Ważnym elementem polskiego *smart city* są aplikacje mobilne służące lepszemu „korzystaniu” z miast przez mieszkańców.

Niektóre aplikacje są tworzone przez urzędy, np. Warszawa 19115, przez którą można zgłosić do urzędu uwagi dotyczące funkcjonowania miasta (zdjęcie, opis, lokalizacja): dziurę w jezdni, niedziałającą latarnię, zaparkowany na trawniku samochód. Umożliwia też błyskawiczne przekazywanie jej użytkownikom ważnych informacji dotyczących miasta, np. o utrudnieniach w funkcjonowaniu metra.

Słyszac zwrot *smart city*, widzimy miasto naszpikowane nowoczesnymi technologiami. Jednak miasto aspirujące do bycia inteligentnym to znacznie więcej niż technologie.

Zdecydowana większość aplikacji mobilnych to inicjatywy mieszkańców. Pomaga w tym udostępnianie (wciąż w niewielkim zakresie) przez samorządy posiadanych cyfrowych zbiorów danych – zarówno statycznych (np. dotyczących rozmieszczenia obiektów miejskich lub ewidencji), jak i na bieżąco aktualizowanych (np. przemieszczanie się pojazdów komunikacji miejskiej). Dzięki temu mieszkańcy mogą swobodnie i bezpłatnie korzystać (także do celów komercyjnych) z danych niezbędnych do tworzenia aplikacji czy stron internetowych, a tym samym oferować nowe usługi. Sprzyja to rozwojowi lokalnych start-upów, czyli nowych, innowacyjnych firm technologicznych. W udostępnianiu danych przoduje Warszawa (kilkaset zbiorów), tą drogą podążają również Wrocław, Gdańsk i Poznań. Przykładem działania z obszaru *smart city*, obecnym w kilkuset miastach w Polsce, są budżety obywatelskie. Mobilizują mieszkańców do angażowania się w sprawy miast, a dzięki zgłaszanym projektom zmieniają hierarchię potrzeb społeczności lokalnych. Często okazuje się, że dla mieszkańców ważniejsze od kolejnych dróg i parków są place zabaw, parki, domy kultury, cisza i czysta przestrzeń wokół.

Jeśli chodzi o przyszłość, dużym wyzwaniem jest energetyka, wciąż traktowana przez miasta jako konsumowanie energii elektrycznej i ciepłej. Ale i tutaj zachodzą zmiany, szczególnie w mniejszych ośrodkach. Niewielkie Brzeziny chcą stać się samowystarczalne energetycznie, wykorzystując energię odnawialną. Inne miasto, Opalenica, wdraża program efektywności energetycznej, ale nie tylko w formie powszechnej w całym kraju termomodernizacji budynków, lecz poprzez aktywne zarządzanie zużyciem energii. Jednak prawdziwym wyzwaniem dla miast, szczególnie większych, będzie rozwój elektromobilności i rosnąca liczba samochodów elektrycznych.

Smart city – safe city

Trudno mówić o inteligentnym mieście, jeśli nie mierzy się ono z problemem bezpieczeństwa. Chodzi zarówno o bezpieczeństwo mieszkańców na co dzień, jak i sytuacje zagrożenia wywołane katastrofami naturalnymi lub aktami terroryzmu. Rola inteligentnych rozwiązań w tym zakresie jest nie do przecenienia: od bezpiecznego poruszania się po ulicach, poprzez porządek publiczny i alarmowanie o sytuacjach odbiegających od normy, po sprawne systemy komunikacji, gdy już wystąpią sytuacje nadzwyczajne. Wdrażanie inteligentnych rozwiązań może mieć szybki i pozytywny wpływ na ogólny poziom bezpieczeństwa w miastach. Jednak tworzą one również nowe zagrożenia związane z gromadzeniem danych osobowych, masową inwigilacją, a przede wszystkim narażeniem na cyberataki infrastruktury miejskiej włączonej do Internetu Rzeczy. Na przykład w kwietniu tego roku w Dallas hakerzy włamali się do systemu obsługującego system alarmowy i na niemal dwie godziny uruchomili w nocy ponad 150 syren w całym mieście. W efekcie wywołali zaniepokojenie mieszkańców, którzy nie wiedząc, co się dzieje, zablokowali alarmowe linie telefoniczne.

To z pozoru niewinne zdarzenie sygnalizuje, że idea *smart city* to nie tylko ogromna szansa na zmianę jakości życia w miastach. To również ryzyko nowych zagrożeń. Czy można jednak zawrócić z drogi ku inteligentnym miastom? ■

SINGAPUR

- LEW INTELIGENTNY

Singapur (Miasto Lwa) chlubi się mianem jednego z najbardziej inteligentnych. I rzeczywiście, inteligentna technologia jest obecna w codziennym życiu mieszkańców, począwszy od komunikacji, skończywszy na oszczędzaniu energii w domach. Najważniejszymi obszarami, w których Singapurczycy wykorzystują inteligentne technologie, są transport, dom i opieka zdrowotna.



William Pao,
a&s International

O kreślenie „inteligentne miasto” natychmiast kojarzy się z Singapurem. Agencja Juniper Research umieściła Singapur na pierwszym miejscu listy pięciu najbardziej inteligentnych miast w 2016 r. Na kolejnych znalazły się Barcelona, Londyn, San Francisco i Oslo. Nie budzi żadnych wątpliwości, dlaczego firma przyznała tytuł lidera właśnie Singapurowi, tu bowiem inteligentne technologie i czujniki służą optymalizacji procesów biznesowych, zwiększaniu produktywności mieszkańców oraz poprawie jakości ich życia. To państwo-miasto o powierzchni jedynie 700 kilometrów kwadratowych ma ograniczone zasoby naturalne i ludzkie. Wdrożenie inteligentnej technologii usprawniającej codzienne życie jest koniecznością. *Nie mamy wyboru, musimy funkcjonować inteligentnie. Technologie pomagają nam działać lepiej, szybciej i sprytniej* – podkreśla Philip Leong, wiceprezes w BellaDati na region Azji i Pacyfiku. – *Mamy za mało rąk do pracy i starzejącą się populację, zatem automatyzacja jest jedyną drogą.*

Jak twierdzi Patrick Lim, dyrektor grupy sprzedaży i marketingu w Ademco Security Group, niektóre inteligentne technologie – elektroniczny system opłat drogowych, systemy informacji w transporcie publicznym, monitorowanie jakości powietrza, monitorowanie ruchu drogowego na wyspie, kamery dozorowe, sieć czujników czy e-administracja – już są w użyciu lub rozważa się ich wprowadzenie. *Inteligentny system czujników i urządzeń pomoże Singapurowi także w zarządzaniu nieruchomościami oraz infrastrukturą użyteczności publicznej. Składają się na to np. inteligentny monitoring wind czy zarządzanie energią i nieruchomościami. Wszystkie te rozwiązania umożliwiają zwiększenie produktywności i skrócenie czasu postoju, co przekłada się na znaczne oszczędności* – mówi P. Lim. *Dzięki tabletom i smartfonom mieszkańcy poszerzają swoje umiejętności w zakresie nowinek technologicznych, co sprawia, że ich życie staje się wygodniejsze* – wyjaśnia William Goh, dyrektor ADP Tech. – *W każdej sytuacji, czy to w autobusie, MRT (system kolejki miejskiej w Singapurze), czy centrum handlowym, dzięki Wi-Fi można sprawdzić interesujące nas wiadomości, np. o sklepach*

otwartych w danym rejonie, repertuar kin czy menu restauracji. Wszystko przez Internet.

Transport

W Singapurze najważniejszą rolę w inteligentnym transporcie, a szczególnie na parkingach odgrywają czujniki. Coraz częściej do poprawy bezpieczeństwa i jakości usług jest też wykorzystywany obraz z kamer.

Aby usprawnić nawigowanie, na parkingach stosuje się inteligentne czujniki i technologie. *Większość parkingów w dużych centrach handlowych w Singapurze jest wyposażona w czujniki wskazujące liczbę wolnych miejsc. Cyfrowe tablice informacyjne znajdujące się przy głównych drogach dojazdowych wyświetlają dostępność miejsc parkingowych w pobliskich centrach. Większość publicznych parkingów jest przekształcana w systemy z bramkami elektronicznymi* – wyjaśnia John Tan, menedżer ds. klientów kluczowych w ABB.

Uiszczanie opłat za parking czy poruszanie się autostradą w dużym stopniu zautomatyzowano. Każdy zarejestrowany pojazd został wyposażony w urządzenie z cyfrową kartą-portfelem, z której pobierane są opłaty za parkowanie i przejazd. John Tan podkreśla, że na początku 2016 r. rząd Singapuru rozstrzygnął przetarg o wartości 397 mln dol. na satelitarny system *Electronic Road Pricing (ERP)*. System ten pozwala śledzić dowolny pojazd w Singapurze i naliczać opłaty według trasy przejazdu. Kontrola ruchu i zarządzanie nim są dzięki temu skuteczniejsze.

Na podstawie uzyskanych danych rząd może podejmować decyzje np. o podwyżce opłat ERP w określonych porach dnia w celu zmniejszenia korków, o potrzebie rozbudowy dróg czy też budowie nowych autostrad – podkreśla J. Tan.

Kamery dozorowe odgrywają ważną

To państwo-miasto o powierzchni jedynie 700 km² ma ograniczone zasoby naturalne i ludzkie. Wdrożenie inteligentnej technologii jest tu koniecznością.

INICJATYWA INTELIGENTNEGO NARODU

Za rozwój inteligentnego miasta odpowiada inicjatywa *Smart Nation (Inteligentny Naród)* zapoczątkowana w 2014 r.

Jej celem, zgodnie z informacjami zamieszczonymi na stronie internetowej, jest „poprawa poziomu życia, upowszechnianie inteligentnej technologii w społeczeństwie oraz udostępnianie jej większym grupom”. Twórcy tej inicjatywy zamierzają realizować to poprzez technologię służącą „roz-

wiązaniu problemów i radzeniu sobie z żywymi wyzwaniami”.

Projekt wskazuje pięć najważniejszych obszarów, na które technologia cyfrowa może wywrzeć istotny wpływ. Są to: transport, dom i środowisko, wydajność przedsiębiorstw, zdrowie i godne starzenie się oraz sektor usług publicznych. Wprowadzenie tej inicjatywy ma zachęcić obywateli i przedsiębiorstwa do wspólnego tworzenia rozwiązań zmienia-

jących codzienne życie, rząd natomiast ma zadbać o infrastrukturę, przepisy i środki sprzyjające innowacji. Ponadto rząd przeznaczył dla firm i naukowców tereny, na których mogą rozwijać, wypróbować i wdrażać swoje technologie. I tak dzielnica północna stała się pierwszym w Singapurze miejscem testów samochodów autonomicznych, czyli poruszających się bez kierowcy, oraz nowych koncepcji przemieszczania się.

rolę nie tylko w utrzymaniu płynności ruchu. Obraz przyczynia się do podniesienia jakości usług i pomaga zidentyfikować pewne zachowania kierowców.

Aby zapewnić ochronę i bezpieczeństwo podróżującym, funkcję analityki wideo stosuje się np. do analizy zmian we wzorcach zachowań oraz w profilu wieku i płci ludności. Dane te mogą być również wykorzystywane w planowaniu i optymalizacji rozkładu jazdy autobusów – mówi Lim Kok Quee, dyrektor zarządzający w Singapurze w NEC na region Azji i Pacyfiku. – *Od roku 2014 NEC i SMRT (operator komunikacji miejskiej w Singapurze) współpracują przy wdrożeniu pierwszego systemu telematycznego do monitorowania zachowania kierowców autobusów. Pozwoli to operatorowi zoptymalizować plany szkoleniowe konkretnego kierowcy na podstawie jego umiejętności.*

Kolejną technologią, którą interesują się władze Singapuru, są pojazdy autonomiczne. W niedalekiej przyszłości mogą stać się podstawą transportu publicznego. *Za pomocą smartfonu wezwiemy taksówkę, która bez kierowcy zawiezie nas np. na dworzec kolejowy. Większość ludzi nie będzie potrzebowała własnych samochodów, więc zwolni się miejsca parkingowe i zmniejszy korki, co usprawni poruszanie się po mieście* – podkreśla P. Leong. – *Pojazdy bez kierowców są wciąż w fazie prób związanych z bezpieczeństwem i uregulowaniem kwestii prawnych. Pracujemy nad tym z nadzieją, że za trzy czy pięć lat po Singapurze będą się poruszać pojazdy autonomiczne.*



William Goh,
dyrektor, ADP Tech



Shermaine Koh,
dyrektor marketingu i komunikacji, iglooHome

Życie w stylu smart

Poprawa monitorowania zużycia energii elektrycznej to jeden ze sposobów, w jaki technologia przyczynia się do inteligentnego życia w Singapurze. *Technologie inteligentne zapewniają mieszkańcom Singapuru liczne korzyści. Wśród nich duże znaczenie ma oszczędność ener-*

PRAWDZIWIE SMART

Inteligentne technologie pomagają mieszkańcom Singapuru na różne sposoby. Czujniki zamontowane w całym mieście i generowane przez nie dane usprawniają procesy i usługi dotyczące transportu, gospodarstw domowych i opieki zdrowotnej.

gii elektrycznej. Technologie komunikacji smart, takie jak system i-bus KNX czy system automatyki inteligentnego domu, pozwalają na bardziej wydajne korzystanie z energii i zapewniają zdalny dostęp do funkcji za pośrednictwem aplikacji w urządzeniach mobilnych. Co więcej, ta sama aplikacja może zarządzać systemem telewizji dozorowej i zużyciem prądu – mówi J. Tan. Czujniki i generowane przez nie dane przynoszą korzyści zarówno mieszkańcom, jak i władzom w tworzeniu przepisów. W raporcie Engadget przytoczono przykład osiedla Yuhua, gdzie zainstalowano tysiące czujników informujących dostawców o nawykach mieszkańców, pozwalając ograniczyć zużycie prądu i wody, która stanowi w mieście ogromny problem. Singapur co roku importuje dziesiątki miliardów litrów wody z Malezji. Rząd może te dane połączyć, a stosując narzędzia analityczne i symulacje komputerowe – jak podano w raporcie – usprawniać planowanie, projektowanie i prace konserwacyjne osiedli.

Singapurczycy nieustannie mierzą się w życiu codziennym z koniecznością wielozadaniowości i w coraz większym stopniu polegają na inteligentnych technologiach. Mieszkańcy Singapuru stoją w obliczu coraz większych wyzwań w życiu codziennym, co wymusza poprawę organizacji pracy. Muszą zachować równowagę pomiędzy pracą a obowiązkami w domu. Inteligentne technologie pomagają je połączyć, jednocześnie usprawniając zarządzanie każdej z nich – wyjaśnia Shermaine Koh, dyrektor marketingu i komunikacji w igloohome, firmie

produkującej inteligentne zamki. – Podam przykład: będąc w pracy, musisz wpuścić do domu osobę, która raz na jakiś czas przychodzi sprzątać. Nie jest to problem, ponieważ można to zrobić zdalnie. Co więcej, możesz ustawić czas dostępu w taki sposób, że po wyjściu tej osoby dom będzie znowu chroniony. Z tej technologii mogą korzystać także zarządcy nieruchomości, którzy z poziomu panelu informacyjnego oceniają status setek nieruchomości. Nikt nie musi jechać do tych miejsc, aby sprawdzić, co się tam dzieje.

Inteligentna opieka zdrowotna

Singapur podejmuje intensywne działania w zakresie inteligentnej opieki zdrowotnej. W obliczu starzejącego się społeczeństwa zdrowie i komfort życia seniorów są kwestią priorytetową.

Inteligentne technologie, takie jak czujniki ruchu w domach czy detektory, mogą pomóc w opiece nad osobami starszymi. Staramy się wykorzystywać dostępną technologię, zwłaszcza w służbie osobom starszym – mówi P. Leong. – Gdy np. ktoś w domu się poślizgnie i upadnie, uruchamia się alarm, który powiadomi bliskich lub odpowiednio służby. Innym obszarem zastosowania inteligentnych technologii jest telemedycyna – kontuuje P. Lim. – Pacjenci nie muszą udawać się na badania kontrolne czy rehabilitację do szpitala. W ciągu ostatnich dziesięciu lat Singapur testował różne rodzaje telemedycznych usług medycznych z centralną bazą danych. Trwają poszukiwania spo-

sobu, w jaki big data mogłyby dostarczyć większą ilość gotowych informacji o trendach zdrowotnych i kontroli schorzeń. Telemedycyna może być pomocna w powrocie do zdrowia. Ofiary udaru mogą np. przebywać w domu i tam ćwiczyć pod okiem rehabilitantów monitorujących ich zdalnie. Dowiedziono, że dane pacjentów przetwarzane przez inteligentne technologie SI zapewniają dokładniejszą ocenę i rokowania powrotu do zdrowia pacjentów po udarze. Z takimi informacjami jesteśmy w stanie skuteczniej dopasować opiekę pielęgniarską innym pacjentów, którzy jej bardziej potrzebują – mówi Mervyn Cheah, szef NEC Laboratories w Singapurze. Chorzy na gruźlicę pracują, a jednocześnie muszą pojawić się w klinice raz lub dwa razy dziennie, by zażyć lekarstwo, co jest raczej trudne – W. Goh z APD podaje inny przykład. – Inteligentne rozwiązania natomiast będą wiedzieć, kiedy lekarstwa zabraknie, i zorganizują dostawę do domu.

Bądź smart dzięki robotom

Kilka specyficznych cech sprawiło, że Singapur zwrócił się w kierunku robotyki. Jedną z nich jest niedobór rąk do pracy. Poważne wyzwania, z jakimi borykają się firmy w Singapurze, wynikają z braku siły roboczej, co z kolei jest związane z surowymi przepisa-

Singapurczycy nieustannie mierzą się w życiu codziennym z koniecznością wielozadaniowości i w coraz większym stopniu polegają na inteligentnych technologiach.

mi dotyczącymi pracy cudzoziemców. Żeby móc produkować mimo braku pracowników, rząd Singapuru zdecydował się pójść w stronę innowacji i zmniejszyć uzależnienie od siły ludzkich rąk – mówi John Tan, menedżer ds. klientów kluczowych w ABB. Kilka korporacji gastronomicznych, np. McDonald's, KFC i Yoshinoya, wprowadza samoobsługowe automaty do zamawiania i płacenia w większości swoich restauracji na wyspie. Ma to skrócić czas zamawiania potraw i zmniejszyć liczbę pracowników potrzebnych do obsługi tradycyjnej kasy.

Od niedawna firmy coraz liczniej zwracają się w stronę robotyki, która pozwala wyeliminować żmudną pracę ręczną. Lokalna chińska restauracja, znana jako Supreme Tastes Jiang Nan Chun, wprowadziła

robota, który pomaga w zbieraniu naczyń – opisuje J. Tan. – Inteligentne technologie pozwalają firmom ograniczyć zapotrzebowanie na pracowników, a jednocześnie umożliwiają lepszą alokację kadry i poprawę zarządzania.

W sektorze opieki zdrowotnej zaczęto używać robotów np. do rozdzielania leków w szpitalach. Na brak pracowników cierpi także opieka medyczna. Inteligentne technologie zaczynają przejmować proste prace manualne, takie jak funkcja gońca szpitalnego – twierdzi J. Tan. – W szpitalu Changi General w Singapurze robot o nazwie HOSPI rozwozi leki, próbki czy dokumentację pacjentów.

Oprócz wykonywania prac automatycznych roboty w służbie zdrowia mogą mieć namiastkę cech człowieka. W tym kierunku podążają prace nowo powstałego przy szpitalu Changi General Centrum Technologii Wspierania Opieki Zdrowotnej i Robotyki (Center for Healthcare Assistive and Robotic Technology, CHART). Jednym z projektów jest interaktywny robot, który będzie zabawiał pacjentów podczas oczekiwania na wizytę, a także odwracał uwagę dzieci w czasie szczepień – opowiada z uśmiechem J. Tan. – Kolejnym pomysłem jest automatyczna maszyna kąpielowa. ■



Philip Leong,
wiceprezes na region Azji
i Pacyfiku, BellaDati



Lim Kok Quee,
dyrektor zarządzający na
region Azji i Pacyfiku, NEC,
Singapur



Patrick Lim,
dyrektor grupy sprzedaży
i marketingu, Ademco
Security Group



John Tan,
menedżer ds. Klientów
kluczowych, ABB

PRZYKŁAD GODNY NAŚLADOWANIA

Specyficzne cechy Singapuru pomogły w uzyskaniu statusu miasta inteligentnego. Inteligentne technologie, począwszy od czujników zainstalowanych na ulicach, skończywszy na urządzeniach pracujących w domach, wspierają firmy i mieszkańców

w skutecznym działaniu. Analiza danych generowanych przez owe czujniki pomaga rządowi w planowaniu rozwoju i usprawnianiu zarządzania. Nieprzerwany rozwój Singapuru stanowi dla innych miast azjatyckich przykład do naśladowania.

Spacer po smart city

Inteligentne miasta stają się modne. Nie ma jednej definicji *smart city*, tym mianem można określić wiele projektów. **Łączy je jedno: wzorcowe *smart city* jest technologiczną formą gościnności.** Przykładem może być Dubaj – inteligentna metropolia w sercu pustyni.

Charles Trybus
Comarch

Nad poprawą warunków życia człowiek zastanawiał się jeszcze długo zanim barbarzyńcy weszli do Rzymu. W „analogowym” świecie zaowocowało to m.in. wybudowaniem systemu kanalizacji czy ustaleniem optymalnej szerokości chodnika. Skrajnym przykładem jest wyburzenie w XIX w. średniowiecznego Paryża, by odbudować go na planie dróg krzyżujących się w formie gwiazdy. W XXI wieku nie ma już miejsca na takie rewolucje – nowoczesne miasta zmieniają swoje oblicze dzięki rozwiązaniom IT. Wyzwaniem w każdym dużym mieście jest transport. Problemu korkujących się ulic nie uda się jednak rozwiązać, budując coraz szersze drogi czy autostrady. W godzinach szczytu na Sheikh Zayed Road w Dubaju, 12-pasmowej autostradzie przebiegającej przez centrum miasta, widać niekończący się korek. Wysoka cena za przejazd nie stanowi

przeszkody – jest tu wystarczająco wiele osób, dla których pieniądze to nie problem. Liczy się czas. Miastu zależy więc na przekierowaniu ruchu na transport publiczny. W ekspresowym tempie wybudowano dwie supernowoczesne linie metra (jedyne na świecie, w którym funkcjonuje elitarna I klasa), jednak i ten środek komunikacji jest już przeładowany, a częstotliwość i liczba kursujących pociągów nie pozwala na zintensyfikowanie przejazdów. Jak więc skłonić mieszkańców, aby zostawili swoje auta w domu? Dubajskie Road and Transport Authority (RTA) stara się promować *car sharing*. Powstała nawet dedykowana aplikacja mobilna, jednak ta forma „współdzielenia” przejazdów samochodem w mieście milionerów nie zyskała dużego zainteresowania. Kolejną próbą była współpraca miasta z Uberem, światowym

gigantem w przewozie osób. O wadze problemu może świadczyć fakt, że kierowcy Ubera są największą konkurencją dla korporacji taksówkowych, licencjonowanych właśnie przez RTA. Alternatywą może być ruch rowerowy, problem stanowią jednak ekstremalne temperatury sięgające nawet 50°C. Dubaj poważnie zastanawia się nad klimatyzowanymi ścieżkami rowerowymi. Innymi przykładami inicjatyw ułatwiających komunikację w miastach jest możliwość płacenia zbliżeniowego (np. za pomocą smartfonu) za przejazd metrem czy autobusem. Dzięki technologii NFC nie wymaga to już dostępu do Internetu. Smartfony wykorzystuje się też do wskazywania wolnych

miejsc parkingowych w najbliższej odległości – tu korzysta się z analizy obrazów z kamer monitoringu wizyjnego lub (co ciekawe) z kamer zainstalowanych na parapetach mieszkańców. W Dubaju testowano też aplikację wyszukującą wolne miejsce parkingowe i rezerwującą je na określony czas. Jeden z prelegentów ubiegłorocznej konferencji *Smart City* w Marsylii, w której uczestniczyłem, przekonywał, że ma wszczepiony chip w prawej ręce. Mógł otwierać i uruchamiać auto zbliżając do niego dłoń, w podobny sposób płacić za zakupy i kontrolować swoją kondycję fizyczną czy stan zdrowia. W bliskiej przyszłości chip ma też gwaranto-

wać mu rozpoznawanie przez autonomiczne auta. Konstruktorzy i branża IT wspólnie pracują nad koncepcją systemu autonomicznego ruchu ulicznego. To wyzwanie niezwykle, z perspektywy miast bardzo kuszące – auta, które dowiozły swoich pasażerów na miejsce, wracająby dopiero, by ich odebrać. Zanim jednak dojdzie do w pełni autonomicznego ruchu ulicznego, przemysł samochodowy i ubezpieczyciele, wychodząc naprzeciw oczekiwaniom i zmieniającym się warunkom ekonomicznym, promują współdzielenie prywatnych samochodów. Koncepcja jest prosta – skoro twoje auto nie jest Ci teraz potrzebne, wypożycz je. Działają już aplikacje *Koolicar* (we Francji) oraz *Car2Go* (w Europie i USA). Paradoksalnie, wyzwaniem w realizacji idei *smart city* może być sama innowacyj-

ność tych projektów. Przekonanie instytucji publicznej (samorządu) do produktu, który jest jeszcze w końcowej fazie R&D może okazać się trudne. Wydając środki publiczne instytucja wymaga dostarczenia rozwiązań sprawdzonych i pewnych. Wdrożenie tylko w środowisku testowym może nie być wystarczające, by przekonać inwestora. Choć zdarzają się odważni – spotkałem się z miejskim projektem rewitalizacji dzielnicy. Aby go zrealizować, musiano przekonać prywatnych inwestorów i mieszkańców. Zlecono realizację makietki odnowionej dzielnicy, po której każdy chętny mógł się przespacerować dzięki technologii VR (wirtualna rzeczywistość). Projekt zakończył się sukcesem! Mówiąc o *smart city* nie można pominąć ważnej kwestii tzw. monetyzacji projektu. Miasta często mogą chcieć uczestniczyć w takich przedsięwzięciach, ale nie zawsze stać je na ich finansowanie. Projekty są więc kierowane także do sektora prywatnego. Powstają już rozwiązania *smart city*, uzupełniane komunikatami handlowymi. Zakupy czy roz-

rywka stanowią dużą część miejskich aktywności. Podczas weekendowej wyprawy do galerii handlowej na użytkownika czekają dedykowane oferty wyświetlane na ekranie jego smartfonu dopiero gdy znajdzie się w bliskiej odległości od sklepu, w którym może z oferty skorzystać. Tego typu aplikacje marketingowe są budowane na bazie beaconów. Te sprytne „pastylki” bardzo dokładnie lokalizują urządzenie na danym obszarze. Wykorzystują do tego fale Bluetooth, a interakcja z użytkownikiem nie wymaga połączenia z Internetem czy zasięgu GPS. Możemy być dumni, że zagłębiem produkcyjnym beaconów stał się Kraków, w którym tego typu rozwiązania realizują trzy firmy i szczytą się wdrożeniami na całym świecie. Wyświetlanie dedykowanego (więc interesującego odbiorcę) contentu w zależności od lokalizacji odbiorcy otwiera wiele możliwości. Stanowi np. ciekawą ewolucję dla programów lojalnościowych. „Przyjdź tu, zrób to, a dostaniesz atrakcyjną nagrodę” – to scenariusz wdrażany obecnie w branży paliwowej czy lotniczej. Lokalizacja i jej kontekst mogą także idealnie prowadzić turystę po mieście, mogą mu również pomóc w skorzystaniu z transportu publicznego, czy realizacji transakcji na lotnisku, na-

licząc jednocześnie punkty w wybranym programie lojalnościowym. Innym przykładem dostosowania do potrzeb i okoliczności jest zastosowanie podobnego schematu (nadajnik–odbiornik) w Kuala Lumpur. Ogromnym problemem w stolicy Malezji są gangi motocyklistów, wyrwujących torebki przechodniom. Szkody materialne są niczym wobec poważnych obrażeń ofiar, które kończą się nawet śmiercią. Kradzieży bardzo trudno zapobiec, równie trudno złapać sprawcę. Wymyślono jednak proste urządzenie, które może „oznakować” złodzieja – elegancki inteligentny brelok zawieszony na torebce. W przypadku kradzieży ofiara, wykorzystując aplikację mobilną, przesyła sygnał do breloka, w którym umieszczono pojemnik z silnie farbującą substancją. Ten sygnał powoduje, że trudno zmywalna farba (podobna do tej używanej do znakowania kradzionych banknotów) znakuje rabusia, którego łatwo rozpoznać w tłumie.

BIO

Charles Trybus, Pół Francuz, pół Polak. Absolwent dziennikarstwa na Uniwersytecie Jagiellońskim. Od 3 lat jako Project Manager/Head of PMO zajmuje się projektami *smart city* w polskiej firmie Comarch, jednej z największych spółek informatycznych w Europie.



Miasta, które myślą... To naprawdę możliwe

Smart city, czyli idea, w myśl której systemy inteligentnych technologii pomagają w zarządzaniu miastami, to już rzeczywistość. Co więcej, niektórzy już się do niej przyzwyczaili. Świadczą o tym przykłady rozwiązań z całego globu, takie jak inteligentne przystanki autobusowe z interaktywnymi tablicami, kosze na śmieci komunikujące się ze służbami oczyszczania miasta czy oświetlenie miasta dopasowujące się do potrzeb jego mieszkańców. **Czy w Polsce istnieją inteligentne miasta? Jak na tle światowych metropolii prezentują się nasze aglomeracje?**

Okazuje się, że miasta mogą myśleć, choć jeszcze nie samodzielnie. Inteligencja miast polega głównie na zbieraniu obszernych danych tzw. *Big Data* i ich analizie, dzięki której można dotrzeć do źródła problemu w konkretnym miejscu w mieście. *Smart city* to idea polegająca na wykorzystaniu rozwiązań zaawansowanych technologicznie, które mają na celu wspomóc środowisko, wygenerować oszczędności

lub usprawnić funkcjonowanie miasta i jego mieszkańców. Pojęcie inteligentnego miasta po raz pierwszy pojawiło się dzięki grupie naukowców z uniwersytetów w Lublanie, Wiedniu i Delfcie w Holandii, którzy w 2007 roku rozpoczęli badania nad projektem *European Smart Cities*. Przykładem przełożenia inteligencji miasta na jego użyteczność jest wprowadzony w Barcelonie system inteligentnych przystanków au-

tobusowych. Każdy z nich został wyposażony w tablice interaktywne z dostępem do Internetu, wyświetlające informacje dla mieszkańców i turystów. Zebrane informacje pozwalają skrócić czas oczekiwania, umożliwiają analizę zatłoczenia w środkach komunikacji i na jej podstawie dostosowanie do potrzeb użytkowników. Czy podobne zmiany można wprowadzić w polskim mie-

ście? Oczywiście że tak, ale taka zmiana nie jest możliwa bez społecznych innowacji, odpowiednio rozłożonego budżetu czy przemyślanej strategii rozwoju miasta – tłumaczy Artur Pollak, prezes APA Group, prekursora na rynku inteligentnej automatyki budynkowej w Polsce. – *Rozmowy z samorządami pokazują, że jest ogromne zapotrzebowanie na wiedzę i technologie w skupiskach miejskich. W Polsce jest wiele realizacji, które wskazują na początki wykorzystywania smart city, np. do zarządzania transportem miejskim przy użyciu systemów Park & Ride. Na razie projekty te są realizowane bez podejścia systemowego, tzn. ekscytujemy się osiągnięciami lokalnymi, nie zastanawiając się, jak rozwiązać narastające problemy społeczne i ekonomiczne w sposób bardziej uniwersalny.*

W Europie Zachodniej „wskaźnik inteligencji miast” jest zdecydowanie większy od tego np. w Polsce. Dzieje się tak za sprawą większej świadomości obywateli oraz wypracowanej przez lata odpowiedzialności społecznej, która determinuje zaangażowanie w projekty, przekładające się na widoczne efekty. Na przykład w Rotterdamie wprowadzono system inteligentnego oświetlenia miasta. Można nim sterować zdalnie, kontrolować bieżące zużycie energii oraz monitorować jego sprawność. Oświetlenie to może być jaśniejsze lub ciemniejsze, dopasowane do pogody lub natężenia ruchu. Dzięki takiemu pozornie błahemu rozwiązaniu mieszkańcy poczuli się bezpieczniej, a statystyki dotyczące przestępczości spadły. Z kolei za oceanem ciekawy projekt, który przyczynił się do zmniejszenia zanieczyszczeń środowiska, został wdrożony w Nowym Jorku. W koszach na śmieci zamontowano czujniki, które informują służby o stanie wypełnienia odpadkami. Każdy taki kubek jest dodatkowo wyposażony w kamery i sensory, aby zgłosić ewentualne wyrzucanie nielegalnych odpadów. Docelowo wszystkie kosze na śmieci będą jednocześnie punktami *hot spot*. W Polsce istniejące rozwiązania ograniczają się do ulepszeń w organizacji ruchu ulicznego lub ograniczenia emisji szkodliwych substancji. Kierunek zmian i chęć rozwoju napawają optymizmem. Konferencje i wymiana doświadczeń pozwalają mieć nadzieję, że na usprawnienia będziemy już niedługo patrzeć w szerszej perspektywie. Warto zwrócić uwagę, że zadaniem systemów automatyki jest nie tylko wsparcie człowieka, ale także jego ochrona. Pierwsze realizacje idei *smart city* mają

za sobą Warszawa, Rzeszów i Wrocław, do tego nurtu dołączają kolejne samorządy – dodaje Artur Pollak. Zdecydowanie wyróżniającym się miastem w tej kategorii w Polsce jest Wrocław. Posiada on infrastrukturę dla pojazdów elektrycznych i jednocześnie pracuje nad stworzeniem dla nich miejskich wypożyczalni. W całym mieście znajduje się ponad 500 punktów dostępu do Internetu, a pod ziemią położono ponad 130 km światłowodu i 200 km kanalizacji teletechnicznej. W innych miastach technologia *smart city* ogranicza się do kontroli ruchu drogowego i emisji spalin. W światowych rankingach coraz częściej pojawiają się Rzeszów, Szczecin, Bydgoszcz i Białystok. Według Integrated Solutions (część grupy Orange Polska) aż 73 proc. samorządów deklaruje, że chce sięgnąć po środki unijne w celu wdrożenia rozwiązań *smart city*. Praktycznie wszystkie programy krajowe i regionalne w ramach perspektywy 2014–2020 przewidują tego typu wsparcie. Według danych resortu infrastruktury i rozwoju na ten cel może być przeznaczonych aż ok. 18 mld euro. Z dotacji i wprowadzonych dzięki nim innowacjom samorządy mogą skorzystać podwójnie, ponieważ efektem zdecydowanej większości systemów *smart city* jest m.in. ograniczanie kosztów. Nie możemy zapomnieć, że celem światowego trendu *smart city* jest ograniczenie kosztów emisji CO₂ i zużycia energii – podkreśla Artur Pollak. To bardzo ważne, szczególnie w kontekście badań środowiska, w których polskie miasta wypadają zdecydowanie najgorzej w porównaniu z innymi miastami europejskimi. ■

PEOPLE MATTER.

**WYZWANIA NIE
ZNIKAJĄ, LECZ ZMIENIAJĄ SIĘ.**

Świat pracy zmienia się dynamicznie. Najlepiej wiedzą o tym ludzie mający do czynienia z cyfryzacją, nowymi technologiami, rosnącą elastycznością oraz masową intensyfikacją pracy. Przygotuj się na nowe wyzwania rynku z targami nr 1 w branży i 1.900 wystawcami z całego świata.

www.AplusA-online.com

Analiza krytycznych systemów w SMART CITY

Przy omawianiu koncepcji działania miasta typu *smart city* szczególną uwagę należy zwrócić na jego krytyczne systemy składowe. Integracja systemów zarządzania miastem przyszłości stwarza nowe zagrożenia, co może przełożyć się na bezpieczeństwo całego miasta.

prof. AGH Jerzy Mikulik,
AGH Akademia Górniczo-Hutnicza

Problematyka bezpieczeństwa była jednym z podstawowych zagadnień, jakimi zajmował się człowiek. Od umiejętności szacowania ryzyka i oceny bezpieczeństwa zależało jego życie. Wraz z rozwojem społeczności pojawiały się nowe zagrożenia, które należało uwzględnić. Zaczęto stosować metody naukowe, by ocenić, czy dane rozwiązanie jest bezpieczne, czy też nie. Współcześnie działające systemy są bardzo złożone, połączone ze sobą, tworzą skomplikowane sieci powiązań i pracują w stanach około chaotycznych. Świat jest pełen zagrożeń zarówno ze względu na ograniczenia stosowanej techniki, jak i na fakt, iż ludzie nie zawsze działają dla wspólnego dobra. Dlatego współczesne systemy bezpieczeństwa już na etapie projektowania powinny uwzględniać wszystkie potencjalne zagrożenia. W związku z tym można zaobserwować rozwój różnych metod ich analizy. Nie zawsze jednak możliwe jest dokładne liczbowe określenie zagrożeń czy ich efektów. Dlatego coraz częściej sięga się po metody heurystyczne, które nie są próbą wtłoczenia wszystkie-

go w sztywne ramy, a raczej tworzą zbiór wskazań dla użytkownika, na co powinien zwrócić szczególną uwagę. Jest to dla inżynierów stosunkowo nowe podejście. Pojawiało się, gdy stopień złożoności urządzeń doszedł do takiego punktu, że dokonanie oceny problemów wyłącznie w sposób obliczeniowy było trudne lub wręcz niemożliwe. Choć wraz z rozwojem komputerów i ich sieci możliwości przeprowadzania dużej liczby skomplikowanych obliczeń rosną, to metody przybliżone i heurystyczne dają wystarczająco dobre efekty. Czasami nie można zastosować innych metod niż heurystyczne, gdyż zagrożenia trudno zweryfikować i nie da się ich dokładnie ocenić, w innych przypadkach zaś potencjalne skutki są tak poważne, iż metody przybliżone nie wchodzą w grę [3]. Dzisiaj inżynierowie posługują się pojęciem systemu w szerokim zakresie. Systemami są dla nich nie tylko urządzenia techniczne składające się z podzespołów, ale również fragmenty środowiska, społeczności ludzkie oraz wszystkie układy składające się z tych kombinacji. *Smart city* jest nową koncepcją w procesie rozwoju infrastruktury miast. Idea powstania miasta zawsze wiązała się z bezpieczeństwem. Pierwsze osady budowano, by zapewnić bezpieczeństwo większej grupie ludzi za pomocą mniejszych środków. Rozwój techniki przez długi czas był w dużej mierze napędzany potrzebą zabezpieczenia potrzeb ludzi w miastach. Rozwijano budownictwo, by otaczać miasto coraz lepszymi umocnieniami, chronić je przed pożarami i podnosić komfort życia. Choć ze względu na zmiany we współczesnym świecie mury odeszły do przeszłości, to nadal bezpieczeństwo jest najwyższym priorytetem.

Trzeba jednocześnie pamiętać, iż same systemy tworzące *smart city* są potencjalnym źródłem zagrożeń, a miasto inteligentne jest dla potencjalnych napastników celem samym w sobie, stąd też musi być szczególnie zabezpieczone. Dlatego też jego eksploatacja powinna być powiązana z ciągłą analizą zagrożeń i stanu bezpieczeństwa. Inteligentne miasto w swojej idei zakłada istnienie skomplikowanych struktur powiązań pomiędzy jego systemami. Podstawowym założeniem jest unikanie dublowania infrastruktury, dostępność wszystkich usług z każdego terminala, aby niepotrzebnie nie zużywać zasobów. Wymaga to łączenia niezależnych dotychczas systemów, w wyniku czego powstają złożone struktury wymagające nowych metod analizy.

Działanie miasta typu *smart city*

Kategoria *smart city* zakłada, iż wszystkie systemy miejskie będą zintegrowane i będą wymieniać między sobą dane oraz korzystać ze wspólnej infrastruktury [1], co spowoduje powstanie skomplikowanej sieci powiązań. Pierwszym i zapewne najważniejszym krytycznym systemem miejskim mogą być sieci energetyczne typu *smart grid*, w których wszystkie elementy składowe sieci – producenci, infrastruktura przesyłowa i odbiorcy – przesyłają sobie nawzajem, w czasie rzeczywistym, dane na temat aktualnych parametrów pracy, a także prognozowanego zapotrzebowania. Pozwoli to w lepszym stopniu dostosowywać pracę systemu do aktualnego obciążenia, zwiększając niezawodność podzespołów i umożliwiając lepsze gospodarowanie energią elektryczną. Prowadzi to do integracji na dwóch płaszczyznach. Po pierwsze istnieje integracja systemów na płaszczyźnie „galwanicznej” zasilania (tak jak w tradycyjnym sys-

temie) oraz dochodzi druga płaszczyzna integracji cyfrowej. Pierwsze połączenie w sposób oczywisty przenosi tradycyjne zagrożenia, np. przeciążenie jednego fragmentu sieci energetycznej może spowodować awarie w sąsiednich sieciach, doprowadzając do lawinowej reakcji odłączeń. To przykład zagrożenia związanego z techniką, gdzie skomplikowana struktura powiązań umożliwia rozprzestrzenienie się awarii na sąsiednie systemy. Druga, cyfrowa integracja w inteligentnej sieci energetycznej ma to zagrożenie zmniejszyć. Dzięki monitorowaniu w czasie rzeczywistym można przewidywać awarie na podstawie parametrów pracy systemu i im przeciwdziałać. Jednak powoduje to inny rodzaj zagrożeń, tak zwane celowe działania człowieka. Cyfrowe sieci przesyłu danych mogą stać się celem działań czy to przestępców, czy organizacji terrorystycznych, czy agencji obcych państw. Przestępcy mogą chcieć wniknąć poprzez te systemy do baz danych producentów energii, by fałszować dane lub pobierać poufne informacje. Organizacje terrorystyczne mogą próbować doprowadzić do zniszczeń w systemie poprzez sfingowane kody sterujące, np. doprowadzając do fałszywych przeciążeń sieci. Siły obcych państw mogą postrzegać taki system jako pierwszy cel ataku, aby poprzez odłączenia energii elektrycznej wprowadzić chaos w strukturze dowodzenia w kluczowych momentach. Zagrożenia są różnorodne i system musi mieć stosowne zabezpieczenia, aby im sprostać, szczególnie że w tym przypadku nie za bardzo można przeciwdziałać atakowi poprzez czasowe odłączenie zaatakowanych elementów [2, 4]. Kolejnym przykładem krytycznego systemu zarządzania jest system sterujący ruchem w mieście. Powstaje w wyniku połączenia niezależnych podsystemów sygnalizacji świetlnej na skrzyżowaniach w jedną sieć, powiększoną o systemy informacyjne dla kierowców oraz czujniki mierzące natężenie ruchu na poszczególnych trasach. Taki system pozwala na optymalizację przepływu strumienia pojazdów, dostarczenie kierowcom informacji o trasach alternatywnych, a także – po sprzęgnięciu z systemami komunikacji zbiorowej oraz służbami porządkowymi – na ustalanie priorytetów dla tych uczestników. Pod względem efektywności jest to rozwiązanie bardziej skuteczne niż tradycyjna syn-

Systemy tworzące *smart city* są potencjalnym źródłem zagrożeń, a inteligentne miasto jest dla potencjalnych napastników celem samym w sobie, stąd też musi być szczególnie zabezpieczone.

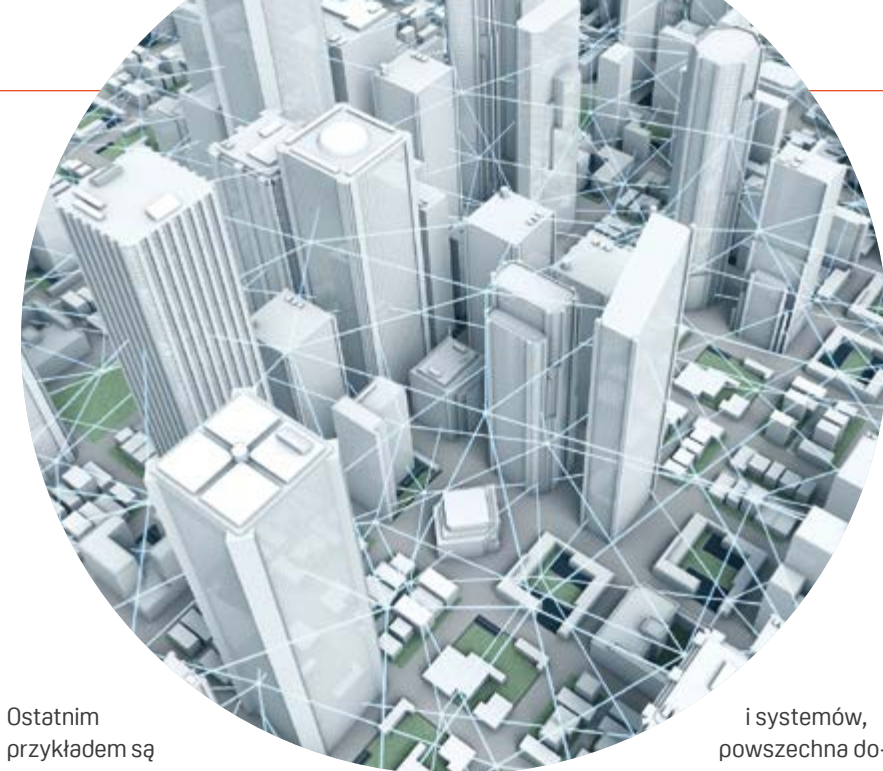
chronizacja „zielonej fali” czy ustawianie innych czasów dla komunikacji zbiorowej i reszty pojazdów, ponieważ reaguje w czasie rzeczywistym na zmiany w natężeniu ruchu i sytuacje nadzwyczajne. Pojawiają się jednak zagrożenia – ryzyko, iż awaria pojedynczego składnika podsystemu przeniesie się na cały system. Powoduje to potrzebę zachowania większych wymagań co do niezawodności. Po części jest to ułatwione, ponieważ system monitoruje również stan swoich podzespołów. Jednak podobnie jak w przypadku inteligentnych sieci elektroenergetycznych, również ten system może się stać celem przestępców czy terrorystów. Mimo wszystko, w przeciwieństwie do poprzedniego przypadku, tutaj w razie ataku pozostaje opcja, by każdy z lokalnych podsystemów przeszedł na „sterowanie lokalne”. Spowoduje to wprawdzie utratę części użyteczności, ale zmniejszy ryzyko wyeliminowania systemu jako całości [4]. Następnym przykładem skomplikowanego systemu *smart city* jest system wspierający pracę służb porządkowych: policji, straży pożarnej i pogotowia ratunkowego. Polega to na połączeniu systemów tych służb w całość poprzez wymianę danych również z systemem kierującym ruchem w mieście, tak by można było w niezawodny sposób zarządzać użyciem tych służb oraz skrócić czas potrzebny na interwencje. System ten, ze względu na specyfikę służb, składa się z komponentów o wysokim wskaźniku bezpieczeństwa. Problemem jest to, iż aby działać wydajnie, powinien komunikować się z innymi systemami miejskimi, a one mają niższy poziom bezpieczeństwa. Należy pamiętać, że na styku systemów o różnym poziomie bezpieczeństwa muszą pojawić się dodatkowe zabezpieczenia uniemożliwiające nieuprawnione wtargnięcie do systemu lub sfingowanie awarii. Wymaga zasta-

Kategoria *smart city* zakłada, że wszystkie systemy miejskie będą zintegrowane i będą wymieniać między sobą dane oraz korzystać ze wspólnej infrastruktury.

nowienia, czy taki system ze względów bezpieczeństwa nie powinien być odstępstwem od zasady wspólnej infrastruktury. Oddzielne łącza danych zwiększyłyby bezpieczeństwo systemu, a w sytuacjach kryzysowych działałyby jako rezerwa na wypadek niezdatności głównych linii, przysyłając informacje krytyczne do innych systemów miasta.

Systemy monitoringu miejskiego to systemy pozornie najpopularniejsze. Jednak oprócz spełniania podstawowej funkcji, jaką jest poprawa bezpieczeństwa, mogą wspierać również inne działania związane z monitorowaniem ruchu, naliczaniem opłat za wjazd do płatnych stref czy też nawet funkcje informacyjne lub turystyczne. Wiąże się to z integracją tego systemu z miejską siecią danych. Należy pamiętać, iż spora część strumienia danych generowanych przez ten system to dane wrażliwe, dlatego też należy je odpowiednio zabezpieczyć. Trzeba uważać, aby forma danych przesyłanych do innych systemów była adekwatna do ich potrzeb, szczególnie gdy chodzi o inne systemy związane z bezpieczeństwem, np. system kierowania ruchem czy płatnościami.

Idea *smart city* wymaga wysokiego poziomu integracji systemów należących zarówno do miasta, jak i prywatnych podmiotów. W tym celu zaleca się przyjęcie uniwersalnego modelu przesyłania danych opartego na kodzie *open source*. To spore utrudnienie w zapewnieniu bezpieczeństwa przesyłu danych. Wszystkie dane będą płynąć po wspólnych magistralach, posługując się tym samym kodem, a bezpieczeństwo tak naprawdę będzie się opierać wyłącznie na szyfrowaniu danych, gdyż dostęp do sieci będzie mógł mieć każdy. Dużym problemem staną się rozproszone ataki dostępu do usługi. Ochrona przed zalewem informacji stanowi i będzie stanowić duże wyzwanie nie tylko dla administratorów firm, ale również dostawców Internetu.



Ostatnim przykładem są zagrożenia ze strony środowiska. Są one takie jak klasycznych systemów i zwykle ochronę przed nimi regulują odpowiednie normy i przepisy. Trzeba jednak podkreślić, że nowoczesne systemy są pod niektórymi względami wrażliwsze na warunki i zagrożenia środowiskowe, co wynika z kilku przyczyn. Pierwszą jest złożoność systemów. Współczesne systemy często są bardziej skomplikowane, głównie dlatego że mają zapewniać dodatkowe funkcje, np. monitorowania stanu podzespołów. Podstawowe elementy to zwykłe „elektronika”, która jest dość wrażliwa na trudne warunki pracy i wymaga dobrego zabezpieczenia. Następny problem wynika stąd, że podsystemy coraz częściej współpracują ze sobą na takim poziomie, iż prawidłowe ich działanie nie jest możliwe, gdy łączność między nimi zostanie zakłócona. Dzisiejsza „elektronika” jest też bardziej wrażliwa na zakłócenia napięcia zasilającego czy impulsów elektromagnetycznych (uderzenie pioruna).

Wnioski

Smart city stawia szczególne wymagania, gdy chodzi o jego bezpieczeństwo. Wspólne łącza, upublicznienie formatu danych, wspólna infrastruktura podsystemów

i systemów, powszechna dostępność do informacji – te wymagania komplikują rozwiązania dotyczące bezpieczeństwa. Jednocześnie, jak dowodzi praktyka, poziom działań niebezpiecznych przeciwko miastom i ich systemom rośnie. Skala złożoności nowoczesnych systemów powoduje problemy techniczne, które w układach silnych powiązań mogą się rozprzestrzeniać na sąsiednie obszary działania. Dlatego coraz ważniejsze jest, by wszystkie działania, na etapie zarówno planowania, jak i eksploatacji wspierać ciągłą analizą ryzyka.

Aby zapewnić bezpieczeństwo miastom, trzeba być przygotowanym na wszystkie zagrożenia i mieć środki, by się im przeciwstawić. Skala złożoności problemu rośnie. Niedawno nowością było łączenie systemów sterowania w jednolitą zintegrowaną strukturę w skali budynku. Systemy automatyzacji BMS rozwijają się nieprzerwanie. Teraz łączy się je z istniejącymi systemami w skali miasta. To nowość, dotychczas nie udało się tego zrobić w sposób pełny, ale ta dziedzina stale się rozwija. Można przypuszczać, że wkrótce nastąpią kolejne skoki cywilizacyjne na skalę regionu, państwa czy nawet o zasięgu globalnym. Za każdym razem jednak następuje wykładniczy wzrost skomplikowania struktury i działania systemów. ■

Bibliografia

- [1] BSI Standards Publication PAS181: *Smart city framework - Guide to establishing strategies for smart cities and communities*, 2014.
- [2] Mikulik J., *Inteligentne budynki - Nowe możliwości działania*, Wyd. LIBRON, Kraków, 2014.
- [3] Grotowski M., *Analiza systemów Smart City pod kątem zagrożeń bezpieczeństwa, wyszukiwanie punktów krytycznych za pomocą metody DEMATEL*, AGH w Krakowie, 2016.
- [4] Mikulik J., *Inteligentne budynki - Informacja i bezpieczeństwo*, 2016, Wyd. LIBRON, Kraków.

Zarządzanie systemowe w miejskim systemie monitoringu



Mieszkańcy oczekują, że gdy wpadną w kłopoty, to na miejscu szybko pojawi się policja, która skutecznie zareaguje wobec sprawców. Nie chcą setek wiszących kamer, tylko sprawnego działania. W celu spełnienia tego postulatu konieczne jest zarządzanie różnymi elementami, które tworzą miejski system monitoringu wizyjnego, by móc w pełni wykorzystać potencjał tkwiący w technice, ludziach i dostępnych informacjach.

Paweł Wittich
Akademia Monitoringu Wizyjnego

Mieszkańcy oczekują reakcji – instalacja kamer to za mało

Z „Polskiego badania przestępczości 2015” [1] wynika, że Polacy w pierwszej kolejności oczekują od policji szybkiego przybycia na miejsce zdarzenia – tak deklaruje 41,1 proc. respondentów. Po łatwym dodzwonieniu się na numer alarmowy następnym oczekiwaniem jest skuteczna reakcja policjantów, 35,8 proc. respondentów chce, by zatrzy-

mali sprawców lub odzyskali skradzione mienie itd., 21,4 proc. mieszkańców wymaga, by w okolicy, w której mieszkają, regularnie pojawiały się patrole policyjne. Te oczekiwania nie zmieniają się od wielu lat [2]. Badania nt. skuteczności miejskich systemów dozoru wizyjnego wskazują, że sama instalacja kamer nie zwiększa poczucia bezpieczeństwa mieszkańców, nawet jeżeli jest ich dużo [3]. Swoje poczucie budują m.in. na podstawie ważniejszych dla nich elementów – jakości przestrzeni oraz jakości relacji z sąsiadami i osobami, które pracują lub często przebywają w ich miejscu zamieszkania (*spatial perception*) [4]. Zainstalowanie

kamer nie sprawia, że mieszkańcy chętniej odwiedzają miejsca, które objęto dozorem kamer [3]. Z badań przeprowadzonych w Hamburgu wynika, że ofiara przestępstwa nie musi automatycznie popierać instalowania kamer [5]. Według brytyjskich badaczy nie obecność kamer, ale realna liczba zagrożeń w danym miejscu decyduje o tym, jak bardzo mieszkańcy czują się zagrożeni przestępczością [5]. Oznacza to, że od miejskich systemów monitoringu wizyjnego należy oczekiwać przede wszystkim skutecznego wykrycia zagrożenia i szybkiej reakcji. Będzie to możliwe tylko wtedy, gdy różne elementy

[BIO]

dr hab. inż. prof. AGH Jerzy Mikulik, Katedra Inżynierii Zarządzania, Wydział Zarządzania, AGH Akademia Górniczo-Hutnicza w Krakowie

Artykuł powstał w ramach pracy statutowej nr 11/11.200.322 na podstawie tematu wielozadaniowego: „Analiza możliwości poprawy efektywności działania inteligentnego budynku”, etapu pracy za rok 2017.

tworzące ten system, zasoby straży miejskiej i policji będą skutecznie zarządzane.

Podejście techniczne nie zapewnia skuteczności

Przez długi czas nie tylko w miejskich systemach monitoringu dominowało „podejście techniczne”, reaktywne – przez system CCTV rozumiano kamery, rejestratory i kable umożliwiające transmisję obrazu. Główną funkcją tych instalacji była rejestracja obrazu. Ich podstawową wadą – brak reakcji w momencie wystąpienia zagrożenia, ponieważ nikt nie obserwował obrazów z kamer. Prawdopodobieństwo identyfikacji sprawcy na podstawie zarejestrowanego obrazu było ograniczone, ponieważ nierzadko na nagraniu sprawca stał tyłem do kamery, znajdował się w martwym polu, zasłaniał twarz kapturem, ciemnymi okularami albo obiektyw kamery był skierowany w inną stronę wtedy, gdy sprawca rozbijał szybę, atakował ofiarę itd. W związku z tym, że operatorzy nie podążali kamerami za napastnikami prawdopodobieństwo uchwycenia sprawcy w ujęciu pozwalającym na identyfikację także było niskie. Wielka Brytania pierwsza podjęła kompleksową próbę zdiagnozowania problemów ograniczających skuteczność systemów CCTV, po tym jak w latach 1994–1999 wpompowała 38,5 mln funtów w 585 miejskich systemów monitoringu [6], nie osiągając oczekiwanych efektów. Przygotowany przez jednostkę naukowo-badawczą brytyjskiej policji (PSDB) cykl wydawnictw „CCTV: Making it work” i badania zlecone przez Ministerstwo Spraw Wewnętrznych (Home Office) wskazały szereg zależności i wymagań, które muszą zostać spełnione, żeby miejski monitoring był skuteczny.

W pierwszym okresie rozwoju nowoczesnych systemów monitoringu w Polsce obserwowaliśmy, jako specjaliści Akademii Monitoringu Wizyjnego, że większość miast na własnej skórze musiała potknąć się o te same problemy, jakich kilka lat wcześniej doświadczyli Brytyjczycy, żeby zmienić filozofię zarządzania nimi. Z analogiczną zmianą mieliśmy do czynienia w zakładach przemysłowych.

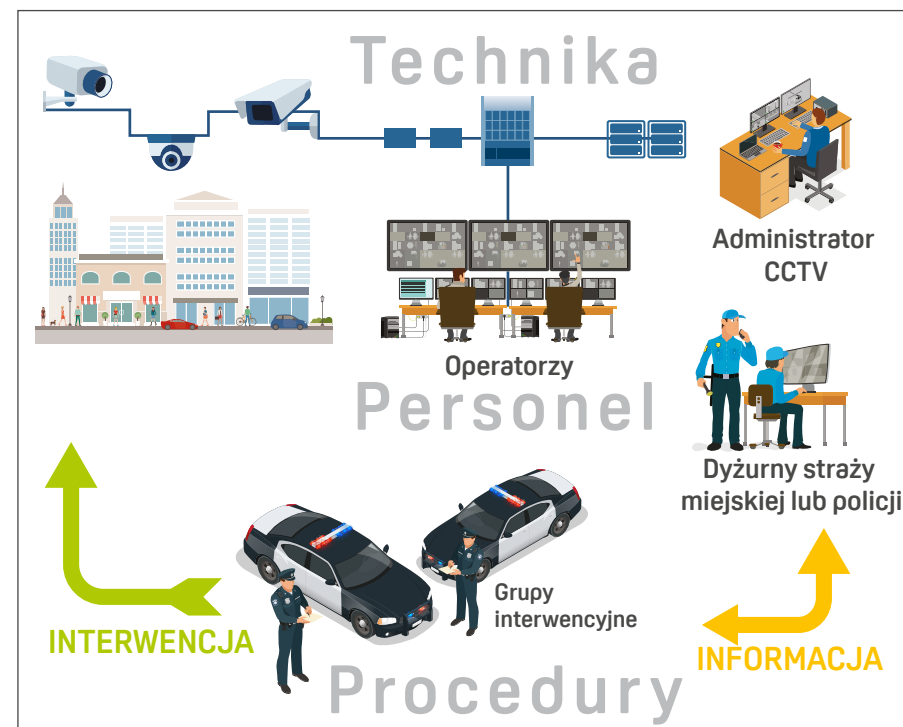
Podejście systemowe

Specjaliści Akademii Monitoringu Wizyjnego zaproponowali w poprzedniej dekadzie stosowanie teorii systemowej w od-

niesieniu do systemów CCTV [7]. Jest to wywodzące się z biologii podejście do objaśniania zależności między składowymi tworzącymi komórki, tkanki lub funkcjonowanie złożonych organizmów; chętnie stosowane w socjologii, ekonomii, informatyce i cybernetyce [8]. W ujęciu systemowym kamery i urządzenia, które tworzą techniczny komponent systemu CCTV, są bazą do działań personelu. Wysoka jakość obrazu nadal jest jednym z najważniejszych kryteriów efektywności systemu, ale nie jedynym. Ze względu na rozwój techniki i większą dostępność kamer łatwiej ją dziś zapewnić. Obrazy z kamer są obserwowane przez operatorów. W przypadku wykrycia zagrożenia operator przekazuje informację do dyżurnego policji lub straży miejskiej. Ten jest zobowiązany wysłać najbliższy patrol, aby działanie zostało podjęte szybko i skutecznie. Co ważne, reakcja odbywa się nie tylko na poziomie policjantów i strażników miejskich, ale także na poziomie operatorów. Od momentu wykrycia zagrożenia prowadzą kamery za sprawcami, żeby zarejestrować najważniejsze fakty i przebieg zdarzenia. Mogą informować interweniujących funkcjonariuszy o przemieszczaniu się lub zwiększeniu liczby napastników, co pozwala modyfikować reakcję systemu adekwatnie do zmieniającej się sytuacji. Rejestrują też działania

funkcjonariuszy, co pozwala zabezpieczyć ich przed fałszywymi oskarżeniami, np. o przekroczenie uprawnień. Takie podejście jest nazywane także proaktywnym, ponieważ jednym z najważniejszych kryteriów oceny działania systemu jest czas reakcji całości i poszczególnych komponentów. Ujęcie systemowe pozwala zidentyfikować kluczowe zależności występujące między elementami, z których składa się miejski system monitoringu wizyjnego: jeżeli operatorzy nie obserwują obrazów z kamer, to dyżurny nie otrzyma informacji o sprawcach, którzy „rozrabiają” w polu widzenia kamer. Gdy jakość obrazu jest zła, scena zbyt ciemna lub kamera nie działa, to nawet operator o najlepszych predyspozycjach do prowadzenia obserwacji nie wykryje zagrożenia. Analogicznie, gdy jeden operator będzie obserwował zbyt wiele kamer lub gdy obrazy będą prezentowane w zbyt małych oknach, jego możliwość zauważenia zachowań sygnalizujących zagrożenie będzie niska. Jeśli dyżurny ma zbyt dużo zgłoszeń albo uzna operatorów za ułożonych nisko w jego hierarchii przyjmowania informacji, to mimo że wykryją oni zagrożenie, ich zgłoszenie utknie między obserwatorami a dyżurnym. Reakcje będą opóźnione lub sprawcy oddalą się z miejsca zdarzenia.

Systemowe zależności w miejskim systemie CCTV



Podobne ryzyko pojawia się, gdy policja i straż miejska nie zapewnią odpowiedniej liczby patroli lub będą one rozlokowane zbyt daleko od miejsc, w których najczęściej dochodzi do zdarzeń. Brzmi prosto? Z kontroli przeprowadzonej przez NIK w 2013 r. wynika jednak, że nadal w polskich miastach zdarzają się sytuacje, że nikt nie obserwuje obrazów z kamer, operatorzy kończą pracę o godz. 15.00 – tak jak urząd miasta, mimo że policja zgłasza potrzebę prowadzenia obserwacji popołudniami, wieczorem i w dni wolne od pracy, ponieważ wówczas dochodzi do największej liczby zdarzeń. NIK zwróciła także uwagę na niskie zaangażowanie policjantów (dyżurni nie chcieli przyjmować zgłoszeń od operatorów) i wiele innych problemów [9]. Podejście systemowe wskazuje, że budowanie skutecznego miejskiego systemu CCTV wymaga stworzenia struktury organizacyjnej, która łączy różne podmioty (podsystemy) – samorząd, policję i straż miejską, a także różne elementy i procesy systemu, ale to wymaga skutecznego zarządzania!

Ujęcie systemowe pozwala zidentyfikować kluczowe zależności występujące między elementami, z których składa się miejski system monitoringu wizyjnego.

Zarządzanie systemowe na różnych poziomach

Podejście systemowe umożliwia skuteczne zarządzanie miejskim systemem monitoringu wizyjnego na różnych poziomach i etapach projektu. Przy projektowaniu pozwala ustalić wymagania użytkowe, które obejmują cel oraz optymalne z punktu widzenia efektywności i kosztów sposoby jego osiągnięcia, typy zagrożeń i czas ich występowania, charakterystyki sprawców i konsekwencje braku przeciwdziałania na zagrożenie – rodzaj i wysokość strat. Bardzo istotnym wymaganiem z punktu widzenia skuteczności systemu monitoringu jest rodzaj podejmowanej reakcji i jej szybkość. Jeżeli operator widzi osobę, która zachowuje się agresywnie, np. jest napięta lub pijana, zaczepia lub prowokuje prze-

chodniów, uderza w kosze na śmieci, to z wysokim prawdopodobieństwem można przyjąć, że dojdzie do bójki lub wandalizmu, istnieje więc zagrożenie życia, zdrowia lub poważnych strat finansowych. Jeżeli takim zachowaniom zostanie nadany najwyższy priorytet, wówczas wszystkie działania w systemie powinny być podporządkowane błyskawicznej wymianie informacji i szybkiemu przyjazdowi patrolu na miejsce zagrożenia. Częstochowska stała miejska uzyskała wyłączenie radiowozów z zakazu skrętu w lewo w centrum miasta, skracając w ten sposób czas interwencji. Przez długi czas utrzymywała patrol dedykowany zdarzeniom ujawnianym przez operatorów, w którego skład wchodziła strażnica, którzy przeszli dodatkowe szkolenia w technikach obezwładniających. Podobny model z sukcesami jest stosowany w Newark, w USA. Przykładowo częstochowska straż miejska utrzymywała wyłącznie do obsługi zdarzeń ujawnianych przez operatorów patrol interwencyjny ze strażnikami, którzy przeszli dodatkowe szkolenia w technikach obezwładniających. Uzyskała wyłączenie radiowozów z zakazu skrętu w lewo w centrum miasta, co skraca czas interwencji [10]. Na drugim biegunie w zakresie szybkości reakcji jest nieprawidłowe parkowanie, które nie generuje poważnych strat, więc tu reakcja może być odroczone. Podejście systemowe może być także stosowane na etapie rozbudowy miejskiego systemu CCTV. Obecnie w związku z zakończeniem umów gwarancyjnych na systemy budowane przed 3–5 laty ze środków unijnych wiele miast staje przed decyzją, co dalej. Część z nich chce wybrać kamery producentów oferujących niższe ceny. Może to oznaczać konieczność zmian systemowych w zakresie rejestracji i transmisji obrazu. W pracy spotykam się także z propozycjami ze strony spółdzielni mieszkaniowych czy szkół, żeby je włączyć do monitoringu miejskiego. Wyzwaniem jest nie tylko kwestia technicznej zgodności różnych systemów, ale także obserwacja obrazów z kamer, bo miejscy operatorzy byliby wówczas nadmiernie obciążeni. Jednym z rozwiązań jest prowadzenie obserwacji przez pracowników agencji ochrony lub dozorców w szkołach i przesyłanie obrazów policjantom lub strażnikom tylko wtedy, kiedy zidentyfikują zagrożenie. Alternatywą może być bezpośrednia linia

telefoniczna na stanowisko dyżurnego, pozwalająca na szybkie przekazanie informacji o zagrożeniu. Ciekawy przykład podejścia systemowego w miejskim monitoringu wypracował Rotterdam, w którym utrzymuje się stałą liczbę kamer – nieco ponad 300 [11]. Władze miasta wskazują, że mieszkańcy widzą, czy policja reaguje na zdarzenie „pod kamerą”. Brak reakcji oznacza spadek zaufania po stronie mieszkańców. Skarżą się wówczas, że nie czują się bezpiecznie, a płacone przez nich podatki są źle wykorzystywane. Instalacja kolejnych kamer wiąże się z koniecznością zapewnienia dodatkowych operatorów i patroli, ale miasto nie zamierza wydawać zbyt dużo na monitoring. Gdy mieszkańcy chcą kamer, to w pierwszej kolejności w konsultacjach społecznych są ustalane ich potrzeby w zakresie bezpieczeństwa. Efektem konsultacji są najczęściej: porządkowanie terenu, poprawa oświetlenia, przycięcie roślinności zwiększające tzw. naturalny nadzór, budowa dróg rowerowych, placu zabaw itd. Gdy te działania nie przynoszą rezultatu, dopiero wtedy montuje się kamerę, która jest przenoszona z miejsca, gdzie już jest niepotrzebna, bo doprowadzono do zminimalizowania liczby zagrożeń. Kielce na etapie projektowania swojego systemu przyjęły podobną filozofię przenoszenia kamer, przygotowując miejską sieć światłowodową na zmiany ich lokalizacji [12]. W podejściu systemowym Rotterdam zbudował model współpracy operatora ze strażnikami miejskimi (Stadtoezicht). Strażnik porusza się w wyznaczonym obszarze. Rozpoczynając służbę, „melduje się” operatorowi. Jest ustalany algorytm patrolowania, żeby wzajemnie się nie dublować. Operator ubezpiecza strażnika w przypadku zagrożenia i natychmiast po wykryciu melduje mu o zdarzeniach, co pozwala na szybką reakcję [11]. Obecnie ten model współpracy operatorów i strażników wdraża Częstochowa – miasto chce wykorzystać fakt, że wszyscy działają w jednej strukturze organizacyjnej, więc jest między nimi możliwa komunikacja radiowa i telefoniczna. W Wielkiej Brytanii i RPA operatorzy mogą słuchać radia policyjnego i nadawać komunikaty za jego pomocą. Słyszając dyżurnego wydającego dyspozycje patrolom, wiedzą, gdzie skierować obiektyw kamery. Mogą przekazać interweniującym ważne informacje o zachowaniu czy przemiesz-

czaniu się sprawcy, zanim policjanci przyjadą na miejsce [13].

Z ujęcia systemowego wynikają także zmiany w strukturze przekazywania informacji. W Częstochowie dyżurnego odciąża koordynator, który jest doświadczonym operatorem. Jego rolą jest kolejowanie zdarzeń wg ustalonego katalogu priorytetów i pomaganie operatorom przy weryfikowaniu niejednoznacznych sytuacji. W krajach anglosaskich w centrach nadzoru pracują policjanci – oficerowie łącznikowi. Podobnie jak w Polsce, ze względu na uprawnienia i bezpieczeństwo komunikacji cywile lub strażnicy miejscy nie mogą wydawać poleceń policjantom; nie ma także wspólnych łączny radiowych. Oficer łącznikowy pracujący z operatorami zapewnia im szybką wymianę informacji i bezpośrednią komunikację z policjantami. Rotterdam, żeby nie odrywać operatorów od bieżącej obserwacji, zleca operatorom „śledczym” przeglądanie nagrań zdarzeń, które nie zakończyły się zatrzymaniem, oraz przygotowywanie nagrań na potrzeby śledztw. Coraz wyraźniejszy jest także trend budo-

Analiza obserwowanych zjawisk pozwala dostosować liczbę operatorów i obsługiwanych przez nich kamer do natężenia zagrożeń.

wania baz danych i mapowania zdarzeń – nie tylko na potrzeby miejskiego monitoringu, ale miasta w ogólności. Analiza tendencji pozwala dostosować liczbę operatorów i obsługiwanych przez nich kamer do natężenia zagrożeń, np. powszechnie wiadomo, że w weekendy, zwłaszcza w ciepłe wieczory, liczba zdarzeń jest większa niż zimą. Umożliwia także zmiany lokalizacji kamer czy wskazywanie nowych lokalizacji. Systemy uwzględniające zależności systemowe osiągają lepsze wyniki niż te, gdzie nadal traktuje się monitoring wąsko, jako instalację techniczną. Wyraźnie pokazały to wyniki kontroli przeprowadzonej przez NIK w 2013 r. W najlepszych systemach (Radom, Warszawa, Gniezno) dbano, by ope-

ratorzy nie obserwowali obrazów ze zbyt dużej liczby kamer, by byli wybierani pod kątem predyspozycji, zadbano też o ich dobrą współpracę z policją [9]. W prezentowanej tabeli wyróżnia się system częstochowski, w którym dużą uwagę przywiązuje się do zależności systemowych na różnych poziomach [10].

Podejście systemowe w erze smart city i deep learning

Wprowadzenie nowych sposobów wykrywania zagrożeń – algorytmów analizy obrazu, do miejskich systemów CCTV, nie powoduje, że potrzeby mieszkańców w zakresie bezpieczeństwa ulegają zmianie. Będą oczekiwali szybkiej reakcji na zagrożenie, więc aktualne pozostają wyzwania związane z weryfikacją fałszywych alarmów, przekazywaniem informacji, dysponowaniem patrolami, kierowanie kamerami, tak żeby zapewnić rejestrację przebiegu zdarzenia, identyfikację sprawców i zabezpieczenie interweniujących policjantów. Z doświadczeń specjalistów Akademii Monitoringu Wizyjnego wynika, że

Część użytkowników traktuje „inteligentny” monitoring jako gotowy produkt, który nie wymaga ich zaangażowania. W naszej opinii to błędne podejście.

część użytkowników traktuje „inteligentny” monitoring jak gotowy produkt, który nie wymaga ich zaangażowania. W naszej opinii to błędne podejście. Katalog algorytmów jest ograniczony, podobnie ich skuteczność. Warto realnie ocenić, gdzie można je zastosować, a gdzie będą generowały dużą liczbę fałszywych alarmów, zniechęcając operatorów do ich obsługi, co może doprowadzić do tragedii. Podczas jednego z audytów zastanawialiśmy się nad implementacją analizy obrazu na przykładach komunikacji publicznej, ponieważ dla przedstawicieli miasta problemem był wandalizm. Z uwagi na dużą liczbę osób, które korzystały z wiat, w różnych konfiguracjach – pojedyncze osoby, pary, grupy i różne sposoby dokonywania zniszczeń, trudno było wskazać wzór, pozwalający na wykrycie sprawcy. Czy ze złożonymi zachowaniami poradzi sobie uczenie maszynowe, deep learning? Trudno jest zająć jednoznaczne stanowisko. Uczestniczyłem w konferencji podsumowującej prace nad projektem monitoringu nowej generacji – SAVA, prowadzone

przez OBRUM i Polsko-Japońską Akademię Technik Komputerowych, finansowanym przez NCBR. Podczas prezentacji na żywo, algorytmy dobrze radziły sobie z prostymi zachowaniami, jak chodzenie, siadanie. Z drugiej strony, kopnięcie zostało zinterpretowane przez oprogramowanie jako przytulanie(!), mimo, że osoba prezentująca znajdowała się bokiem do obiektywu kamery, była ubrana kontrastowo do dobrze oświetlonej sceny, więc ruchy jej ciała i kończyn były widoczne. Analogicznie, jedno przywitanie dwóch osób zostało prawidłowo zinterpretowane przez algorytm, drugie nie zostało wykryte. Wydaje się, że wyzwaniem dla analityki opartej o uczenie maszynowe jest prawidłowość rozpoznawania złożonych zachowań. Drugim problemem mogą być „klasyczne” wyzwania dla IWA wynikające częściowo z ograniczeń optyki, jak skuteczność w gorszych warunkach oświetleniowych, odporność na fałszywe alarmy powodowane przez migające reklamy, drzewa, zwierzęta, oraz „trudniejsze” ujęcia - kiedy osoba jest tyłem do kamery, tyłem - bokiem lub w większej odległości, czyli kiedy trudniej jest rozróżnić ruchy kończyn.

Wydaje się, że trudno będzie tu uciec od zależności systemowych. W modelu przedstawionym przez OBRUM i PJATK, algorytmy analizowały wiele ścieżek ruchu kończyn i ciała każdej osoby na ekranie, co oznacza duże ilości danych. Dla zapewnienia odpowiednio dużych postaci, w złożonych miejskich scenach. Może to tworzyć

wysokie wymagania w zakresie infrastruktury, a więc wysokie koszty implementacji i utrzymania monitoringów opartych o uczenie maszynowe, przy pytaniu o stosunek skuteczności do ceny. Katowice na nowy monitoring, wyposażony w algorytmy analizy obrazu wydały niebagatelną kwotę 13 milionów złotych.

Wiedza o zarządzaniu monitoringiem miejskim jest coraz bardziej dostępna

Kolejne edycje Polskiej Normy 50132-7 przez blisko 20 lat wspierały podejście systemowe do projektowania – wskazywały kluczowe elementy systemu CCTV i zalecały projektantom sformułowanie wytycznych użytkowych. Aktualna norma PN-EN 62676-4:2015-06 kontynuuje tę filozofię. Opracowana przez brytyjską policję 20 lat temu metoda „wytycznych funkcjonalnych” nie traci nic z aktualności, oferując użytkownikom i projektantom przyjazną metodologię ustalania zależności funkcjonalnych technika – personel – procedury dla miejskiego dozoru wizyjnego [14]. Dostępne są dobre praktyki, artykuły i badania wskazujące zasady zarządzania miejskimi systemami monitoringu wizyjnego, np. „Karta demokratycznego zastosowania monitoringu wizyjnego” [15]. Warto pamiętać, że pod względem zasad zarządzania miejski system monitoringu wizyjnego nie różni się od innych organizacji, takich jak firma, basen czy przedsiębiorstwo komunikacji publicznej. ■

Miasto	Liczba kamer (stan na 2012 r.)	Liczba zdarzeń ujawnionych przez operatorów w 2013 r.		Średnia liczba zdarzeń na 1 kamerę / 1 rok		Średnia liczba zdarzeń na 1 kamerę / 1 miesiąc	
		Wszystkie	Bez zdarzeń w ruchu drogowym i nieprawidłowego parkowania	Wszystkie	Bez zdarzeń w ruchu drogowym i nieprawidłowego parkowania	Wszystkie	Bez zdarzeń w ruchu drogowym i nieprawidłowego parkowania
Radom	61	4255	4027	69,75	66,02	5,81	5.50
Warszawa	323	14015	14015	43,39	43,39	3,62	3.62
Gniezno	13	2500	539	192,31	41,46	16,03	3.46
Piekary Śląskie	18	653	595	36,28	33,06	3,02	2.75
Zamość	80	2499	2245	31,24	28,06	2,60	2.34
Kielce	95	2675	2637	28,16	27,76	2,35	2.31
Starachowice	16	704	407	44,00	25,44	3,67	2.12
Ząbrze	24	631	600	26,29	25,00	2,19	2.08
Poznań	251	7955	4497	31,69	17,92	2,64	1.49
Katowice	46	1362	675	29,61	14,67	2,47	1.22
Siedlce	12	316	156	26,33	13,00	2,19	1.08
Sieradz	17	332	182	19,53	10,71	1,63	0.89
Ostrowiec Świętokrzyski	70	773	692	11,04	9,89	0,92	0.82
Łęczna	10	564	64	56,40	6,40	4,70	0.53
Łęczycza	9	44	37	4,89	4,11	0,41	0.34
Nowy Tomyśl	10	35	31	3,50	3,10	0,29	0.26
Kraśnik	25	44	43	1,76	1,72	0,15	0.14
Ozorków	10	6	6	0,60	0,60	0,05	0.05
Częstochowa	18	3299	3222	183,28	179,00	20,36	19.89
Rotterdam	318	22131		69,59		5,80	

Częstochowa i Rotterdam nie były objęte kontrolą NIK

WNIOSKI

Mieszkańcy oczekują szybkiej i skutecznej reakcji na zagrożenie.

Podstawowym zadaniem miejskiego systemu monitoringu jest wykrycie zagrożenia i zapewnienia adekwatnej reakcji.

System monitoringu zawiera różne elementy – technikę, personel, procedury, które łączą różne zależności. Jeżeli jeden element nie działa, to ogranicza możliwość działania innych.

Zapewnienie sprawności każdego elementu i systemu jako całości wymaga skutecznego zarządzania.

Podstawowe zasady zarządzania miejskim systemem CCTV nie różnią się od zarządzania organizacjami czy firmami.

Literatura

- [1] <http://bip.podkarpacka.policja.gov.pl/download/41/76675/raportPBP2015.pdf>
- [2] red. Siemaszko P., *Geografia występków i strachu*. Polskie badanie przestępczości, 2007, Instytut Wymiaru Sprawiedliwości, Warszawa 2008 oraz kolejne edycje Polskiego badania przestępczości.
- [3] Gill M., Spriggs A., *Assessing the impact of CCTV*.
- [4] <http://www.surveillance-and-society.org/articles5%281%29/maps.pdf>
- [5] http://www1.uni-hamburg.de/surveillance/cctv_hh_english_summary.pdf
- [6] <http://www.statewatch.org/news/2007/nov/uk-national-cctv-strategy.pdf>
- [7] Pierzchała P., Wittich P., *Jak zbudować efektywny (nie efektywny) system nadzoru wizyjnego miasta*, „Systemy Alarmowe” nr 3/2007, s. 54.
- [8] https://pl.wikipedia.org/wiki/Teoria_system%C3%B3w
- [9] Wittich P., *Skuteczny monitoring, czy maszynka do wystawiania mandatów?*, „Systemy Alarmowe” nr 4/2014, s. 34.
- [10] Wittich P., Pierzchała P., *Częstochowa – organizacja bliska idealowi*, „Systemy Alarmowe” nr 1/2011, s. 13.
- [11] Wittich P., *Rotterdam – lepiej instalować w technikę niż w operatorów*, „Systemy Alarmowe” nr 5/2012, s. 20.
- [12] Pierzchała P., Wittich P., *Kielce – dobra koncepcja wdrażana w życie*, „Systemy Alarmowe” nr 5/2011, s. 10.
- [13] <http://www.cctv.org.pl/publikacje/poradniki-brytyjskiej-policji-police-scientific-development-branch/304-qfunkcjonowanie-centrow-nadzoru-systemu-monitoringu-wizyjnego-wnioski-z-obszerności>
- [14] <http://www.cctv.org.pl/publikacje/poradniki-brytyjskiej-policji-police-scientific-development-branch/307-qjak-przygotowa-wytyczne-funkcjonalne-dla-systemu-cctvq>
- [15] <http://www.cctv.org.pl/publikacje/aspekty-prawne/349-karta-demokratycznego-zastosowania-monitoringu-wizyjnego>

Kamery w miastach

Choć trudno to przyznać, niemal każdy system dozoru wizyjnego jest budowany z myślą o analizie zdarzeń post factum, w którym obraz z kamery stanowi nieprzetworzoną i wierną informację dotyczącą zajścia, tak istotną dla szybkiego wyjaśnienia zdarzeń. Niemniej takie potraktowanie systemu dozoru wizyjnego, zwłaszcza w ujęciu bezpieczeństwa publicznego, kłóci się z ogólną koncepcją Wielkiego Brata, który obserwuje, czuwa i stara się zapobiec najgorszemu. Okazuje się, że nie zawsze, a w zasadzie sporadycznie i nie wszędzie. A to z kolei wpływa na dobór urządzeń wykorzystywanych w systemie monitoringu.

RAPORT

Niedawno trafiłem na raport¹⁾ o inteligentnych miastach przygotowany przez Departament Planowania Przestrzennego z Politechniki Wiedeńskiej. Dokument jest dostępny w formie interaktywnej i umożliwia wykonanie zestawienia miast oraz zaprezentowanie tych interesujących na tle pozostałych. Badania dotyczyły wybranych aglomeracji z liczbą mieszkańców w przedziale od pięciuset tysięcy do miliona. Zwróciłem uwagę na wysoki wskaźnik indywidualnego poczucia bezpieczeństwa we wszystkich analizowanych polskich miastach – jeden z wyższych w Europie. Trudno to przełożyć bezpośrednio na fakt posiadania systemu dozoru wizyjnego, ten aspekt bowiem nie został wyszczególniony. Inną sprawą jest brak wskaźników skuteczności zainstalowanego systemu monitoringu, gdyż większość polskich miast w ogóle ich nie stosuje²⁾. W niewielu przypadkach, gdzie taka obserwacja została poczyniona, wykazano spadek przestępczości w zakresie od 7 do 90 proc. a policja wykazała wzrost wykrywalności przestępstw w wybranych lokalizacjach kamer³⁾.

Jan T. Grusznic

Magia kamer obrotowych

Większość systemów dozoru wizyjnego miast została zdominowana przez kamery szybkoobrotowe lub stałopozycyjne zainstalowane na głowicach uchylno-obrotowych. Wynika to głównie z dość ela-

stycznej funkcji tych kamer, które mogą stanowić stałopozycyjny punkt kamerowy i obserwować przez dłuższy czas stały fragment miasta, a jednocześnie wykonać precyzyjną obserwację zdarzenia ze znacznej odległości, gdy zajdzie taka potrzeba. Alternatywnie wykorzystuje się trasy dozoru po zaprogramowanych wcześniej pozycjach lub odtwarzających ciąg zmiennych zapamiętanych jako tura operatora. Niezależnie od typu uruchomionej trasy patrolowej kamera jest w ciągłym ruchu, dozoru dynamicznie przestrzeń wokół punktu kamerowego. Oba rozwiązania mają zalety i wady. W pierwszym przypadku obszar obserwacji jest znany, kamera bowiem zawsze wraca do punktu wyjściowego po zadanym czasie, gdy nie jest wykorzystywana przez użytkownika. Dzięki temu utrzymywana jest ciągłość obserwacji wcześniej zdefiniowanej strefy, a materiał archiwalny zwykle dotyczy zdarzeń zaobserwowanych właśnie na określonym obszarze. Periodycznie wykorzystuje się funkcję zmiany pozycji i ogniskowej, a wtedy taki materiał automatycznie jest oznaczany w systemie jako manualne przejęcie kontroli nad kamerą. Dzięki temu użytkownik potrafi szybko wskazać miejsca na osi czasu, gdy kamera była w ruchu, i szybko je przejrzeć albo też zignorować w przypadku wyszukiwania zdarzeń, wykorzystując automatyczną analizę obrazu w materiale archiwalnym.

W przypadku kamer poruszających się po trasie patrolowej wyróżnia się dwa jej typy: po pozycjach zaprogramowanych (presetach) oraz turę zaprogramowaną przez użytkownika w formie ciągłego ruchu. Ta druga wersja stanowi nagranie koordynat (najczęściej obrót, pochylenie, zoom) z odpowiednią częstotliwością (gęstość zapisu nie powinna być rzadsza niż raz na 1/15 s), które wynikają bezpośrednio z ruchu wskaźnikiem myszy po obrazie lub za pomocą manipulatora. Ruch w tym przypadku jest płynny w całym przebiegu trasy od jej początku do końca, a wszelkie przestoje w wybranych miejscach trasy są jej integralną częścią. Trasa dozoru wykorzystująca presetu należy do ruchu interwałowego, tj. w konkretnych cyklach zmieniają się koordynaty ustawienia kamery (najczęściej obrót, pochylenie, zoom, ostrość, czasami również wartość przysłony). Czas

przebywania w presece może się różnić w zależności od potrzeb i celu obserwacji, czas przejścia między kolejnymi pozycjami natomiast na ogół jest jak najszybszy. Kamera po przejściu do kolejnego presetu zachowuje się jak kamera stałopozycyjna, tj. przez określony czas obserwuje wybraną scenę.

Praca z trasami dozoru łączy się z ograniczoną w czasie obserwacją wybranej przestrzeni. Oznacza to, że pomimo teoretycznie dużego pokrycia terenu obserwowany jest tylko wycinek obszaru przez względnie krótki okres, co znacznie redukuje możliwość wykrycia anomalii przez algorytmy analizujące zawartość obrazu (VCA) czy nawet przez przeszkolonego operatora. W przypadku materiału archiwalnego odnalezienie konkretnego zdarzenia bez znajomości dokładnych parametrów czasowych wymaga więcej uwagi i... czasu, ponieważ materiał w żaden sposób nie jest znakowany. Oznacza to, że dane wizyjne muszą być przejrzane przez użytkownika tradycyjnie. Inną sprawą jest brak pewności, czy incydent w ogóle został zarejestrowany, ponieważ kamera odtwarzająca turę operatora mogła znajdować się w zupełnie innym położeniu.

W przypadku wykorzystania trasy po presetach istnieje możliwość automatyzacji pracy operatora oraz sposobu przeglądania materiału archiwalnego. Każda pozycja kamery PTZ jest bowiem programowana z konkretnego powodu, wynikającego z analizy zdarzeń, ryzyka, liczby zgłoszeń lub interwencji itp.

Operator dla każdego presetu ma scenariusze, na co zwraca uwagę. W Częstochowie np. każda kamera ma kartę, w której zostały opisane cele i priorytety dozoru oraz miejsca szczególnego zainteresowania. Operator jest zobowiązany do patrolowania tych miejsc za pomocą kamery i ich oznaczania w zapisie obrazu, kiedy kieruje na nie obiektyw. Proces ten jest podstawowym kryterium oceny jego pracy. Zmusza to zatem zatrudniony personel do gruntownego poznania obszarów objętych dozorem i uważnego przyglądania się miejscom, w których dochodzi do zagrożeń. W efekcie operatorzy mają także okazję obserwować zachowania ludzi, którzy przebywają w tych miejscach. W związku z tym prawdopodobieństwo, że zauważą niepokojące sygnały, się zwiększa [4].

A co w przypadku, gdy operatorów jest mniej niż kamer? Otóż kamera ustawiona w presece może ten fakt oznaczać automatycznie w materiale archiwalnym. Dzięki temu możliwy jest przegląd nagrań tylko tych obrazów, które są związane z daną pozycją zaprogramowaną. Stanowi to niewątpliwą korzyść wynikającą z przyspieszenia analizy materiału archiwalnego, ograniczonego tylko do scen, którymi jesteśmy zainteresowani. Przykładowo, jeśli trasa dozorowa ma 12 presetów, a kamera pozostaje w każdym z nich przez 5 min, oznacza to, że wykonanie pełnej trasy trwa 1 godzinę. Zamiast przeglądać

cały materiał, można odnaleźć tylko sekwencje skojarzone z miejscami znajdującymi się w kręgu zainteresowania. Jeśli jest to jedna scena, oznacza to przegląd tylko 5 min zapisu archiwalnego, nie zaś całej godziny. Wyszukanie materiału ogranicza się natomiast do wyszukania oznaczonego nagrania z numerem pozycji zaprogramowanej i zakresu czasu.

Czas wysokich rozdzielczości

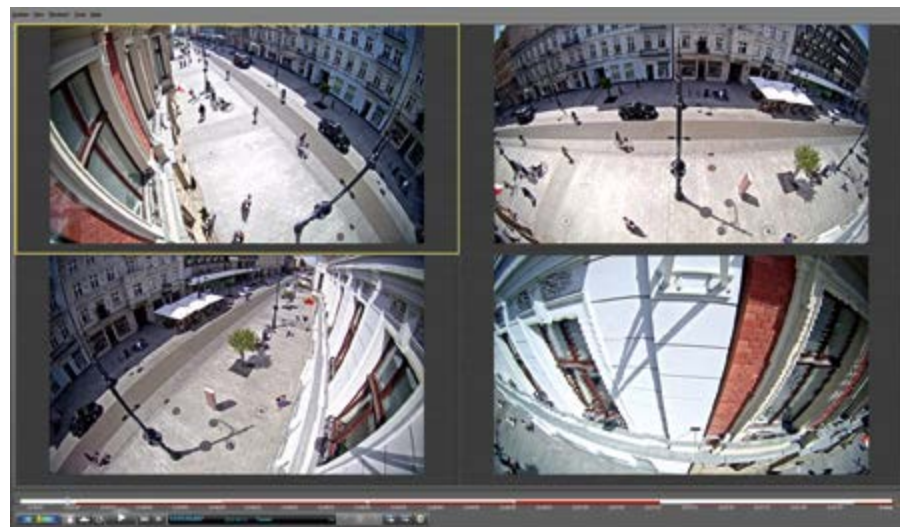
Jako rezultat analizy ostatnich incydentów o charakterze terrorystycznym w miastach Europy Zachodniej zalecono wprowadzenie zmian w miejskich wizyj-

nach systemach dozoru. Oprócz wciąż popularnych kamer szybkoobrotowych zaczęły pojawiać się kamery stałopozycyjne o rozdzielczości znacznie przewyższającej standard 2160p. Takie modele zostały już zainstalowane w punktach gromadzenia się osób w Berlinie po wydarzeniu przed Bożym Narodzeniem zeszłego roku. Dzięki wysokiej rozdzielczości użytkownicy systemu są w stanie na bieżąco monitorować tłum oraz, jeśli to potrzebne, powiększać cyfrowo wybrane części obrazu w celu odczytania szczegółów, nie tracąc jednocześnie ogółu z podglądu. Jest to niewątpliwą przewagą nad kamerami PTZ, które realizując zbliżenia, nie mogą utrzymać w dozorze ogólnego planu. Zasięg detekcyjny kamer o wyższej rozdzielczości w porównaniu do 1080p oczywiście będzie większy. Dla tego samego kąta obserwacji (67°) kamera np. 20 Mpix umożliwia rozpoznanie (8 mm/pix) z odległości 33 m, podczas gdy kamera full HD – z 12 m. PTZ jednak zyskują przewagę dzięki wielokrotnemu zbliżeniu optycznemu, co umożliwia rozpoznanie osoby z odległości ponad 370 m (zoom 30x) i w tym są trudne do zastąpienia. Cały czas jednak za pomocą kamer PTZ trudno obserwować ogólny plan i detale jednocześnie. Problem znany od dawna niedawno znalazł rozstrzygnięcie. Producenci kamer zdecydowali się wprowadzić do oferty rozwiązanie uzupełniające w postaci dodatkowych kamer stałopozycyjnych instalowanych dokoła jednostki PTZ (rys. 1). Kamery te są dostępne w postaci dodatkowego modułu nakładanego na kamerę PTZ lub już w wersji zintegrowanej, a ich rolą jest niezależny dozór najbliższej przestrzeni wokół punktu kamerowego (rys. 2). Za pomocą tego modułu możliwe jest sterowanie kamerą PTZ z obrazów kamer stałopozycyjnych oraz oznaczenie

Oprócz wciąż popularnych kamer szybkoobrotowych zaczęły pojawiać się kamery stałopozycyjne o rozdzielczości znacznie przewyższającej standard 2160p.



Rys. 1. Przykładowy zestaw punktu kamerowego składający się z kamery PTZ i kamer dookólnych zainstalowanych na elewacji budynku przy ul. Piotrkowskiej w Łodzi (źródło: materiały firmy Sprint SA)



Rys. 2. Obraz ukazujący widok na ul. Piotrkowską w Łodzi z czterech kamer umieszczonych wokół kamery PTZ, pozwalający na ciągły dozór przestrzeni w okolicy punktu kamerowego



Rys. 3. Paryż, widok na wieżę Eiffla – obraz z przetwornika Canon 250MPX APS-H. Na górze: zaznaczony obszar zoomu cyfrowego, na dole: widoczny powiększony fragment (źródło: <https://petapixel.com/2015/10/18/a-demo-of-canons-250mp-sensor-and-its-turbulence-removal-feature/>)

na nich pozycji kamery szybkoobrotowej. Sumaryczna rozdzielczość takich modułów kamerowych sięga 8 Mpix, co nazwałbym obecnie standardem. Nie jest to rozwiązanie rewolucyjne, ale idące z duchem czasu i wynikające z wymagań użytkowników. Rewolucyjnym natomiast można nazwać rozwiązanie zaprezentowane przez firmę Canon na targach EXPO w Paryżu w 2015 r. Wówczas koncern pokazał matrycę CMOS zawierającą blisko 250 mln aktywnych pikseli. Już podczas targów rozważano zastosowanie tej technologii głównie w wyspecjalizowanych narzędziach dozoru i zapobiegania przestępczości, przyrządach pomiarowych o wysokiej rozdzielczości i innym sprzęcie przemysłowym [5]. Przetwornik obrazu wielkości APS-H (29,2 x 20,2 mm) dostarcza obrazy o wy-

miarach 19580 x 12600 pix. Wielkość pojedynczego piksela wynosi ok. 1,6 µm, czyli podobnie jak dla przetworników o wielkości 1/3" i rozdzielczości 4K. Czas odczytu danych z matrycy wynosi 1,25 mld pikseli na sekundę, co w przeliczeniu na liczbę klatek dla podanej rozdzielczości przekłada się na 5 kl./s. Canon zapewnia, że ujęcia wykonane za pomocą nowatorskiego przetwornika zapewniają odczytanie numerów samolotu z odległości 18 km (przy wykorzystaniu obiektywu o ogniskowej 800 mm). Tak wysokie rozdzielczości nie są pozbawione wad. Wymagają bowiem wykorzystania większej optyki, efekt dyfrakcji szybciej przybiera na sile ze względu na zmniejszenie powierzchni piksela, głębia ostrości jest zdecydowanie krótsza, ponieważ zwęża się wraz ze wzrostem wielkości przetwornika, a ruchy mas powietrza skutecznie obniżają

Wysokie rozdzielczości nie są pozbawione wad – wymagają wykorzystania większej optyki, efekt dyfrakcji szybciej przybiera na sile, głębia ostrości jest zdecydowanie krótsza, a ruchy mas powietrza skutecznie obniżają jakość obrazu przy obserwacji z dużej odległości.

jakość obrazu przy obserwacji z dużej odległości. A jednak zaprezentowane możliwości promowanego produktu udowodniły zasadność kontynuowania prac nad rozwojem takich matryc i pokonywania kolejnych trudności z nimi związanych. Przykłady możliwości można zobaczyć na rys. 3 – odległość od punktu instalacji kamery do wieży Eiffla wynosi 20 km. Na zastosowanie produkcyjne przyjdzie nam pewnie jeszcze trochę poczekać. Chwilowo tak wysokie rozdzielczości osiąga się przez przetwarzanie obrazów z wielu kamer jednocześnie najczęściej o rozdzielczości nie wyższej niż 4K, zgromadzonych w jednej obudowie. Każda kamera strumieniu obraz niezależnie, który następnie jest „klejony” po stronie stacji klienckiej (tzw. *stitching*). Tak spreparowany obraz jest prezentowany na ekranie jako jeden, dając możliwości przybliżania cyfrowego. Niewątpliwie koncepcja *stitchingu* pozwala na uzyskanie większej głębi ostrości, zróżnicowanie ogniskowych w zakresie pola obserwacyjnego, zastosowanie mniejszych przetworników i dzięki temu obiektywów. Niestety, aby móc w pełni korzystać z zalet takiej kamery, należy dysponować konkretnym oprogramowaniem producenta. Próba integracji z innymi platformami skutkuje podłączeniem każdej kamery niezależnie i podglądem strumieni wizyjnych jak w przypadku tradycyjnych źródeł obrazu. Kamery wieloprotetwornikowe wymagają odpowiedniego zaprojektowania instalacji, w tym precyzyjnego ustawienia punktów ostrości. Stąd nie są to rozwiązania z tzw. półki, tak jak w przypadku kamer PTZ czy też wysokorozdzielczych kamer jednoprotetwornikowych.

Big Data rozwiązaniem na rosnącą liczbę danych wizyjnych?

Raport NIK dotyczący systemów monitoringu miejskiego dość brutalnie punktuje sposób wykorzystania systemów kamer zainstalowanych w przestrzeni publicznej. Wśród wielu uchybień pojawia się niski poziom wykrywalności wynikający głównie z przypisania zbyt wielu kamer jednemu operatorowi. Tymczasem operatorzy systemu dozoru wizyjnego w miastach uważają, że maksymalna liczba obrazów, jakie są w stanie efektywnie monitorować, wynosi 16. Nieco ponad połowa operatorów uważa nawet, że nie powinna przekraczać od 1 do 4 [6]. Dane eksperymentalne wskazują, że wraz ze wzrostem liczby nadzorowanych kamer maleje efektywność pracy obserwatorów próbujących wykryć pojawiające się zdarzenia. Wnioski te idą w parze z wynikami badań Ticknera i Poultona, którzy porównywali efektywność pracy przy zwiększającej się liczbie monitorów. Przy 4, 9 i 16 monitorach pokazujących bardzo ruchliwe obszary miejskie skuteczność działań operatorów przy wykrywaniu postaci wyniosła odpowiednio: 93, 84 i 64 proc. [7]. Współczesny system monitoringu wizyjnego charakteryzuje się ciągłym wzrostem liczby instalowanych kamer, a obecnie wzrostem ich rozdzielczości, a co za tym idzie zwiększeniem liczby szczegółów w obrazie.

Częste przeglądanie dużej liczby takich obrazów w celu uzyskania niezbędnych informacji o obserwowanych obszarach lub szybkiego zidentyfikowania zdarzeń wymagających szczególnej koncentracji sprawia, że długotrwałe prowadzenie obserwacji staje się trudniejsze, a niektóre zadania wymagające skupienia wzroku na szczegółach, np. odczytanie znaków szczególnych na ciele lub ubraniu obserwowanej osoby, są wręcz niemożliwe do wykonywania. Według wytycznych PSDB [8] zaleca się projekcję maksymalnie czterech obrazów na jednym monitorze, jeżeli operator musi skupiać się na szczegółach [9].

Przy powszechnie stosowanych technologiach komputerowych umożliwiających prezentację obrazów na wiele spo-

ICT (INFORMATION AND COMMUNICATIONS TECHNOLOGY), CZYLI TELEINFORMATYKA

Pojęcie ICT obejmuje szeroki zakres wszystkich technologii umożliwiających przetwarzanie i przesyłanie informacji. W zakres pojęciowy technologii ICT wchodzi wszystkie media komunikacyjne (Internet, sieci bezprzewodowe, sieci Bluetooth, telefonia stacjonarna, komórkowa, satelitarna, technologie komunikacji dźwięku i obrazu, radio, telewizje itp.) oraz media umożliwiające zapis informacji (pamięci przenośne, dyski twarde, dyski CD/DVD, taśmy itp.), a także sprzęt umożliwiający przetwarzanie informacji (komputery osobiste, serwery, klastry, sieci komputerowe itp.). Ponadto technologie ICT obejmują gamę aplikacji informatycznych oraz złożonych systemów IT umożliwiających realizację przetwarzania i przesyłania danych na wyższym poziomie abstrakcji niż poziom sprzętowy.

sobów kładzie się nacisk na rozwiązania zwiększające efektywność pracy operatora. W procesie projektowania systemu kamer powinno się dokładnie rozważać liczbę obrazów z kamer oraz stopień ich szczegółowości do nadzoru przypadających na jednego operatora, a także wykorzystanie systemów wspomagających skuteczność działań podejmowanych przez użytkowników systemu dozoru wizyjnego. Należy mieć świadomość, że ta decyzja będzie miała kluczowe znaczenie dla osiągnięcia przez system zakładanych celów, gdyż istnieją granice efektywnego nadzoru. Jednocześnie należy mieć świadomość, że człowiek nie jest w stanie wszystkiego przeanalizować. Gdybyśmy przeliczyli liczbę danych, jaka dociera do każdego z nas, to według różnych źródeł ta wartość wynosi ok. 109 b/s, czyli ok. 1 Gb/s. Uświadomionych informacji jest jednak tylko niewielka liczba, od 10 do 100 b/s [10].

Mimo że badania PSDB i inne nie podają żadnych rozstrzygających danych dotyczących maksymalnego czasu prowadzenia efektywnej obserwacji przez operatora CCTV, to operatorzy, monitorując obrazy z kamer w centrach miast, stwier-

dają, że maksymalny czas obserwacji waha się od 30 min do 2 godz. Jest to złożona kwestia, gdyż czas obserwacji będzie zależał od wielu czynników, nie tylko od tych związanych z wymogami pracy. Przepisy BHP dotyczące ekranów wskazują, aby w celu uniknięcia nadmiernego zmęczenia wywołanego używaniem tego wyposażenia, robić krótkie, częste przerwy, które mają korzystniejszy wpływ niż sporadyczne, dłuższe przerwy [11]. Niestety, koncentracja operatora systemu obserwującego pojedynczą scenę spada liniowo z upływem czasu. Już po 30 min pracy w systemie skuteczność wykrywania zdarzeń przez użytkownika zmniejsza się o 75 proc. [12].

Z tego m.in. powodu algorytmy wyszukujące w danych wideo wzorce zachowań, kształtów, ruchu lub rozmieszczenia punktów szczególnych, stanowią jeden z chętniej wykorzystywanych elementów do szybkiego oznaczania miejsc ich występowania w materiale wizyjnym. Analiza zawartości obrazu, jaką znamy z niektórych filmów szpiegowskich, jest stosowana w profesjonalnych systemach dozoru wizyjnego, również miejskich. Na ich podstawie można bezinwazyjnie określić prawdopodobieństwo posiadania broni lub improwizowanych ładunków wybuchowych, pojedynczego ruchu w tłumie lub przemieszczania się jednostek w przeciwnym kierunku do naturalnego przepływu osób. Możliwa jest również analiza rysów twarzy w większych skupiskach ludzi i porównywanie wyników z konkretną bazą

osób. Informacje z analizy same w sobie nie są użyteczne dla użytkownika, jeśli nie zostały powiązane z odpowiednimi procedurami lub innymi danymi i w przystępny sposób zaprezentowane. Rola samego rozkładu obrazu jest ograniczona do dostarczenia informacji będącej podstawą do dalszych działań podejmowanych automatycznie przez system lub świadomie przez użytkownika. Sposób analizy będzie różnił się w zależności od charakteru poszukiwanych zmian. Każdy algorytm badający zawartość obrazu działa inaczej, ale upraszczając, obraz jest „rozdzielany” na fragment przedstawiający jego „statyczną” część oraz obiekty nienależące do tła. Informacja o każdym obiekcie jest „opisem” miejsca zajętego przez niego w obrazie, wielkości czy wektora ruchu powiązanych ze znacznikiem czasu itp. Te dane przetworzone w ramach *Big Data* dostarczą nowych informacji wynikających chociażby z połączenia z danymi z innych kamer, czujników czy wiadomości z portali społecznościowych itd.

Big Data to termin odnoszący się do dużych, zmiennych i różnorodnych zbiorów danych, których przetwarzanie i analiza jest trudna, ale jednocześnie wartościowa, ponieważ może prowadzić do pozyskania wiedzy [13]. W przypadku miast celem jest lepsze zrozumienie zachodzących zmian i w konsekwencji lepsze zarządzanie aglomeracją i określenie kierunków rozwoju w przyszłości. Przetwarzanie dużych zbiorów danych otwiera przed nimi zupełnie nowe możliwości. Biorąc przykład tylko

z rynku komercyjnego, organizacje przetwarzające w sposób właściwy posiadane dane prześcignęły swoich konkurentów o 5–6 proc. Tymczasem w miastach rozwijających się rzeczywistość jest taka, że operacje są nieskoordynowane, a przechwytywanie danych jest wciąż trudnym procesem ręcznym. Współczesne środowiska korzystają ze skonsolidowanych usług w różnych obszarach, takich jak zarządzanie zasobami, flotą i personelem. Są tam dostępne odpowiednie informacje ułatwiające utrzymanie ciągłości świadczonych usług, ogólną satysfakcję klientów oraz zrozumienie wąskich gardeł. Jest to możliwe dzięki wdrożeniu hurtowni danych i analiz biznesowych – zasobów ICT (*patrz: ramka*), które wciąż rozwijają nowoczesne miasta. Wzorec syntezy danych, stanowiący podstawę tego typu środowiska, pozwala na wykorzystanie różnorodnych źródeł danych, takich jak wideo z kamer dozoru wizyjnego, audio, media społecznościowe, logi czujników, systemy kontroli procesów i zbierania danych (SCADA), tradycyjne struktury i niestrukturyzowane dane, które mają być połączone ze sobą w celu wsparcia wizji miasta [14].

Smart city oparte na kamerach

Droga rozwoju monitoringów miejskich nie jest już dyktowana jedynie troską o bezpieczeństwo mieszkańców, które – jak wskazują oceny – jest zadowalające. Niebawem, jeśli jeszcze nie jest to powszechne, kamery będą należały do serii istotnych czujników, które zbierają

informacje pozwalające na szybkie reagowanie. Przykład Londynu jako jednego z trójki miast, które w obszarze *smart* (obok Paryża i Nowego Jorku) rozwijają się najszybciej, pokazuje, w jaki sposób kamery dozoru wizyjnego pozwoliły osiągnąć to wyróżnienie. Od dłuższego czasu rozwija wizualizację miasta 3D w połączeniu z danymi z kamer CCTV i informacjami o nowych inwestycjach budowlanych, by płynniej zarządzać ruchem w mieście dzięki redukcji nieuzasadnionych robót drogowych oraz utrudnień w ruchu wynikających z tego, że kilka firm budowlanych działa na zbyt bliskim sobie terenie. Mapa 3D aktualizowana w czasie rzeczywistym ma być ukończona do 2020 r. i zostanie wtedy udostępniona wszystkim zainteresowanym firmom.

Londyn wykorzystuje monitoring wizyjny do detekcji wypadków i skrócenia czasu dotarcia na miejsce zdarzenia. Dane są również pomocne w projektowaniu ścieżek rowerowych oraz budowaniu bardziej efektywnych sposobów komunikacji dla pieszych i osób niepełnosprawnych. Korzystając z analizy danych, rozwija transport publiczny w zrównoważony sposób, by doprowadzić w 2020 r. do 50-proc. redukcji zanieczyszczania powietrza przez komunikację miejską. Jeśli się to uda, stolica Wielkiej Brytanii będzie miała najczystsze powietrze wśród wszystkich głównych miast Europy.

Przy okazji – Warszawa w rankingu IESE *Cities in Motion* zdobyła 74. miejsce na 181 badanych miast [15]. ■

Literatura

- [1] <http://www.smart-cities.eu/>
- [2] Najwyższa Izba Kontroli, Informacja o wynikach kontroli „Funkcjonowanie miejskiego monitoringu wizyjnego”.
- [3] Tamże.
- [4] P. Wittich, Skuteczna obserwacja wymaga dobrego zarządzania, „a&s Polska”, 2/2017.
- [5] Informacja prasowa Canona z 7.09.2015 r., <http://global.canon/en/news/2015/sep07e.html>
- [6] M.L. Garcia, *The design and evaluation of physical protection systems*, Butterworth-Heinemann 2001r.
- [7] A.H. Tickner, E.C. Poulton, Monitoring up to 16 Synthetic Television Pictures Showing a Great Deal of Movement. *Ergonomics* (14)4, 1973 r.
- [8] PSDB – (Police Scientific Development Branch) Policyjny Departament Rozwoju Technicznego przy Ministerstwie Spraw Wewnętrznych w Wielkiej Brytanii został powołany do przeprowadzenia niezależnych badań zwiększenia skuteczności wykorzystywanych technologii w zapobieganiu przestępstw. W roku 1992 zapoczątkował on program How it Works, poprawy ergonomii i wykorzystania stanowisk monitoringu wizyjnego i alokacji punktów kamerowych. (<http://www.crimereduction.home.office.gov.uk>)
- [9] E. Wallace, C. Diffley, CCTV: Making It Work. CCTV Control Room. *Ergonomics*, PSDB 14/98.
- [10] Nauka o pracy - bezpieczeństwo, higiena, ergonomia, pakiet edukacyjny dla uczelni wyższych, prof. dr hab. med. Bolesław Gwóźdź, Śląska Akademia Medyczna, <http://nop.ciop.pl/>
- [11] Na podstawie Rozporządzenia Ministra Pracy i Polityki Socjalnej z dnia 1 grudnia 1998 r. w sprawie bezpieczeństwa i higieny pracy na stanowiskach wyposażonych w monitory ekranowe (DzU 1998.148.973) i Display Screen Equipment Work - Guidance on Regulations (ISBN 0717604101).
- [12] G. Modliński, Inteligentne systemy monitoringu wizyjnego, 2005.
- [13] https://pl.wikipedia.org/wiki/Big_data
- [14] Raport Deloitte, Smart Cities, Big Data, styczeń 2015.
- [15] <http://www.unicard.pl/blog/3-najbardziej-inteligentne-miasta-swiata-smart-city/>

Wpływ zastosowania kamer sieciowych na poprawę komfortu życia w inteligentnym mieście

Kamery sieciowe są wykorzystywane na całym świecie do monitorowania ruchu ulicznego, prowadzenia dozoru wizyjnego oraz innych zastosowań związanych z bezpieczeństwem.

Andrea Sorri

Director Business Development,
Government, City Surveillance
and Critical Infrastructure,
Axis Communications

Oparte na technologii przyszłości, wypierają analogowe systemy CCTV, których możliwości znacznie przewyższają. W dobie Internetu Rzeczy przyczyniają się do usprawnienia funkcjonowania inteligentnych miast, poprawy jakości życia, przemieszczania się i pracy ich mieszkańców.

Zastosowania kamer sieciowych są rozległe – od systemów informacji miejskiej, w których stanowią kluczowy element centrum monitoringu nadzorującego różne funkcje miasta związane z bezpieczeństwem, energią, zdrowiem, ruchem ulicznym i transportem, po zrównoważone zarządzanie infrastrukturą miasta z uwzględnieniem rozwiązań środowiskowych obejmujących monitorowanie jakości powietrza, poziomu hałasu czy promieniowania ultrafioletowego. Ponadto urządzenia te można wykorzystać w sposób innowacyjny w handlu, rozrywce i turystyce,

w szczególności we współpracy z technologiami mobilnymi i lokalizacyjnymi.

W artykule przedstawiono kilka możliwych zastosowań pod kątem inteligentnych miast.

Wirtualne miasto z mapami 3D w czasie rzeczywistym

Zarówno mieszkańcy miast, jak i odwiedzający je turyści chcą śledzić na bieżąco informacje o zdarzeniach, problemach komunikacyjnych czy zatłoczonych miejscach, które należy omijać. Potrzeby te spełniają trójwymiarowe modele wirtualnego miasta przekazywane na telefony komórkowe, dostarczające wygodnie, w czasie rzeczywistym potrzebnych informacji. Dzięki technologii rozszerzonej rzeczywistości rolę inteligentnych czujników mogą spełniać kamery sieciowe rozmieszczone w strategicznych punktach miasta. Mapę 3D składającą się z kilku warstw aktualnych informacji, w tym przekaz na żywo obrazu, utworzy zaawansowane oprogramowanie. Zastosowanie tego typu map jest rozległe – od zapewnienia bezpieczeństwa po przemysł, ochronę zdrowia, edukację, rozrywkę czy reklamę.

Lepsza komunikacja z mieszkańcami

Władze miejskie są zobowiązane informować mieszkańców, których stale przybywa, o sytuacji w mieście. W tym celu muszą posiadać sprawne narzędzia komunikacji, szczególnie w sytuacjach zagrożeń bądź konieczności powiadomienia w czasie rzeczywistym o utrudnieniach występujących w określonych rejonach miasta. Na ekranach zainstalowanych przy głównych placach czy stacjach kolejowych służby miejskie, na podstawie informacji z kamer sieciowych, mogą wyświetlać ważne komunikaty ostrzegające przed niebezpieczeństwem oraz zalecać zachowania.

Zadowoleni mieszkańcy

Dzisiaj ludzie zwykle noszą ze sobą smartfony. Aplikacja mobilna z lokalizacją GPS umożliwia poinformowanie odpowiednich służb miejskich o problemach typu przepełniony koszyk na śmieci czy zepsuta sygnalizacja uliczna. Służby mogą weryfikować zgłaszane nieprawidłowości za pomocą własnej sieci kamer i decydować o najlepszym i najszybszym sposobie ich usunięcia, a poprzez komunikację zwrotną w tej samej aplikacji

przekazać mieszkańcom wiadomości o podjętych działaniach. W efekcie sami mieszkańcy będą przekazywać informacje o podejmowanych przez miasto działaniach, które mają służyć poprawie jakości ich życia.

Wykorzystanie informacji z mediów społecznościowych

Media społecznościowe, takie jak Facebook czy Twitter, są istotnym źródłem informacji dla policji, mediów oraz innych użytkowników, których może dotyczyć konkretne zdarzenie. Kiedy służby miejskie dowiedzą się o zdarzeniu dzięki wyświetlającym się słowom kluczom, dzięki kamerom sieciowym mogą natychmiast pozyskać informację wizualną, zlokalizować problem, monitorować sytuację i ocenić jej wagę. Mogą połączyć treści publikowane w mediach społecznościowych z danymi pochodzącymi z kamer sieciowych, inteligentnych czujników oraz innych aplikacji i wprowadzić je do dużych zbiorów danych (*big data*) umożliwiających analizowanie zdarzeń i reakcji.

Śledzenie i odnajdywanie przedmiotów

Klucze, portfele, telefony, laptopy i rowery to najczęściej

gubione lub kradzione przedmioty. System zdolny śledzić utracone rzeczy byłby przydatny zarówno dla właścicieli, jak i policji. Taki system mógłby się opierać na czujnikach i technologii GPS. Kamery sieciowe dostarczałyby potrzebny materiał wizyjny umożliwiający policji lub innym służbom miejskim przeprowadzenie drobiazgowego dochodzenia.

Zdalna eskorta pieszych

Nieoświetlone przejścia czy parki nocą nie należą do bezpiecznych miejsc. Chcąc chronić przechodniów i zapewnić im poczucie bezpieczeństwa, służby miejskie mogłyby zaproponować aplikację mobilną łączącą smartfon użytkownika bezpośrednio z systemem monitoringu miejskiego. Wbudowana funkcja wywołania alarmowego umożliwiłaby nawiązanie bezpośredniego kontaktu z operatorem policji, a połączenie danych lokalizacji i kamer sieciowych z inteligentnym oświetleniem umożliwi operatorowi w centrum nadzoru śledzenie trasy użytkownika i bezpieczne przeprowadzenie przez potencjalnie niebezpieczne obszary.

Monitorowanie za pomocą dronów

Latające drony to coraz częstszy widok. Kilka razy niemal doszło do kolizji dronu z samolotem. Mogą też być wykorzystywane do celów niezgodnych z prawem, np. szpiegostwa czy przenoszenia niebezpiecznych materiałów. Dlatego urządzenia te muszą być zdalnie monitorowane. Kamery sieciowe można wykorzystać przez całą dobę do śledzenia i monitorowania ruchu dronów z odległości do 100 m. Mogą także wspomagać ochronę przed dronami rozległych obiektów przemysłowych czy biurowców. Zapewniają sygnalizację alarmu w czasie rzeczywistym oraz identyfikację potencjalnych zagrożeń, nawet jeżeli te znajdują się wysoko nad ziemią.

Blokowanie niebezpiecznych zachowań w pracy

Kamery sieciowe mogą służyć do monitorowania placów budowy, robót drogowych czy potencjalnie niebezpiecznych miejsc pracy w celu zapobiegania wypadkom, jak również zabezpieczenia przed dostępem osób nieupoważnionych. Mogą też w czasie rzeczywistym monitorować warunki w miejscach

niebezpiecznych i sygnalizować alarmem, gdy np. zachowanie robotnika stanowi zagrożenie dla niego samego bądź innych.

Poprawa bezpieczeństwa pieszych i rowerzystów

W inteligentnych systemach zarządzania ruchem ulicznym szczególnie nacisk kładzie się na poprawę bezpieczeństwa rowerzystów i pieszych przechodzących przez jezdnię. Stosowanie jaskrawych świateł ostrzegawczych, wznoszenie fizycznych barier czy odtwarzanie komunikatów akustycznych, zwłaszcza w warunkach zmniejszonej przejrzystości powietrza, mogą stanowić proste, ale skuteczne sposoby informowania kierowców o zamiarze przejścia przez jezdnię pieszych czy rowerzystów. Stosowanie tego typu rozwiązań przyczyni się do zmniejszenia liczby wypadków z udziałem pieszych czy rowerzystów, a tym samym zwiększenia bezpieczeństwa miejskich ulic.

Zarządzanie parkingami

Znalezienie miejsca do parkowania w zatłoczonych centrach miast graniczy niemal z cudem. System zawierający kamery sieciowe z aplikacjami analitycznymi oraz funkcjami zli-

czania pojazdów byłby zdolny dostarczyć w czasie rzeczywistym informacje o dostępnych miejscach parkingowych, które następnie zostałyby przesłane kierowcom poprzez aplikację mobilną, wyliczając dodatkowo najszybszą trasę do wolnego miejsca na podstawie aktualnej lokalizacji pojazdu. Zarządzanie miejscami parkingowymi dla niepełnosprawnych też może opierać na tej samej zasadzie, co zapewni, że z tych miejsc będą korzystały tylko pojazdy z odpowiednimi uprawnieniami.

Przytoczone przykłady nie wyczerpują potencjalnych obszarów zastosowań kamer sieciowych współpracujących z innymi czujnikami, systemami informatycznymi oraz rozwiązaniami w zakresie analizy danych, będącymi częścią sieci inteligentnego miasta. Choć nadal będą odgrywać istotną rolę w wykrywaniu przestępstw, ochronie infrastruktury i skutecznym reagowaniu na nagłe zdarzenia, czas już wyjść poza schematy i rozpocząć poszukiwanie nowych obszarów zastosowań, w których kamery sieciowe wykażą swój potencjał – poprawa komfortu życia mieszkańców miast. ■



IndigoVision

praktyczny system monitoringu miejskiego

Jednym z rozwiązań, które cieszy się uznaniem operatorów obsługujących systemy monitoringu miejskiego, jest produkt brytyjskiej firmy IndigoVision. Platforma Control Center wraz z transponderami IP była jednym z pierwszych tego typu rozwiązań w technologii IP na polskim rynku.

Platforma została wdrożona w kilkudziesięciu miejskich systemach monitoringu, oferując wszystkie niezbędne elementy systemu CCTV w postaci różnego typu kamer, profesjonalnych urządzeń do rejestracji, funkcjonalnego oprogramowania oraz wielu modułów integracji. Zmieniony pod koniec ubiegłego roku sposób licencjonowania zwiększył konkurencyjność rozwiązania, a tym samym stworzył perspektywę na znacznie szersze zastosowania w małych i średnich obiektach. Budując system oparty w całości na urządzeniach marki IndigoVision, można w pełni zarządzać wszystkimi elementami, łącznie z ich konfiguracją z poziomu aplikacji do zarządzania Control Center.

Architektura systemu

Zanim zostaną omówione cechy funkcjonalne niezwykle przydatne w trakcie codziennej pracy operatorów obsługujących miejskie systemy monitoringu, należy zwrócić uwagę na budowę systemu i elementy gwarantujące stabilną i niezawodną pracę. Zastosowanie architektury DNA sprawia, że w systemie IndigoVision można mówić o braku pojedynczego punktu awarii. Oznacza to, że uszkodzenie któregoś z elementów systemu nie ma wpływu na

pracę pozostałych. W typowej architekturze klient-serwer w przypadku uszkodzenia serwera rejestracji system jest pozbawiony też podglądu, ponieważ to właśnie serwer odpowiada za kierowanie strumienia z kamer do jednostek wyświetlających obrazy. W IndigoVision każda kamera wysyła strumienie niezależnie – do stacji podglądu i urządzeń rejestrujących. Zapewnienie jak największej niezawodności systemu jest jednym z głównych wyzwań stawianych przed inżynierami działu rozwoju IndigoVision. Producent kładzie duży nacisk na odpowiednie przygotowanie najbardziej newralgicznego elementu systemu, jakim jest rejestrator. Wszystkie urządzenia, począwszy od wersji Enterprise, są wyposażone w macierz RAID, poziom 5 lub 6. Każde urządzenie oparte na oprogramowaniu Linux lub Windows zawiera dwie niezależne karty sieciowe, redundantne zasilacze, dwa kontrolery RAID. Oferuje też usługę ProSupport, co oznacza, że w przypadku problemu z rejestratorem w ciągu 48 godzin od zgłoszenia w obiekcie pojawi się inżynier firmy IndigoVision lub partnera technologicznego, który dokona naprawy. Nowy sposób licencjonowania umożliwił łatwe, bezpłatne uruchomienie funkcji serwera awaryjnego. Stała kontrola

obecności dotyczy wszystkich urządzeń w systemie. Tym samym, jeżeli jakiś serwer się nie zgłasza, strumienie z kamer, które dotychczas obsługiwał, są automatycznie kierowane do innego rejestratora. Taka budowa i konfiguracja systemu stanowi gwarancję ciągłości zapisu. Kolejnym istotnym elementem w systemach rozproszonych jest zapewnienie jednolitego czasu dla wszystkich urządzeń. Z tego powodu rejestratory IndigoVision w wersji Linux zostały wyposażone w serwer czasu będący wzorcem dla pozostałych rejestratorów, kamer i stacji podglądu.

System monitoringu miejskiego – praktyczne funkcje

System IndigoVision ma wiele cech funkcjonalnych. W artykule zostaną opisane tylko te, które w systemach monitoringu miast są najczęściej wykorzystywane. Pierwszym elementem wpływającym na skuteczną pracę są przyciski szybkiego przejścia do odtwarzania obrazów ze wszystkich kamer lub z jednej wybranej. Ta prosta funkcja pozwala operatorowi, który zaobserwował dynamiczne zdarzenie, na sprawne odtworzenie obrazu z ostatnich 10, 15 lub 30 sekund bez konieczności wyboru daty, czasu i rejestratora, z którego zapis jest odtwarzany. Tym



Budując system oparty w całości na urządzeniach marki IndigoVision, można w pełni zarządzać wszystkimi elementami, łącznie z ich konfiguracją z poziomu aplikacji do zarządzania Control Center.

samą osobą obsługującą niemal natychmiast uruchamia odtwarzanie obrazu z interesującej ją kamery. Niezwykle przydatna w sprawnym i dynamicznym podążaniu za „intruzem” jest tzw. funkcja kamer otaczających. W rozproszonych systemach wielokamerowych administrator może określić dla każdego punktu obserwacji urządzenie zlokalizowane najbliżej. Funkcja ta polega na logicznym połączeniu sąsiadujących ze sobą kamer. Jeżeli operator uzna, że uwagę skupić należy na przemieszczającym się obiekcie, może sprawnie prowadzić obserwację. Po wyświetleniu np. śledzonego pojazdu w miejscu, które jest przypisane kamerze centralnej, rozpoczyna pracę w trybie kamer otaczających. Gdy obserwowany obiekt zmieni lokalizację, zostanie wyświetlony w jednym z przylegających okien. Wybór tego okna spowoduje, że kamera ta stanie się centralną i wówczas zostaną automatycznie uruchomione zdefiniowane dla niej kamery sąsiadujące. System ma również wiele mechanizmów przydatnych w pracy z zarejestrowanym obrazem. Jest to między innymi system miniatur. Miniatury czasowe dzielą wybrany zakres zapisu na równe odstępy, pozwalając na szybkie wyszukanie zdarzeń w obrazach z kamer stałopozycyjnych. IndigoVision umożliwia też wykonanie wy-

kresu prezentującego natężenie ruchu w obrazie zapisanym. Pomimo zapisu ciągłego operator, wykorzystując miniatury alarmowe, może wyświetlić tylko istotne zmiany w obrazie, a zignorować np. ruch powodowany przez drzewa będące tłem. W podobny sposób można przeszukiwać wybrany fragment obrazu lub uruchomić jeden z trybów wykrywania: kierunkowy, detekcję pozostawienia lub zniknięcia obiektu. Przeglądając zarówno zapisany obraz, jak i obraz „na żywo”, operator może wprowadzić znaczniki z komentarzami. W późniejszym czasie, aktywując miniatury od zakładki, można szybko przejrzeć wszystkie wpisy w całym archiwum. Wybrane fragmenty obrazu mogą zostać zabezpieczone przed nadpisaniem. Omawiając pracę na obrazie zarejestrowanym, należy też wspomnieć o tzw. funkcji *Storyboard*. Mechanizm ten pozwala na wyeksportowanie w postaci filmu nagrań z kilku kamer, na których np. pojawiał się intruz. Wówczas na jednym ekranie kolejno są wyświetlane obrazy z poszczególnych kamer, które rejestrowały zdarzenie. W systemach wielokamerowych stosunkowo często korzysta się z map lokalizacji kamer. W tym zakresie IndigoVision oferuje kolejny praktyczny moduł. Pozwala on

na wprowadzenie wielu map, rozpoczynając od mapy całego miasta, dokładniejszych map osiedli lub map obrazujących rozmieszczenie kamer w budynku. Dzięki interaktywnym ikonom można dokładnie zobrazować miejsce i pole widzenia każdej kamery oraz przełączać się pomiędzy mapami. Aplikacja Control Center pozwala na lokalizowanie kamer, co jest wykorzystywane przez nowych pracowników stacji monitorowania do szybkiego odszukania miejsca montażu interesującej ich kamery.

Jeżeli zachodzi taka potrzeba, system można rozbudować o funkcję analizy wideo. Do wyboru jest wiele modułów. Najistotniejszymi w zakresie omawianego tematu są rozpoznawanie tablic rejestracyjnych aut oraz rozpoznawanie twarzy.

Nowe możliwości: kamery interwencyjne

W ostatnim czasie wzmożonym zainteresowaniem służb mundurowych cieszą się kamery interwencyjne FrontLine 2. Urządzenia te są przeznaczone do pracy mobilnej, służąc jednocześnie jako rejestrator osobisty. Przypięte do munduru, paska czy noszone na specjalnych szelkach zapewniają użytkownikowi swobodę ruchu. Kamery interwencyjne są spójne z całym systemem, a obraz po zgraniu na rejestrator lokalny jest synchronizowany w czasie z obrazami z innych kamer systemu monitoringu miejskiego. Urządzenia FrontLine 2 Plus są przygotowane do pracy ciągłej nawet przez 14 godzin, rejestrując obraz w rozdzielczości HD. Nagrania z kamer są oznaczane dokładnym czasem zapisu oraz identyfikatorem użytkownika, dzięki czemu mogą posłużyć jako dowód w sądzie – system ma zaimplementowaną funkcję znaku wodnego. Rozwiązania firmy IndigoVision stanowią doskonały wybór do wszelkich zastosowań wymagających niezawodności, stabilnej pracy i funkcjonalności. Z tego właśnie powodu system znalazł szerokie zastosowanie do ochrony wielu obiektów o znaczeniu strategicznym. ■



Bezpieczne miasta i obiekty biurowe



Każdy chciałby, żeby służby odpowiedzialne za bezpieczeństwo w jego mieście natychmiast reagowały w sytuacji zagrożenia życia bądź uszkodzenia mienia. **Bezpieczeństwo to nie tylko ochrona mieszkańców czy pracowników, to również ochrona elementów infrastruktury, zapewniających prawidłowe funkcjonowanie miasta lub obiektów biurowych.**

Marcin Ruciński
Hanwha Techwin Europe

Użyteczność informacji uzyskanych z systemu monitoringu wizyjnego w standardowym wydaniu nie zapewni ochrony na wysokim poziomie. Do tego są potrzebne rozwiązania zintegrowane, umożliwiające koordynację działań wielu służb oraz integrację innych systemów zabezpieczeń tworzących kompleksowy system bezpieczeństwa.

Oprogramowanie do centrów nadzoru

Trudno sobie wyobrazić bezpieczne miasta i obiekty biurowe bez profesjonalnego centrum nadzoru. Firma Hanwha Techwin oferuje zaawansowane oprogramowanie Smart Security Manager, które pozwala stworzyć centrum nadzoru bez ograniczeń co do pojemności systemu, z geograficzną lokalizacją elementów infrastruktury. Architektura modułowa

umożliwia delegowanie zadań zarządzania bezpieczeństwem do mniejszych centrów nadzoru lub delegowanie w całości autonomicznej infrastruktury bezpieczeństwa w ramach federacji, a to z kolei pozwala stworzyć centralny system nadzoru dla wielu miast bądź obiektów biurowych, optymalizując koszty nadzoru. System SSM oferuje ogromne możliwości integracji z innymi systemami zabezpieczeń, takimi jak KD, SSWin i SSP nie tylko poprzez wejścia alarmowe, ale również na podstawie kryteriów generowania alarmów w oparciu na danych tekstowych wysyłanych przez sieć Ethernet z innych systemów zabezpieczeń, a także stworzenie dedykowanych sterowników, co tym samym stanowi najbardziej rozbudowany poziom integracji. Dzięki integracji SSM umożliwia opracowanie scenariuszy alarmowych, które automatyzują pracę operatora, wyświetlając podgląd z kamery znajdującej

się najbliższej miejsca zdarzenia, a także automatyczne nadawanie komunikatów głosowych i załączenie wyjść alarmowych z kamer, rejestratorów i innych systemów zabezpieczeń, umożliwiając np. automatyczne uruchomienie funkcji kamery PTZ. SSM pozwala tworzyć różne scenariusze w relacji wiele urządzeń na wejściu i wiele urządzeń na wyjściu. W przypadku, gdy dany scenariusz alarmowy nie był zdefiniowany, a wystąpiło zagrożenie, operator może zweryfikować wszystkie alarmy zarejestrowane w oprogramowaniu SSM bądź skorzystać z funkcji Smart Search zaimplementowanej również w najnowszych rejestratorach serii X i P, co umożliwia analizę obrazu w zapisanym

materiale. Na podstawie parametrów zdefiniowanych przez operatora można wykorzystać takie algorytmy, jak przekroczenie wirtualnej linii, wejście/wyjście z obszaru, detekcję ruchu. Rozwiązanie jest pomocne w identyfikowaniu pojazdów lub osób, które brały udział w incydentach (stłuczki parkingowe, kradzież mienia, poruszenie się w obszarze wyłączonym z ruchu itp.). Oprogramowanie pozwala również umieścić wszystkie kamery na mapie Google, uzyskać błyskawiczny dostęp do informacji o ich lokalizacji i pozwolić na efektywną koordynację działań.

Kamery sieciowe

Bezpieczeństwo miast i obiektów biurowych to również efektywna kontrola ruchu pojazdów.



Hanwha Techwin oferuje kamery w wersji drogowej i parkingowej. Oba rozwiązania można zintegrować z rejestratorami IP umożliwiającymi tekstowe wyszukiwanie tablic rejestracyjnych i przeglądanie zarejestrowanego materiału. Rejestratory pozwalają na zarządzanie (API) danymi tekstowymi, w tym numerami tablic rejestracyjnych jako zdarzeniami, a w powiązaniu ze scenariuszami alarmowymi operator otrzymuje informację, że kamera zidentyfikowała pojazd, który jest na liście alarmowej. Kamera PTZ może dodatkowo wspomagać identyfikację kierowcy. W przyszłości to rozwiązanie będzie pomocne w identyfikacji pojazdów, które poruszają się bez wymaganego ubezpieczenia OC lub łamały przepisy ruchu drogowego.

Istotne dla bezpieczeństwa miast i obiektów biurowych są funkcje analityczne zaimplementowane na kamerze, m.in. wirtualna linia, wejście/wyjście w obszar (np. parkowanie w niedozwolonym miejscu), pojawienie się/zniknięcie obiektu, detekcja dźwięku, wykrywanie kierunku jazdy, utrata ostrości lub detekcja sabotażu (zmiana kadru lub przesłonięcie pola widzenia). W specjalnych wymaganiach dedykowaną aplikację można zainstalować bezpośrednio na kamerze.

Cały system nie byłby skuteczny, gdyby nie wysokiej jakości kamery oferujące doskonały obraz w nocy dzięki zastosowaniu przetworników o dużej czułości, zaawansowanych algorytmów poprawy kontrastu, funkcji HLC z maskowaniem, w dzień natomiast – WDR o dynamice nawet do 150 dB. Dużą bolączką instalacji monitoringu miejskiego jest wrażliwość kamer na wibracje spowodowane np. wiatrem lub przemieszczaniem się pojazdów o wysokim tonażu. Najnowsze kamery serii WiseNet X zostały wyposażone w stabilizator

żyroskopowy, umożliwiający kompensację drgań i wibracji będących poza zasięgiem funkcji cyfrowej stabilizacji. Bardzo użyteczną funkcją wprowadzoną wraz z tą serią jest klasyfikacja dźwięku wg wzorca (np. stłuczenie szkła, krzyk, eksplozja strzały z broni palnej). Całości dopełnia seria kamer WiseNet P o wysokiej rozdzielczości 4K, w tym modele wieloobiektywowe mające zastosowanie w dozorze parkingów, skrzyżowań czy ciągów komunikacyjnych oferujące obraz o wysokim stopniu szczegółowości. W kamerze zaimplementowano funkcję Digital Auto Tracking, która umożliwia wykrycie obiektów ruchomych, w tym ludzi, w miejscach mało uczęszczanych (skwery lub parki).

Rejestratory sieciowe

Rejestratory Hanwha Techwin są odporne na awarie, wspierają takie funkcje, jak ARB (automatyczne odzyskiwanie danych z karty SD w kamerze) oraz Failover (skonfigurowanie jako awaryjnego jednego rejestratora w grupie do 32 – w przypadku awarii rejestratora podstawowego przejmuje jego funkcję). Najbardziej zaawansowane technicznie modele zostały wyposażone w porty SFP, kontroler RAID 5/6 oraz redundantne zasilacze, które podobnie jak dyski pracujące w RAID mogą być wymieniane podczas pracy rejestratora bez konieczności jego ponownego uruchomienia.

Firma Hanwha Techwin, dzięki dużej elastyczności, ogromnym możliwościom konfiguracyjnym, integracyjnym oraz zgodności z obowiązującymi standardami swoich produktów, oferuje rozwiązania zwiększające bezpieczeństwo obiektów biurowych i monitoringu wizyjnego miast. Dzięki nim praca operatora jest nieporównywalnie efektywniejsza niż w przypadku tradycyjnych systemów monitoringu. ■



**EXTRA RABAT
i 5 LAT GWARANCJI**

Kupiłeś kiedyś system CCTV firmy Samsung, a teraz chcesz go zmodyfikować, rozbudować i unowocześnić? A może system innego producenta nie spełnił Twoich oczekiwań? Skontaktuj się z naszymi Partnerami lub bezpośrednio z nami i uzyskaj specjalny rabat na zakup nowego sprzętu oraz 5-letnią gwarancję*!



WISENET X

- eXplozja dynamiki obrazu 150dB w funkcji WDR
- eXkluzywna technologia Wisestream II i kompresja H.265
- eXtremalnie stabilny obraz dzięki stabilizacji żyroskopowej
- 2X szybsze przetwarzanie danych dzięki procesorowi DSP piątej generacji



*Dotyczy wyłącznie nowo zakupionego sprzętu, zainstalowanego przez autoryzowanych Partnerów Hanwha Techwin w Polsce. Szczegółowe informacje pod adresem hte.poland@hanwha.com



AxxonSoft VMS dla smart cities

Michał Przybylski
AxxonSoft Polska

Miasto inteligentne można zdefiniować jako wykorzystujące technologie informacyjno-komunikacyjne w celu zwiększenia interaktywności i wydajności infrastruktury miejskiej oraz jej komponentów składowych, a także w celu podniesienia świadomości mieszkańców. Ważnym elementem jest dozór wizyjny wykorzystywany najczęściej do archiwizowania zdarzeń oraz dynamicznego dozoru za pomocą kamer stało- i zmiennopozycyjnych. Zdarzenia są analizowane przez operatorów. Niestety, zarówno liczba operatorów, jak i ich zdolności przetwarzania dużej ilości informacji są ograniczone, dlatego od automatyzacji i wsparcia pracy operatorów rozpoczynają się zadania dla systemów zarządzania wideo (VMS).

Video Management System

VMS to system obejmujący działania oparte na zarządzaniu kamerami, ich konfigurację, rejestrację materiału, zarządzaniu nim oraz analizę wraz z raportowaniem. Najnowsza wersja systemu AxxonSoft nie tylko spełnia wszystkie te funkcje, ale też dostarcza dodatkowych funkcjonalności, takich jak współpraca z innymi systemami czy możliwość zaimplementowania zaawansowanej analizy obrazu.

System Axxon

System VMS AxxonSoft powstał z myślą o środowiskach rozproszonych, takich jak infrastruktura miejska. Zapewnia pełną skalowalność zaprojektowanego rozwiązania nie tylko w wymiarze jego powiększenia (obszaru lub ilości), ale także umożliwia integrację urządzeń końcowych różnych producentów, różnych funkcjonalności, a nawet urządzeń różnych

generacji. Pozwala to uniknąć ryzyka zbudowania systemu zamkniętego, odpornego na postęp technologiczny i ograniczającego inwestora. System Axxon został zoptymalizowany do pracy w środowisku wielkomiejskim zarówno w warstwie technologii pracy z tysiącami kamer, bezpieczeństwa rejestrowanych i przetwarzanych danych, jak i poprzez natywną zaawansowaną analitykę wspomagającą pracę operatorów systemu.

Technologie

Przykładem technologii służących do zwiększenia użyteczności i stabilności systemu jest mikromodułowość (zapewniająca działanie systemu jako całości nawet w przypadku awarii jednego z elementów oprogramowania), Green Stream (umożliwiająca dynamiczne dzielenie i optymalizowanie strumienia wyświetlanego obrazu) czy obsługa Intel Quick Sync (pozwalająca

Dynamiczny rozwój miast wykreował potrzebę wykorzystania nowoczesnych technologii wspierających zarządzanie infrastrukturą miejską. Tak powstała idea inteligentnych miast.

na obsługę setek kamer jednocześnie z poziomu jednego komputera). System, dzięki nowoczesnemu interfejsowi, może też obsługiwać ściany wideo, a wielodomenowy monitoring, umożliwiający pracę z wieloma rozproszonymi serwerami jednocześnie, zapewnia elastyczną pracę w środowiskach obejmujących tysiące kamer. Wszystkie urządzenia końcowe systemu mogą być konfigurowane grupowo.

Bezpieczeństwo

Bezpieczeństwo – zarówno danych, jak i działania systemu – jest zapewniane poprzez redundancję serwerów, zaawansowane zarządzanie prawami użytkowników (np. obsługa LDAP), a także harmonogramy tworzenia kopii zapasowych danych oraz całego systemu i automatyczne przywracanie konfiguracji. AxxonSoft umożliwia też gromadzenie danych wideo w archiwach sieciowych i zapasowych poprzez replikację danych.

Analiza wideo

System Axxon wykazuje największą przewagę w mnogości narzędzi do analizy i interpretacji danych. Nie tylko ułatwia pracę w systemie miejskim dzięki interaktywnym mapom 3D (pozwalającym operatorowi błyskawicznie orientować się w rejonie zdarzenia,



Tag & Track Pro: bezpieczne miasto – Lima w Peru



Inteligentny system zarządzania ruchem w Lublinie

a także odtwarzać widoki z kamer „zanurzonych” wirtualnie w mapach), ale też realizuje wielowarstwowe przetwarzanie danych w czasie rzeczywistym i analizuje dane archiwalne. System, rejestrując obrazy z kamer, oznacza materiał za pomocą metadanych i tworzy w ten sposób rozbudowaną bazę informacji powiązanych z obrazem wideo, które można będzie rozpoznać i przeanalizować.

Analiza real time

Bezpieczeństwo można zwiększyć, wspierając operatorów w automatycznym rozpoznaniu zdefiniowanych zdarzeń w czasie rzeczywistym. Przykładem takiego narzędzia jest detekcja tłumu i zgrupowań, detekcja zachowań niebezpiecznych i potencjalnie niebezpiecznych, wtargnięcia na torowiska, wałęsanie się, ale również nagłych zmian kierunku, detekcja osób biegnących, a także – dzięki obsłudze dwukierunkowej – audiodetekcja krzyku czy tłuczonego szkła oraz możliwość wysłania komunikatów głosowych, np. ostrzeżeń. Chcąc wspomóc operatorów, kamery można ustawić w trybie automatycznej powiększania pojazdów i osób poruszających się w polu widzenia kamery. Dla ułatwienia pracy z kamerami PTZ stworzono dodatkowe funkcje,

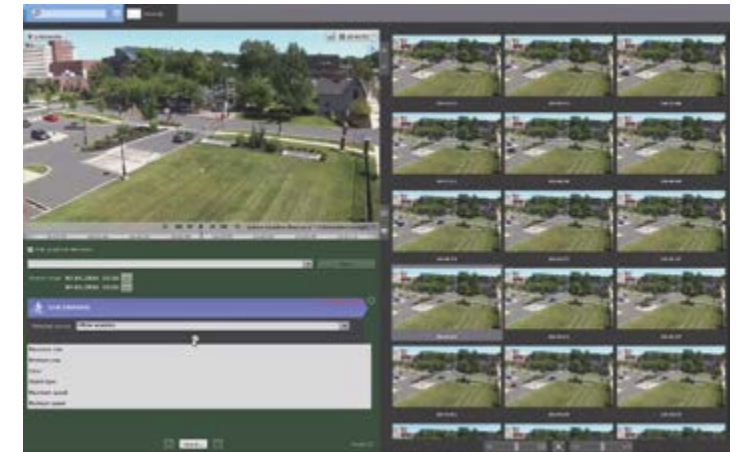
np. *Tag & Track Pro* (pozwala automatycznie śledzić za pomocą kamery obrotowej pojazd lub osobę wskazane na obrazie z kamery stałopozycyjnej).

Analityka auto

Axxon wspiera również analizę ruchu i zachowań pojazdów. Dzięki wbudowanym narzędziom wykrywającym prędkość, kierunek poruszania się, wielkość i kolor obiektu można opracować scenariusze powiadomienia o sytuacjach zagrożenia, takich jak obecność dużych pojazdów w centrum, jazda pod prąd itp. Algorytmy wspierające kontrolę ruchu, takie jak detekcja ruchu na czerwonym świetle czy korków, stają się naturalnym wsparciem dla systemów inteligentnego sterowania ruchem ITS, które niejako definiują smart cities.

Analityka archiwum

Narzędzia wyszukiwania pozwalają na szybkie odszukanie dowolnych zdarzeń dotyczących wskazanego fragmentu obszaru, kadru lub obiektu. Uniwersalność zastosowań przeszukiwania, opartych na metadanych zgromadzonych informacji, pozwala stosować np. detekcję pozostawionych przedmiotów w identyfikacji działań antyterrorystycznych, ale także do wskazywania osób nielegalnie wysypujących



Moment Quest umożliwia wielowarstwowe przeszukiwanie archiwum

śmieci. Każda kamera podłączona do systemu spełnia kilka funkcji – jedna kamera może zarówno śledzić ruch na ulicy w celach statystycznych, jak i chronić elementy małej architektury przed aktami wandalizmu, wykrywać obecność pojazdów komunikacji miejskiej czy zatory drogowe. Wszystkie te zarejestrowane zdarzenia można później błyskawicznie odnaleźć i zinterpretować dzięki takim narzędziom, jak *Moment Quest* (wielowarstwowe przeszukiwanie archiwum), *Time Compressor* (wizualizacja wszystkich zdarzeń w jednym klipie wideo), przeszukiwanie zdarzeń w trybie podglądu miniatur.

Scenariusze zadziałania systemu

W ramach wdrożenia systemu oraz w trakcie obsługi można przygotować łańcuchy wzajemnie wspierających się zadań i funkcji analityk oraz zgrupować je w makra przypisane konkretnym funkcjom.

Raportowanie

Działy promocji miast docenią możliwości generowania zintegrowanych raportów zliczania osób na ulicach w dzień powszedni oraz podczas imprez masowych, które pozwolą ocenić ich powodzenie i popularność. System Axxon może więc stać się narzędziem pomiaru

skuteczności władzy miasta, a także zastąpić bardzo drogie pomiary ruchu, dostarczając raporty codziennie lub na żądanie. Wyniki pomiarów oraz aktywności można nanosić na plany w formie tzw. map ciepła, które zależnie od funkcji wskazują strefy popularności lub występowanie poszukiwanego zjawiska.

Podsumowanie

Zaawansowana analityka zaimplementowana w systemach VMS Axxon znajduje zastosowanie w wielu dziedzinach działania *smart cities*. Liczba tych zastosowań rośnie wraz z możliwościami kamer, serwerów analitycznych i algorytmów. Dzięki implementacjom w miastach pojawiają się obszary, w których dotychczas nie stosowano tego typu narzędzi. Często dzięki szybkości i precyzji działania zaawansowana analiza staje się istotą inteligencji miasta. Stanowi wsparcie dla wielu służb, zwiększając ich sprawność i bezpieczeństwo. Miasta dzięki temu stają się czystsze, mniej zakorkowane, lepiej zarządzane i bezpieczniejsze. Takie parametry cechują ośrodki szybko się rozwijające, w których ludzie chcą się osiedlać i pracować – stają się miejscami dynamicznego rozwoju społeczeństwa, zasługując na miano *smart city*. ■



Miasto w panoramie



Władze zarówno małych miejscowości, jak i dużych aglomeracji miejskich stoją przed wyzwaniem związanym z zapewnieniem bezpieczeństwa mieszkańcom. Podstawowym elementem mającym wpływ na budowanie bezpieczeństwa w przestrzeni publicznej jest miejski system monitoringu wizyjnego, a współpraca samorządów z policją i strażą miejską powinna prowadzić do spadku przestępczości oraz wzrostu wykrywalności niebezpiecznych zachowań.

Dominika Majsterek
Technical Support Engineer,
Hikvision Poland

Działania na rzecz rozbudowy systemów powinny przebiegać dwuetapowo. Po pierwsze – w miastach należy rozwijać infrastrukturę umożliwiającą powstawanie systemów dozorujących przestrzeń miejską, a także ułatwiającą przyłączanie kolejnych kamer do istniejących systemów. Po drugie – rozbudowie powinien podlegać monitoring w środowiskach komunikacji miejskiej. Przestrzeń miejska, ze względu na dynamiczne zmiany oświetlenia, wpływ warunków atmosferycznych (np. wiatr, deszcz), a także konieczność obserwowania rozległych obszarów, stanowi dla kamer trudne środowisko pracy. Muszą one spełniać najwyższe wymagania. Przykładem może być ruchliwe skrzyżowanie. W ciągu dnia panuje tu duży ruch uliczny – pojazdów i pieszych. W nocy problem stanowią intensywne światła reflektorów samochodowych,

oświetlenie uliczne lub jego brak. W przeciwieństwie do obiektów zamkniętych dozór wizyjny otwartych przestrzeni miasta wiąże się z koniecznością objęcia zasięgiem widzenia dużego obszaru. Klasycznym rozwiązaniem tego problemu jest stosowanie większej liczby kamer. To jednak podnosi koszty nie tylko urządzeń, ale także konserwacji i eksploatacji. Dlatego coraz częściej producenci oferują urządzenia, które łączą w jednej obudowie kilka kamer. Proponowana przez Hikvision seria PanoVu obejmuje kilka modeli kamer zoptymalizowanych pod kątem różnych wyzwań związanych z monitoringiem miejskim. Wszystkie modele tej linii, z zapewnianą wysoką czułością technologią Darkfighter, generują obraz o optymalnej jakości nawet w trudnych warunkach oświetleniowych. Kamera PanoVu może się składać nawet z ośmiu modułów stałopozycyjnych, które tworzą jednolity obraz panoramiczny 2 x 180°. Flagowe modele tej serii mają dodatkowo zintegrowany moduł kamery PTZ, łącząc w ten

sposób zalety wynikające z zastosowania kamer panoramicznych i szybkoobrotowych PTZ. Dzięki uzupełnieniu obrazu panoramicznego ujęciami z kamery zmiennoogniskowej operator widzi na obrazie więcej szczegółów z odległych miejsc. Obserwację dalekich scen umożliwiają 36-krotny zoom optyczny oraz zastosowany promiennik podczerwieni o zasięgu 200 m. Całkowita rozdzielczość kamery w przypadku modelu wyposażonego w 8 przetworników obrazu wynosi aż 16 Mpix, co zapewnia doskonałą jakość nagrań. Na poprawę jakości obrazu wpływają także funkcje WDR, HLC czy 3D DNR. Ponadto w kamerach zaimplementowano niemal wszystkie funkcje inteligentnej analizy obrazu, takie jak detekcja przekroczenia linii, naruszenie strefy oraz śledzenie obiektów (ludzi lub pojazdów). Modele PanoVu wyposażone w moduł PTZ wprowadzają również innowacyjny sposób sterowania. W celu ustawienia pozycji kamery obrotowej wystarczy kliknięciem myszki na obrazie dookólnym z kamer stałopo-

zycyjnych zaznaczyć obszar, który ma zostać objęty obserwacją. Usprawnia to kontrolę nad dozorowanym obszarem i minimalizuje czas, jaki upływa od zaobserwowania zdarzenia na podglądzie 360° do uzyskania obrazu z kamery PTZ. Rosną więc szanse na skuteczne zidentyfikowanie obiektu, np. ewentualnego sprawcy czynu zabronionego lub pojazdu naruszającego przepisy drogowe. W przypadku monitoringu miejskiego ma to kluczowe znaczenie dla zmniejszenia wskaźnika przestępczości. Nowością w serii PanoVu jest model DS-2DP1636-D. Dzięki 8 przetwornikom obrazu Darkfighter umieszczonych dookoła i od spodu użytkownik ma możliwość poglądu obrazu w kształcie zbliżonym do sfery (360°), bez martwych stref. Kamera ta idealnie sprawdzi się w dozorcze skrzyżowań. W ofercie Hikvision pojawiła się też kamera panoramiczna 180°, 24 Mpix zbudowana z 4 przetworników 6 Mpix, a także kamera iDS wyposażona w algorytmy *Deep Learning*, umożliwiające nagrywanie metadanych o osobach (budowa ciała czy kolor ubrania), co znacznie przyspiesza przeglądanie zarejestrowanego materiału wideo. Wandaloodporna obudowa zewnętrzna o klasie wytrzymałości mechanicznej IK10 poszerza zakres możliwych zastosowań, począwszy od parkingów, przez stadiony i parki, kończąc na terminalach lotniczych. ■



Nie tylko bezpieczeństwo

Monitoring miasta Karpacz

Poprawa bezpieczeństwa i porządku publicznego to główne, ale nie jedyne cele władz kurortu leżącego u stóp Śnieżki. Korzystając z pozytywnych doświadczeń innych polskich miast, zdecydowały o uruchomieniu monitoringu miejskiego.

Dagmara Dąbrowska
Senior Sales & Marketing Specialist,
CBC Poland

Obok prewencji i zwiększenia wykrywalności sprawców niepożądanych zdarzeń równie istotnym wymogiem zdefiniowanym w założeniach projektowych była możliwość analizy strumienia turystów odwiedzających Karpacz, mająca pomóc w opracowaniu strategii promocyjnej miasta. Wdrożony w dwóch etapach system monitoringu miejskiego został oparty na kamerach GANZ IP oraz systemie rejestrującym firmy ALNET. W dwóch etapach inwestycji zainstalowano łącznie kilkanaście kamer mini-PTZ serii GenSTAR o symbolu ZN8-P5NTAF62L. W pierwszym etapie zamontowano cztery punkty kamerowe na drogach wjazdowo-wyjazdowych (łącznie 7 kamer), mające za zadanie rozpoznawanie numerów tablic rejestracyjnych przy wykorzystaniu funkcjonalności ANPR (*Automatic Number Plate Recognition*). System rozpoznawania numerów tablic złożony z dwóch kluczowych elementów: kamery wyposażonej w liczne funkcje gwarantujące czytelność obrazu w skrajnie trudnych warunkach oświetleniowych występujących m.in. nocą podczas nadjeżd-



Czytelność tablicy rejestracyjnej samochodu jadącego 100 km/h

żającego w kierunku kamery samochodu z włączonymi reflektorami czy też silnego nasłonecznienia w ciągu dnia, oraz oprogramowania Net Station wyposażonego w rozbudowaną funkcjonalność ANPR. Kompaktowa, specjalnie zaprojektowana 3-komorowa obudowa ZN8-P5NTAF62L mieści moduł kamery 3 Mpix z 12-krotnym zoomem optycznym oraz promiennik IR, zamontowane w oddzielnych komorach w celu zredukowania temperatury wewnątrz obudowy, co wpływa na żywotność kamery. Jak poka-



Kamera GANZ IP w Karpaczu

zuje niniejszy przykład, kamera wyposażona w szereg zaawansowanych technologii wspierających jakość obrazu doskonale sobie radzi z odczytem tablic rejestracyjnych aut nawet przy prędkości 100 km/godz. Funkcjonalność modułu ANPR, stanowiąca dodatek do oprogramowania NetStation, pozwala m.in. na: szybkie wyszukiwanie nagrań na podstawie numeru rejestracyjnego • tworzenie tzw. białej i czarnej listy numerów • sterowanie szlabanem czy też bramą otwieraną tylko dla pojazdów uprzywilejowanych • monitorowanie czasu pobytu w strefie • generowanie raportów • tworzenie bazy danych pojazdów oraz identyfikację kilkudziesięciu krajów pochodzenia numeru rejestracyjnego. Warto zaznaczyć, że w przypadku systemu zaimplementowanego w Karpaczu rozbudowana funkcjonalność ANPR

stanowi również potężne narzędzie marketingowe, z powodzeniem wykorzystywane przez urzędników miejskich do analizowania pochodzenia turystów, co jest niezwykle pomocne w opracowywaniu kampanii promocyjnej dla kurortu. Kolejne kamery dodano w drugim etapie inwestycji, montując je w innych newralgicznych miejscach miasta, takich jak centrum, deptak, najbardziej ruchliwe skrzyżowania. System nadzorują strażnicy miejscy w Centrum Zarządzania Kryzysowego, a środki na realizację inwestycji pozyskano m.in. z budżetu partycypacyjnego. Funkcjonalność systemu spełniła wymagania zdefiniowane w założeniach projektowych, czego efektem jest rozpoczęcie kolejnego etapu inwestycji – rozbudowę systemu i montaż dodatkowych kilkudziesięciu kamer GANZ IP w innych newralgicznych miejscach Karpacza. ■



Duża dynamika rozwoju systemów monitoringu wizyjnego w ostatnich latach sprawiła, że czas dostępności urządzeń oferowanych przez producentów się skrócił.



BCS Manager

- wszystko w jednym

Na początku roku pojawiła się nowa linia produktów BCS Point. Nowością jest również oprogramowanie BCS Manager integrujące wszystkie urządzenia BCS, od najstarszych po najnowsze. Oprogramowanie ma wiele udogodnień dla użytkownika, np. podgląd, odtwarzanie materiału oraz automatyczną reakcję na alarmy z urządzeń. Jest również użytecznym narzędziem przy integracji i rozbudowie systemu dozoru wizyjnego.

Podgląd

Bogata gama urządzeń w ofercie BCS udostępnia instalatorowi najnowsze techniki przesyłania sygnału wizyjnego w najwyższych rozdzielczościach. Instalacje systemów, ich topologia, liczba i typ urządzeń w systemie dla każdego obiektu mogą być różne. BCS Manager jest dedykowanym oprogramowaniem do obsługi wszystkich urządzeń BCS w systemach Windows i Mac OS X. Oprogramowanie umożliwia dodanie do listy urządzeń i obsługę nawet 1000 rejestratorów lub kamer, a także wyświetlanie 8 kart (obsługa 8 monitorów). Każda z kart/zakładek obsługuje maksymalnie 64 obrazy z kamer. Pozwala to na tworzenie za pomocą oprogramowania BCS Manager stanowisk wielomonitorowych. Możliwości wyświet-

lania obrazów z kamer w oprogramowaniu są ograniczone głównie wydajnością jednostki, na której został zainstalowany BCS Manager. Do podglądu w podziale przy wyświetlaniu obrazów z wielu kamer wykorzystuje się dodatkowy strumień, który w kamerach i rejestratorach BCS jest domyślnie ustawiony w rozdzielczości D1. Pełna rozdzielczość kamery jest pokazywana po wywołaniu pojedynczego kanału lub uruchomieniu zoomu cyfrowego. Dzięki temu oszczędza się pasmo wykorzystywane przez program w sieci. Użytkownik może skonfigurować i zapisać spersonalizowane okno podglądu, które na jego życzenie zostanie wywołane automatycznie lub ręcznie. Częstym wymogiem jest działanie bezobsługowe. BCS Manager po odpowiednim skonfigurowaniu sekwencji i zadań potrafi po otwarciu programu automatycznie pokazać widok z kamer nawet na wielu monitorach, przypisując konkretne karty podglądu do poszczególnych monitorów.

Alarmy z urządzeń

Ważnym udogodnieniem dla użytkowników jest możliwość

automatycznej reakcji na występujące alarmy. Po odpowiednim skonfigurowaniu reguł oprogramowania powiadomienia o detekcji ruchu z dowolnego kanału, zasłonięciu kamery lub błędzie dysku w rejestratorze. Wystąpienie takiego alarmu wywołuje dowolną kamerę systemu lub zapisany wcześniej widok. Reguły alarmów są konfigurowane dowolnie wg terminarza tygodniowego. W oknie podglądu na liście urządzeń użytkownik widzi również stan wejść i wyjść alarmowych zarówno z kamer, jak i z rejestratorów oraz kamer podłączonych do rejestratora, jeżeli posiadają wejścia lub wyjścia. Oprogramowanie umożliwia aktywację wyjścia alarmowego, co pozwala na integrację z innymi systemami.

Odtwarzanie

Jedną z podstawowych funkcji oprogramowania BCS Manager jest szybki dostęp do nagrań w rejestratorach. Można wybrać dowolny kanał lub kilka kanałów z rejestratorów znajdujących się na liście urządzeń, odtworzyć nagranie i zapisać je na dysku komputera. Odtwarzanie z urządzeń jest możliwe z różnymi

prędkościami, z możliwością dowolnej zmiany czasu odtwarzania dla każdego z kanałów. Podział okien odtwarzania jest dowolny, na karcie odtwarzania można maksymalnie wyświetlić 64 okna. Udogodnieniem jest możliwość włączenia synchronizacji odtwarzania, co pozwala na uporządkowanie czasów odtwarzanych kanałów. Intuicyjna funkcja wycinania nagrań, kryjąca się pod ikoną nożyczek, pozwoli sprawnie zgrać na dysk komputera wyszukany materiał. Użytkownik może dopasować zakres zrywanego materiału co do sekundy, zrezygnować z nagrywania dowolnego kanału oraz wybrać miejsce zapisu na dysku. Po zapisaniu materiału może przejść do folderu zapisu lub zapisany materiał odtworzyć.

Systemy monitoringu wizyjnego podlegają ciągłym przemianom i rozwojowi, dlatego wybrane urządzenia powinny mieć możliwości adaptacji nowych technologii i dołączania pojawiających się coraz nowszych rozwiązań. BCS Manager umożliwia integrację wszystkich produktów z oferty BCS, gwarantując użytkownikowi możliwość rozbudowy lub zmiany technologii bez konieczności wymiany już zainstalowanych urządzeń. ■

BCS MANAGER

1.3

APLIKACJA WIELOMONITOROWA
WSPÓŁPRACUJĄCA
Z WSZYSTKIMI PRODUKTAMI

BCS®



QVR Pro

profesjonalny system dozoru wizyjnego na serwerze NAS

Nowe oprogramowanie do dozoru wizyjnego QVR Pro umożliwia wykorzystanie urządzeń NAS marki QNAP jako profesjonalnego centrum systemu monitoringu wizyjnego, bez potrzeby inwestowania w specjalistyczny wideorejestrator.

Innowacja wpływa na zwiększenie wydajności podczas odtwarzania i eksportowania materiałów wideo, zapewnia spójny interfejs aplikacji do monitoringu z różnych platform i urządzeń, pozwala na automatyzowanie dodawania kamer i zarządzania nimi oraz ułatwia zarządzanie zdarzeniami. QVR Pro integruje wszechstronne funkcje monitoringu wizyjnego IP z oprogramowaniem operacyjnym serwerów QNAP NAS. Do kluczowych możliwości rozwiązania należą:

- wydzielenie dedykowanej przestrzeni dyskowej na dane z systemu monitoringu wizyjnego,
- możliwość rozbudowy pamięci,
- elastyczne funkcje zarządzania pamięcią masową i nagraniami z poziomu systemu operacyjnego NAS,
- konsolidacja monitorowania na żywo z dostępną natychmiast funkcją odtwarzania w jednym widoku upraszcza tryb monitorowania i zapewnia wygodną obsługę.

Zoptymalizowany i zunifikowany interfejs

QVR Pro obsługuje systemy Windows® i Mac®, a także QNAP HD Station, natomiast klient QVR Pro zapewnia jednolity widok monitorowania dla użytkowników wieloplatformowych (nagrania można śledzić na żywo i odtwarzać z poziomu wielu różnych urządzeń). Nowa funkcja QVR Pro Client upraszcza pracę w zakresie dozoru i umożliwia sprawne zarządzanie regułami przez użytkownika. Tworząc QVR Pro, specjaliści z QNAP zdecydowali się na radykalne odświeżenie koncepcji tradycyjnego systemu dozoru. QVR Pro Beta udostępnia zintegrowany tryb monitorowania, uwzględniający zarówno widok na żywo z kamer, jak i odtwarzanie zarejestrowanego wcześniej materiału. QVR Pro Client obsługuje wielokanałowe monitorowanie w jednym widoku i pozwala szybko odtworzyć materiały z minimalnym czasem buforowania.

Dzięki ujednoliconemu interfejsowi użytkownika QVR Pro umożliwia szybsze i wygodniejsze przełączanie się między różnymi trybami monitorowania, co sprawia, że dozór wizyjny jest wydajny i łatwy.

Natychmiastowy dostęp do dowolnego momentu nagrania

QVR Pro umożliwia zsynchronizowanie wszystkich kanałów monitorujących w tym samym widoku tak, by prezentowały nagrania z tego samego momentu. Wystarczy wskazać go na osi czasu, a QVR Pro przewinie nagranie do danego miejsca z minimalnym czasem buforowania.

Układ dynamiczny

QVR Pro obsługuje niestandardowe układy, dzięki czemu można zmieniać proporcje wyświetlania kanałów i swobodnie dopasować wygląd interfejsu do wymagań konkretnego użytkownika, potrzeb danej firmy itp. Oczywiście można również korzystać z domyślnych układów interfejsu.

Funkcja Rejonu Zainteresowań

Pozwala na precyzyjne monitorowanie wskazanego obszaru pozostającego w zasięgu konkretnej kamery (w trybie zarówno podglądu na żywo, jak i odtwarzania). Można zde-

finiować i powiększyć wiele obszarów na obrazie ogólnym bez ograniczeń wyboru lub wymaganych dodatkowych licencji.

Technologia Qdewarp

Qdewarp umożliwia przeglądanie nagrań uzyskanych z kamery „rybie oko” w standardowych proporcjach i parametrach (bez modyfikowania oryginalnego nagrania).

Niezależne środowisko

Wszystkie funkcje dozoru QVR Pro wykonuje niezależnie od systemu operacyjnego QTS. Można np. zapisać nagranie z określonych kamer lub rejonów zainteresowania do wyznaczonej lokalizacji (z uwzględnieniem wskazanych typów dysków twardych lub innych wymagań dotyczących tworzenia kopii zapasowych). Dzięki temu, przy działających jednocześnie QTS oraz QVR Pro serwer QNAP NAS zapewnia bezpieczeństwo danych bez jakichkolwiek zakłóceń wydajności.

Elastyczna rozbudowa pamięci masowej

QVR Pro obsługuje wiele woluminów i typów kopii zapasowych, dzięki czemu rejestrowane za jego pomocą dane pozostają bezpieczne. Użytkownik ma pełną kontrolę nad tym, co, gdzie i jak jest zapisywane. Może np. przypisać miejsce przechowywania nagrań z każdej kamery lub przydzielić nagrywanie zdarzeń do dysków SSD/SAS w celu zwiększenia efektywności składowania. Jeśli cała przestrzeń dyskowa NAS-a zostanie wykorzystana, użytkownik może ją łatwo rozbudować, np. korzystając z obudów rozszerzających.

Najwyższa wydajność

QVR Pro obsługuje technologię autotieringu, co pozwala użytkownikom idealnie dopasować miejsce zapisu danych do ich

charakteru czy specyfiki. Możliwe jest np. zapisywanie materiału wideo 4K o najwyższej przepływności na szybkich nośnikach SSD (w celu uzyskania optymalnej jakości obrazu, bez ryzyka spadków wydajności i płynności odtwarzania). Co więcej, funkcje inteligentnej dystrybucji ruchu sieciowego w serwerze QNAP NAS zapewniają optymalną przepustowość sieci dla przepływów QVR Pro i QTS w celu zapewnienia optymalnej wydajności sprzętu.

Samoczynne reguły

QVR Pro oferuje rozbudowane funkcje zarządzania zdarzeniami i udostępnia powiadomienia ze screenshotami nagrania, a także klasyczne alerty SMS czy e-mail. Dzięki temu użytkownik (np. administrator systemu monitoringu wizyjnego) może szybko podejmować decyzje i reagować na ewentualne incydenty. Oczywiście może również skonfigurować własne reguły powiadomień o zdarzeniach oraz powiązanych z nimi samoczynnych zdarzeniach. Pozwala to w pełni dostosować reguły monitorowania, zdarzenia i działania, co sprawia, że QVR Pro pracuje jako w pełni automatyczne rozwiązanie dozoru wizyjnego.

Zdarzenie

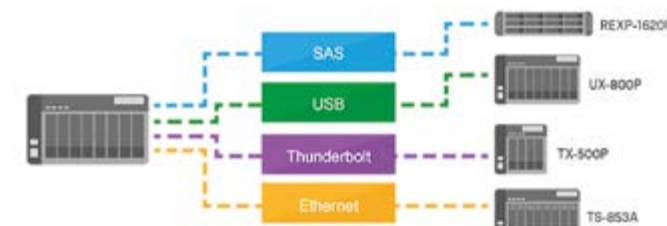
QVR Pro szczegółowo kategoryzuje wszystkie zdarzenia, uwzględniając m.in. to, gdzie zostały zauważone, która kamera je nagrała oraz kryteria zdefiniowane przez użytkownika. Użytkownik może sam definiować listy wydarzeń i same wydarzenia. Co ważne, reguła może obejmować wiele zdarzeń i akcji jednocześnie.

Akcja

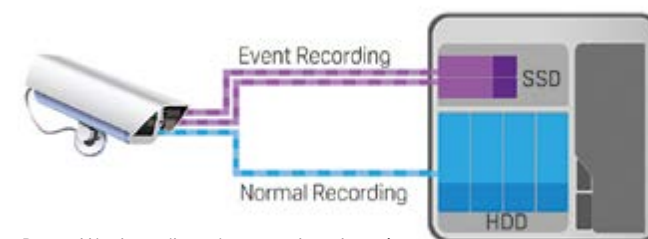
Działania QVR Pro obejmują akcje wykorzystujące kamery – po wykryciu jednego zdarzenia odpowiednio zdefiniowana reguła QVR Pro może spowodować np. uruchomienie określonych kamer w celu rozpoczęcia nagrywania zdarzeń, aktywowanie urządzeń alarmowych lub wysyłanie powiadomień do użytkowników. Co istotne, jedno zdarzenie może powodować kilka niezależnych działań w celu szybkiego reagowania.



Rys. 1. QVR Pro pozwala na odseparowanie wszelkich funkcji i danych związanych z monitoringiem wizyjnym od innych aplikacji i plików w urządzeniu QNAP NAS



Rys. 2. Rozwiązanie do monitoringu wizyjnego QNAP oferuje wiele możliwości rozszerzenia dostępnej przestrzeni dyskowej



Rys. 3. Użytkownik może sam zdecydować, gdzie mają być zapisywane i przechowywane nagrania spełniające różne kryteria. Może np. określić, by wszelkie incydenty były zapisywane na dyskach SSD (co skraca czas dostępu do nagrania i pozwala na szybką reakcję)

wać np. uruchomienie określonych kamer w celu rozpoczęcia nagrywania zdarzeń, aktywowanie urządzeń alarmowych lub wysyłanie powiadomień do użytkowników. Co istotne, jedno zdarzenie może powodować kilka niezależnych działań w celu szybkiego reagowania.

Elastyczne sterowanie kamerami

QVR Pro oferuje automatyczne przeszukiwanie w sekcjach w sieciach lokalnych (LAN). Wystarczy, że użytkownik wskaże odpowiednie segmenty sieci, a QVR Pro znajdzie i wyświetli obrazy ze wszystkich kamer IP wraz z dokładnymi informacjami w tej samej sieci LAN. QVR Pro umożliwia też partycjonowanie i konfigurowanie kamer w celu zwiększenia wydajności oraz optymalne wykorzystanie przepustowości sieci.

Obecnie oprogramowanie QVR Pro jest dostępne w wersji Beta i obsługuje interfejs użytkownika w języku angielskim. QVR Pro Beta obsługuje do 124 kanałów monitorowania w trakcie testu. Użytkownicy mogą korzystać ze wszystkich kanałów bez konieczności posiadania licencji. Oficjalne wydanie QVR Pro będzie oferowało bezpłatne licencje na kanały i modemy QNAP NAS.

Dostępność: oprogramowanie QVR Pro Beta jest dostępne w Centrum aplikacji QTS.

Wymagania systemowe NAS: zalecane 64-bitowe modele NAS z min. 4 GB pamięci RAM. *Do korzystania z QVR Pro wymagane jest QTS 4.3.0 (lub wersje późniejsze). Przed użyciem QVR Pro należy zainstalować aplikację Container Station.* ■

DOZÓR WIZYJNY NAJWYŻSZEJ JAKOŚCI

QVR Pro zapewnia użytkownikom urządzeń QNAP NAS niezależne środowisko pracy do nagrywania materiału wideo z kamer monitoringu, oddzielne miejsca w przestrzeni dyskowej QNAP NAS do przechowywania nagrań, a także wszechstronne funkcje zarządzania pamięcią masową. QVR Pro obsługuje niestandardowe metody rozbudowy pamięci masowej i zarządzanie woluminami, zwiększając bezpieczeństwo danych w zakresie dozoru i przechowywania danych z monitoringu.

Sztuczna inteligencja na usługach systemów zabezpieczeń

Mateusz Zapotoczny
Dahua Technology Poland

Deep Blue

W 1997 r. Garri Kasparow, mistrz świata w szachach, został pokonany przez komputer Deep Blue. Wprawdzie komputer wygrał walkowerem po sześciu rozgrywkach, a IBM nie pozwolił mistrzowi szachowemu na analizę rozgrywek komputera czy rewanż, ale mimo wszystko był to kamień milowy w wyścigu do stworzenia sztucznej inteligencji. Sensacja odbiła się głośnym echem we wszystkich mediach. Przez 20 lat technologia *Deep Learning* i algorytmy sztucznej inteligencji rozwijały się intensywnie, ich skuteczność wzrastała, a rozwój elektroniki pozwolił na imponującą miniaturyzację. Komputer Deep Blue 20 lat temu ważył kilkaset kilogramów i zajmował powierzchnię małego pomieszczenia, obecnie tę samą moc

i możliwości mają układy, które można zmieścić w kieszeni... lub kamerze.

Deep Learning

W kwietniu 2017 r. Dahua Technology nawiązała ścisłą współpracę z firmą Intel Movidius, jednym z liderów w dziedzinie *Deep Learning*, uczenia maszynowego i sztucznej inteligencji. Dzięki tej współpracy wybrane modele kamer Dahua STAR-LIGHT zostaną wyposażone w silne procesory obróbki obrazu Myriad 2 (VPU). Dzięki temu, oprócz szczegółowości i niebywałej światłoczułości, będą mogły oferować zaawansowaną analizę zawartości obrazu. Moduł sztucznej inteligencji (AI) wbudowany w kamerę pozwoli na rozpoznawanie twarzy, monitorowanie zachowań, kontrolę tłumu czy stereoskopowe widzenie i rozpoznawa-

nie obiektów na wzór ludzkich oczu i mózgu. Moduł AI, w przeciwieństwie do zwykłej analizy obrazu, nie analizuje samych pikseli na obrazie z kamery. Uczy się, „jak wygląda świat”, po pewnym czasie jest w stanie odróżnić np. drzewo od samochodu czy człowieka od zwierzęcia. Ponadto analizuje rozpoznane elementy i je klasyfikuje, np. po kolorze, kształcie, typie ubioru (czerwona bluza z kapturem, okulary, plecak, długość włosów). Analiza odbywa się w kamerze, a system prezentuje jedynie jej wyniki, dzięki czemu nie jest wymagane stosowanie drogich i dużych serwerów pochłaniających znaczne ilości energii. Rozwiązanie to pozwala zwiększyć skuteczność rozległych, rozbudowanych systemów monitoringu wizyjnego, w których

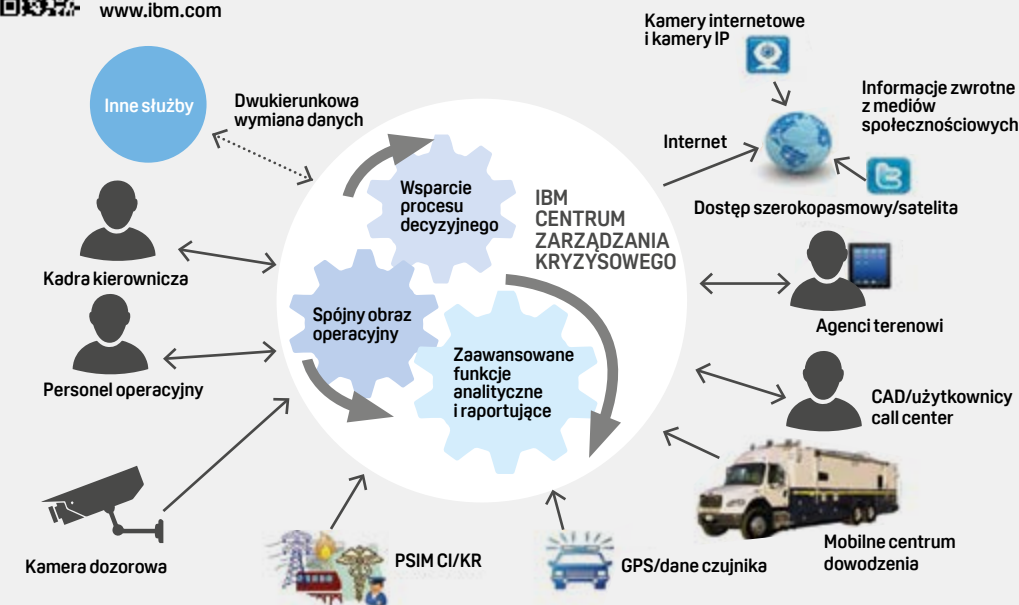
zwykła analiza VCA była podatna na zmiany pogody i oświetlenia, generowała dużą liczbę fałszywych alarmów oraz wymagała długiej i żmudnej kalibracji lub wymuszała sposób montażu kamer w celu zapewnienia skuteczności. Nowe kamery mogą się również komunikować z chmurą obliczeniową, gdzie są gromadzone ogromne ilości danych z obserwowanych scen (*Big Data*) i analizować je np. pod kątem strategii biznesowych. Otwiera też drogę do prawdziwie autonomicznych, samouczących i samokorygujących się systemów zabezpieczeń.

Deep Sense

Dahua Technology poszerza również portfolio rejestratorów. Dzięki współpracy z innym liderem w dziedzinie systemów sztucznej inteligencji – firmą NVIDIA – stworzyła pierwszy na świecie rejestrator NVR *Deep Sense* wykorzystujący układy NVIDIA® Tesla®P4 GPU. Jako serwer jest w stanie przeprowadzać analizę strukturalną aż 192 kanałów wideo, a algorytmy *Deep Learning* sprawiają, że system potrafi przeprowadzić symulację, wręcz dedukować na podstawie przechwytywanego obrazu wideo i reagować, zanim nastąpi incydent. Nowe produkty świetnie uzupełnią systemy rozpoznawania tablic rejestracyjnych i kontroli ruchu, z których firma Dahua Technology jest znana, a także umocnią jej pozycję jako lidera we wdrażaniu innowacyjnych rozwiązań security. ■



Przez kilkadziesiąt lat badań nad sytuacjami kryzysowymi i analiz skuteczności procedur reagowania gremium specjalistów wypracowało model obejmujący wszystkie aspekty zarządzania w czasie kryzysu.



Modelowe zarządzanie kryzysowe

Marek Okularczyk
dyrektor ds. rozwoju,
Program Smarter Cities

Modelowe zarządzanie kryzysowe obejmuje cztery fazy:

ZAPOBIEGANIE pełni podwójną funkcję. Z jednej strony ma możliwie najskuteczniej zapobiec wydarzeniu kryzysowemu, za drugiej zaś – maksymalnie złagodzić jego negatywne skutki. Kluczowe są tu: udoskonalona rekonstrukcja, regulacje, systematyczna analiza luk w zabezpieczeniach i ocena ryzyka.

PRZYGOTOWANIE obejmuje wszystkie czynności, które są prowadzone w oczekiwaniu na wydarzenie kryzysowe. Istotne są tu: analiza zagrożeń, ocena i pozyskiwanie zasobów, współpraca międzyagencyjna, ćwiczenia, przygotowanie dokumentacji.

REAGOWANIE to działania w obliczu kryzysu, niezbędne do ratowania życia, ochrony majątku i zaspokojenia podstawowych potrzeb ludzi, a także zainicjowania tymczasowego proce-

su odbudowy. Kluczowymi elementami tej fazy są: aktywacja trybu kryzysowego, pomoc medyczna, schronienie i ewakuacja, poszukiwania i ratunek, wtórna redukcja zniszczeń.

ODBUDOWANIE obejmuje opracowywanie, koordynowanie i wykonywanie napraw oraz remontów uszkodzonych obiektów i infrastruktury w trybie działań krótkoterminowych i rozłożonych w czasie. Na tę fazę składa się ocena strat, porządkowanie, odnowienie krytycznych systemów i obiektów, szybkie zapewnienie najważniejszych potrzeb, podstawowa rekonstrukcja.

Gdy podejście do zarządzania kryzysowego ewoluowało w czasie, zasoby niezbędne do realizacji tego modelu, w zależności od funkcji, są zorganizowane silosowo, wobec czego wymiana informacji jest tu trudna i często nieefektywna. W każdym mieście zwykle działają straż pożarna, policja, służby medyczne oraz wodociągowe i energetyczne – każda wyspecjalizowana i niezbędna w

swojej dziedzinie. Konieczność współpracy tych służb w obliczu kryzysu jest oczywista, jednak ich odrębność organizacyjna i administracyjna powoduje, że często jest to trudne zadanie. W odpowiedzi na te potrzeby IBM wspólnie ze specjalistami zarządzania kryzysowego opracował Centrum Zarządzania Kryzysowego.

Platforma zapewnia:

- 1) Szybka konsolidacja istniejących źródeł danych, następnie bezpieczny, oparty na uprawnieniach dostęp do informacji wykorzystywanych jednocześnie przez wiele służb. Zdolność do przetwarzania i analizowania danych w czasie rzeczywistym.
- 2) Zarządzanie pracami na terenie całego miasta – poprzez platformę dostępną zarówno kadry kierowniczej, jak i personelowi operacyjnemu – w centrum dowodzenia, a także operatorem pierwszego kontaktu i agentom terenowym. W zależności od uprawnień każdy użytkownik otrzymuje odpowiedni zasób informa-

cji oraz dostęp do spójnego obrazu operacyjnego (COP – *Common Operating Picture*).

- 3) Modelowanie standardowych procedur operacyjnych (SOP) w celu automatyzacji współpracy między służbami – zarówno w trakcie przygotowań, jak i w reagowaniu na wydarzenia i incydenty.
 - 4) Zaawansowane funkcje analityczne i raportujące, usprawniające zarządzanie zasobami we wszystkich fazach zarządzania kryzysowego.
 - 5) Graficzny pulpit użytkownika z interaktywnym podkładem GIS dla uzyskania orientacji przestrzennej i poszerzenia świadomości sytuacyjnej.
 - 6) Wsparcie procesu decyzyjnego dzięki możliwej symulacji i analizie potencjalnego oddziaływania różnych elementów wydarzenia kryzysowego.
- Platforma IBM Centrum Zarządzania Kryzysowego została doceniona przez służby zarządzania kryzysowego w wielu regionach świata, jednocześnie zaczyna już być wykorzystywana w Polsce. ■

Parkuj inteligentnie w erze IoT



STRESUJĄCE POSZUKIWANIA MIEJSCA PARKINGOWEGO

Po ulicach miast na całym świecie jeździ mnóstwo samochodów, które trzeba gdzieś zaparkować. A nie jest to czynność łatwa, ponieważ ograniczenia powierzchni parkingowej i liczby pracowników sprawiają, że zarówno nawigowanie do odpowiedniego miejsca, jak i egzekwowanie przepisów dotyczących parkowania stanowią obecnie duże wyzwanie. **Coraz częściej jednak kierowcy mogą korzystać z urządzeń komunikujących się ze sobą w ramach Internetu Rzeczy.**

William Pao
a&s International

Przy rosnącej liczbie pojazdów i zmniejszającej się powierzchni parkingów znalezienie w miastach miejsca do zaparkowania auta następcza niemałych trudności. Aby ulżyć zdesperowanym kierowcom, opracowano system inteligentnego parkowania. Ma on wiele zalet, do których należy zmniejszenie natężenia ruchu i emisji spalin. *Zredukowanie zatłoczenia o 10 procent przyczynia się do zwiększenia przychodów miasta o 2 procent.* Przykładowo oferowany przez nas system parkingowy przynosi miastu wielkości Los Angeles dodatkowo 20 miliardów dolarów – podaje Kurt Buecheler, wiceprezes ds. marketingu i rozwoju w Streetline, cytując ekonomistę Donalda Shoupa.

Technologia inteligentnego parkowania wpływa na zmniejszenie zatłoczenia, emisji spalin i dwutlenku węgla. Zapewnienie zmotoryzowanym bieżących danych na temat dostępności miejsc parkingowych eliminuje bowiem irytującą jazdę w poszukiwaniu wolnego miejsca – dodaje Jim Short, menedżer ds. sprzedaży na region EMEA w Smart Parking Technology.

Technika

W skład inteligentnego systemu parkowania wchodzi m.in. czujniki wykrywające wolne miejsca parkingowe. Informacje te przesyłają następnie do serwera, który z kolei przekazuje je użytkownikom za pośrednictwem aplikacji lub systemu znaków. Obecnie wykorzystuje się dwa typy czujników: ultradźwiękowe i magnetyczne. Czujniki ultradźwiękowe wykorzystujące fale dźwiękowe w zakresie od 25 do 50 kHz (powyżej zakresu słyszalności ludzkiego ucha) są zazwyczaj stosowane w przestrzeniach zamkniętych. Detektory łączą się z terminalem sterowania przewodowo (RS485) lub bezprzewodowo (na częstotliwości 433 MHz). Z kolei terminal może zostać podłączony do sieci Ethernet.

Na parkingach ulicznych zazwyczaj są stosowane detektory magnetyczne zasilane baterią, które umieszcza się pod ziemią. *Takie urządzenie ma stały zakres pomiarowy $\pm 1200 \mu T$ pola magnetycznego. Dla każdego czujnika użytkownik może określić szybkość*

przepływu danych wyjściowych w zakresie od 1563 Hz do 800 Hz. Czujnik może pracować poprawnie w szerokim zakresie temperatury od -40 do 85°C – wyjaśnia Manu Tayal, dyrektor generalny Centrum Doskonałości Internetu Rzeczy w Happiest Minds Technologies.

Detektory magnetyczne łączą się z terminalem centrali sterującej wyłącznie bezprzewodowo – podkreśla Jieruo Zhang, menedżer ds. systemów parkowania w Dahua Technology. – Dostępne są dwie metody łączenia bezprzewodowego: o krótkim zasięgu oraz NB-IoT. W przypadku rozwiązania o krótkim zasięgu detektor magnetyczny komunikuje się z pobliskim kontrolerem w paśmie 433 MHz. W drugim przypadku natomiast każdy detektor może się komunikować z siecią NB-IoT różnych

44% kierowców w Wielkiej Brytanii przyznaje, że poszukiwanie miejsca do parkowania wywołuje u nich stres.

operatorów mobilnych. Rozwiązanie NB-IoT sprawdzi się idealnie w przypadku wykorzystania urządzeń IoT na dużą skalę.

Nasze czujniki SENSIT łączą się z serwerem metodą bezprzewodową. Na potrzeby sieci radiowej utworzyliśmy węzły przekaźnikowe i bramy SENSIT – dodaje Edwin Siemerink, menedżer ds. ofertowania w Nedap Identification Systems.

Rola obrazu wideo

Tradycyjne czujniki ultradźwiękowe i magnetyczne wykrywają, czy miejsce jest wolne, czy zajęte. Coraz częściej jednak bardziej ekonomiczną alternatywą okazuje się obraz wideo. Kamera pozwala zidentyfikować, czy miejsce parkingowe jest wolne – mówi Adler Wu, menedżer ds. marketingu dla rozwiązań wertykalnych w Hikvision Digital Technology. – *Informacje, takie jak liczba wolnych miejsc, będą wyświetlane na mapce parkingu w czasie rzeczywistym. Użytkownicy mogą skorzystać z aplikacji, by znaleźć wolne miejsce, a system obliczy najszybszą trasę dojazdu.*

Niektóre firmy z branży telewizji dozorowej, takie jak Dahua, wprowadzają do zastosowań miejskich detekcję wideo – dodaje J. Zhang. – Każda kamera obejmuje zasięgiem dwa lub trzy miejsca parkingowe, a na parkingach podziemnych czy w budynkach parkingowych nawet sześć. Jest więc rozwiązaniem ekonomicznym, a jego budowa nie następcza problemów.

ANPR

W przeciwieństwie do tradycyjnych czujników specjalizowane kamery dozorowe mogą realizować ważną funkcję automatycznego rozpoznawania numerów rejestracyjnych (ANPR), pomocną w wielu zastosowaniach, np. parkowanie. Przykładowo rozwiązanie ANPR firmy Genetec – AutoVu – umożliwi użytkownikowi obserwowanie pojazdów znajdujących się na jego terenie lub przy ulicy. W tym przypadku kamerę można zamontować na pojeździe operatora, który objęddza dany teren, albo umieścić nad parkingiem otwartym, pozbawionym szlabanów. Kontrolę parkowania mogą również wspomóc poruszające się po ulicach pojazdy wyposażone w kamerę ANPR.

WSPIERANIE CZUJNIKÓW MAGNETYCZNYCH INNymi TECHNOLOGIAMI

Aby poprawić skuteczność detekcji systemów magnetycznych, niektóre firmy wprowadzają drugą technologię, zazwyczaj detektory podczerwieni. Stosujemy dwie technologie detekcji: w podczerwieni i magnetyczną. Zapewnia to najlepszą obecnie skuteczność – wyjaśnia Edwin Siemerink, menedżer ds. ofertowania w Nedap Identification Systems. – Detekcja magnetyczna może zostać łatwo zaburzona przez inne pojazdy, okablowanie, prace budowlane, linie metra, ruch tramwajów, dlatego dodatkowo wprowadziliśmy technologię IR. Na detekcję opartą na polu magnetycznym wpływa wiele czynników, np. znajdujące się w pobliżu duże elementy metalowe, różnego rodzaju zakłócenia pola, kruszywo w betonie czy mieszanki asfaltowe, mogące mieć właściwości magnetyczne, czy nawet magnesy znajdujące się w najbliższym sąsiedztwie – wylicza Jim Short, menedżer ds. sprzedaży na region EMEA w Smart Parking Technology. – W razie wykrycia w polu zmian na określonym poziomie czujniki magnetyczne wyzwalają detekcję IR, by potwierdzić wykrycie pojazdu.



INTELIGENTA FORMA PŁATNOŚCI ZA PARKING DZIĘKI SYSTEMOWI ANPR

Poza opcją płatności z góry (pre-paid) system automatycznego rozpoznawania numerów rejestracyjnych (ANPR) umożliwia także wnoszenie opłaty za postój jednorazowy. ANPR został już zainstalowany na wielu parkingach. Jego działanie polega na zeskanowaniu numeru rejestracyjnego auta przy wjeździe na parking. Gdy kierowca zamierza opuścić miejsce, musi wpisać numer rejestracyjny na panelu i zapłacić za postój. Innym rozwiązaniem jest automatyczne naliczanie opłat w taki sposób, by kierowca nie musiał udawać się do kasy. Udostępniamy aplikację mobilną dla zmotoryzowanych ze zintegrowaną funkcją płatności. Użytkownik może dowolną kwotą zasilić konto, które jest przypisane do konkretnego numeru rejestracyjnego pojazdu. Po wyjechaniu z parkingu opłata zostanie pobrana automatycznie – mówi Manu Tayal, dyrektor generalny Centrum Doskonalenia Internetu Rzeczy w Happiest Minds Technologies.

Technologię ANPR z powodzeniem można również wykorzystać w przypadku parkowania na ulicy. Firma Acer oferuje np. rozwiązanie składające się z automatu z zamontowanym czujnikiem ultradźwiękowym i kamery. Czujnik wykrywa, czy dane miejsce jest wolne. Gdy samochód je zajmie, kamera czyta tablice rejestracyjne oraz czas przyjazdu i odjazdu. Informacja ta następnie trafia do systemu płatniczego, który pobiera odpowiednią kwotę z konta kierowcy.

Dzięki ANPR bilet parkingowy nie musi już być papierowym kwitkiem, skoro może być wirtualnie powiązany z numerem rejestracyjnym. Wystarczy się zalogować, wpisać numer rejestracyjny i zapłacić za bilet.

Technologia ANPR ułatwia służbom parkingowym pracę. W przeszłości, aby sprawdzić, czy dany pojazd ma pozwolenie na parkowanie, trzeba było do niego podejść i sprawdzić, czy kierowca umieścił za szybą bilet parkingowy. Zajmuje to dużo czasu. Za pomocą ANPR można zrobić to samo, ale to obraz z kamery pozwoli ocenić, czy ktoś jest upoważniony do zatrzymania się w danym miejscu – wyjaśnia Charles Pitman, menedżer ds. marketingu produktu w Genetec. ANPR nie tylko upraszcza procedury, ale też ułatwia życie kierowcom. Przykładem może

być kampus uniwersytecki. Dawniej na początku semestru studenci musieli czekać w kolejkach, by kupić papierowe bilety parkingowe. Obecnie mogą zarejestrować się online i uiszczać należności za parkowanie z wykorzystaniem ANPR. Dzięki ANPR bilet parkingowy nie musi już być papierowym kwitkiem, skoro może być wirtualnie powiązany z numerem rejestracyjnym. Wystarczy się zalogować, wpisać numer rejestracyjny i zapłacić za bilet – dodaje Ch. Pitman.

Prawdziwa wartość tkwi w danych

Oprócz ułatwienia nawigacji dane generowane przez czujniki i urządzenia mogą być poddane analizie, która pomoże władzom miast usprawnić świadczenie usług i podnieść jakość życia mieszkańców. W erze IoT, Big Data i e-gospodarki przepływ danych jest niezwykle istotny. Bez danych o numerach rejestracyjnych nagrań z parkingów niewiele by

wniosły w kwestii inteligentnego parkowania. W przypadku inteligentnego parkowania z detekcją wideo dane o parkowaniu i płatnościach mogą przynieść wartość dodaną przynajmniej w trzech aspektach – podkreśla J. Zhang. – Po pierwsze system prowadzi kierowców na miejsce i do wyjazdu, co poprawia rotację na całym parkingu. Po drugie zapewnia indywidualnie dopasowane usługi parkingowe, takie jak rezerwacje czy zarządzanie miejscami VIP, generując większą wartość dodaną. Po trzecie przy stałej liczbie użytkowników i stabilnym przepływie środków aplikacja parkingowa może stać się popularnym portalem kierowców, z którego będą korzystać np. myjnie czy punkty wynajmu samochodów. ANPR automatyzuje przepływ pojazdów. Zapewnia właścicielom parkingów obszerne dane dotyczące czasu parkowania, a także opracowanie wariantów opłat w zależności od floty i liczby pojazdów – wyjaśnia Adler Wu.

Mieszkańcy Londynu zazwyczaj poświęcają 8 minut na poszukiwanie miejsca parkingowego.

Inteligentne parkowanie w sposób oczywisty przyczynia się do usprawnienia zarządzania miastem. Jego prawdziwą wartość stanowią jednak dane, które pomogą podejmować właściwe decyzje dotyczące planowania i rozwoju miasta. Ułatwi zarówno wskazanie rejonów, w których brakuje miejsc do parkowania, jak i podejmowanie decyzji o budowie garaży, wyznaczeniu dodatkowych miejsc parkingowych lub podniesieniu tam opłat parkingowych. System zbiera wszystkie dane, które można eksportować i na ich podstawie tworzyć raporty oraz określać np. czy dostępność parkingów na danym obszarze jest wystarczająca – wyjaśnia Ch. Pitman. – Jest to pomocne w długofalowym planowaniu i strategii poprawy dostępności parkingów

Kierowcy w Wielkiej Brytanii spędzają średnio 4 dni w roku na poszukiwaniu miejsca parkingowego.

czy decydowaniu o budowie garaży.

Wszystko to jest oparte na analizie Big Data – podkreśla Jay Liu, menedżer ds. inteligentnej identyfikacji i transakcji w firmie Acer. – Jeżeli miasto zamierza zwiększyć przepustowość na danym obszarze, czyli np. nie chce, aby ludzie zostawiali swoje samochody na parkingu na cztery czy pięć godzin, może podnieść opłaty parkingowe. Należy więc dokonywać analiz i wyciągać wnioski. W ten sposób można np. regulować opłaty za parkowanie w zależności od nasilenia ruchu na drogach.

W ostatecznym rozrachunku może to oznaczać więcej wpływów do budżetów miast. Urządzenia są niezbędne do zbierania aktualnych danych dotyczących wykorzystania miejsc na parkingach, prędkości jazdy po autostradach, badania tras przejazdu, ale nie tylko. Oferowany przez nas system

przyczynił się do zwiększenia częstotliwości parkowania w miastach aż o 172 procent. Dzięki niemu zanotowaliśmy wzrost przychodów o 11 procent. Centrum miasta stało się bardziej dostępne, więc przyjeżdża tu więcej osób. Jesteśmy na początku „inteligentnej miejskiej jazdy”, a parking oznacza linię startu – mówi Kurt Buechler, wiceprezes ds. rozwoju marketingu i biznesu w Streetline.

Bardziej inteligentne niż kiedykolwiek

Inteligentne parkowanie z pewnością stanowi istotny element inteligentnego miasta. Komunikujące się czujniki i urządzenia ułatwiają nawigację i płatności, a generowane przez nie dane zapewniają władzom miast i operatorom lepszy wgląd w sposoby usprawniania usług oraz opracowywania odpowiednich do potrzeb planów rozwoju. Miasta na całym świecie dążą do tego, by stać się bardziej inteligentne. W realizacji tego celu inteligentne parkowanie wyznacza kierunek. ■

Źródło: British Parking Association



AS ALNET SYSTEMS
PROFESJONALNE OPROGRAMOWANIE VMS

PRS - bezpłatny dodatek do rozpoznawania tablic rejestracyjnych
minimalne wymagania dla PRS ALNET - NetStation 8 lub wyższy

Ponad 200 000
systemów na świecie
najnowsze referencje:



Sieć sklepów Auchan Rosja
2500 kanałów IP



Państwowe Koleje Łotewskie
6500 kanałów IP



Komisja Europejska Luksemburg
1300 kanałów IP

www.alnetsystems.com www.youtube.com/alnetsystems



Inteligentne miasto musi być przede wszystkim bezpieczne. Systemy security są zatem nieodłącznym elementem projektów *safe cities*. Odpowiadają przy tym nie tylko za aspekt zabezpieczeń, ale także stanowią część „inteligentnego” systemu sterującego i usprawniającego funkcjonowanie w wielkim miejskim organizmie.

Smart cities jako źródła danych pozwalających zrozumieć rytm miasta



Jan T. Grusznicki
Sales Engineer,
Axis Communications

Już 54% ludzi na świecie żyje w miastach. Szacuje się, że postępująca urbanizacja przy ogólnym wzroście populacji przyczyni się do zwiększenia liczby mieszkańców aglomeracji miejskich o 2,5 mld. Jak wskazuje ONZ, zarządzanie obszarami miejskimi stało się jednym z ważniejszych wyzwań XXI w., stąd koncepcja tzw. inteligentnych miast, dla których najważniejszym czynnikiem działania jest lokalizowanie jak największej liczby

– a najlepiej wszystkich – informacji w przestrzeni. Analizowanie zmiennych i różnorodnych zbiorów danych, tzw. *Big Data*, stanie się wkrótce podstawowym elementem prawidłowego funkcjonowania miasta, tak jak znajdujący się niemal w każdej aglomeracji system dozoru wizyjnego. Świadomość planów wykorzystania tego narzędzia w przyszłości już zmienia sposób postrzegania kamer wykorzystywanych dziś głównie do patrolowania okolicy miejsc ich

instalacji. Dotychczas bowiem kamery w przestrzeni miejskiej służyły tylko jako narzędzie do zdalnego nadzoru, wykorzystywane przez operatorów systemu monitoringu lub przedstawicieli służb. W koncepcji *smart city* zaczynają być traktowane jako źródła nieprzetworzonych danych pozwalających zrozumieć rytm miasta. Na wartość wynikową każdej analizy wpływa jakość danych wprowadzanych do systemu, stąd nie bez znaczenia pozostaje odpowiedni do-

Rozwiązania wspierające bezpieczeństwo pracowników biurowców



Wojciech Pawlica
Product Manager,
Dahua Technology Poland

Liczba osób pracujących zawodowo na stanowiskach biurowych od lat systematycznie rośnie. Wymusza to na pracodawcach i pracownikach coraz większą dbałość także o szeroko pojęte bezpieczeństwo. Zmieniają się w tym zakresie również uwarunkowania prawne wprowadzające do obowiązków pracodawców nowe wytyczne. Dla bezpieczeństwa pracowników

w obiektach biurowych instaluje się różne systemy, pośrednio lub bezpośrednio wpływające na poprawę ochrony. Jednym z podstawowych wymogów jest wyposażenie biura w systemy ochrony przeciwpożarowej i alarmowej. Uzupełnieniem są systemy dozoru wizyjnego oparte na technologii IP, coraz bardziej popularne w całej przestrzeni publicznej. Możliwość rejestracji obrazu z kamer, wykorzystanie nowoczesnych metod cyfrowej analizy obrazu czy nowych technologii, np. Starlight w kamerach Dahua Technology, zdecydowanie poprawiło bezpieczeństwo pracowników. Dahua Technology oferuje również uzupełnienie powyższego systemu o dwa kolejne stopnie zabezpieczenia typowego biura. Pierwszym jest system wideodomofonów zabezpieczający wejścia do obiektu. Zastosowana technologia IP ułatwia integrację z kamerami. Obraz z kamer IP może być wy-

świetlany na monitorze wideodomofonu, a obraz z kamery stacji bramowej wideodomofonu – nagrywany na rejestratorze sieciowym. Ciekawym rozwiązaniem jest możliwość dołączenia do monitora czujek alarmowych i wykorzystanie go jako niedużej centrali alarmowej. To idealne rozwiązanie dla małych biur, a przede wszystkim tych, które wcześniej nie miały systemu alarmowego. W przypadku alarmu powiadomienie może trafić do fizycznej ochrony budynku lub ze stacji monitorującej. Dahua Technology oferuje również wideodomofon 2-przewodowy, w którym zasilanie oraz dane wykorzystują jedynie pojedynczą parę przewodów. Rozwiązanie jest atrakcyjne dla firm, które istniejący system analogowy chcą w jak najprostszy sposób wymienić na cyfrowy IP. Drugim rozwiązaniem zwiększającym bezpieczeństwo biura jest system kontroli dostępu. Dahua proponuje kom-

pleksowe rozwiązanie – od różnego rodzaju czytników (klawiatura, karty RFID, czytniki biometryczne), poprzez różne kontrolery (2- i 4-drzwiowe) w różnym wykonaniu (montowane w samodzielnych skrzynkach lub np. w rozdzielniach na szynie DIN), aż po elektroniczne zamki i zwory elektromagnetyczne. Zastosowanie systemu kontroli dostępu do newralgicznych pomieszczeń w biurze (serwerownia, kasa czy archiwum) nie tylko zapewnia ochronę finansów czy danych, ale także znacząco poprawia poczucie bezpieczeństwa osób tam pracujących. Bezpieczeństwo obiektów biurowych można i należy rozpatrywać na wielu płaszczyznach. To nie tylko kontrola dostępu do obiektu, ochrona przed włamaniem, pożarem czy zalaniem. To również ochrona danych komputerowych czy danych osobowych pracowników. Ale to już zupełnie inny temat.

bór kamer w celu utrzymania powtarzalności próby. Powoli, ale coraz częściej w aglomeracjach są instalowane kamery stałopozycyjne pracujące w widmie widzialnym lub termowizyjne służące do obserwacji zagęszczenia pojazdów lub ludzi, płynności ruchu pojazdów czy oznaczenia liczby wolnych miejsc parkingowych. Analizując obrazy w czasie, można lepiej prognozować zmiany wynikające np. z następstw anomalii pogodowych, skutki ewentualnych awarii, konsekwencje zgradowień lub wypadków drogowych. Poprawna analiza wszystkich tych elementów

zlokalizowanych w przestrzeni i czasie pozwala zapobiegać szkodliwym zjawiskom, podejmować decyzje oparte na prawidłowych przesłankach oraz optymalną alokację środków. Z inteligentnym miastem wiąże się duża liczba danych oraz rzeczywisty lub prawie rzeczywisty czas dostarczania informacji, prezentowanych np. w postaci dynamicznych grafik nakładanych bezpośrednio na obraz z kamery. Synergia obrazu bieżącego z dodatkowymi informacjami w ramach tzw. wirtualnej rzeczywistości usprawnia zarządzanie incydentami, a nawet pomaga w zapobieganiu im.

Przetwarzanie dużej liczby danych w sposób zorganizowany w ramach *Big Data* często prowadzi do zdobywania nowej wiedzy. W przypadku miast i wykorzystania systemów kamer Axis stosuje się do tego model rozproszony. Przechwycony obraz jest zapisywany na serwerach, podczas gdy wstępnej analizie zawartości obrazu dokonuje się bezpośrednio w kamerze. Uzyskane w ten sposób dane stanowią podstawę do dalszej, głębszej analizy zmian w obrazie wykonywanej bezpośrednio na danych archiwalnych. Przykładami takiego rozwiązania są algorytmy rozpoznania i póź-

niejsza analiza twarzy w tłumie czy choćby detekcja osób i bardziej wymagająca analiza ich ubioru. *Big Data*, wirtualna rzeczywistość i IoT to nie tylko moda. To kierunek towarzyszący nam zmian, dotyczący każdej dziedziny życia, również w zakresie bezpieczeństwa. W niedalekiej przyszłości wraz ze wzrostem mocy obliczeniowej procesorów w kamerach będą możliwe coraz bardziej skomplikowane operacje matematyczne, co przełoży się na wykorzystywanie mechanizmów z rodziny *Deep Learning* i w konsekwencji ugruntowanie pozycji tych popularnych zwrotów.

Kamery w miejskich systemach monitoringu wizyjnego



Kamil Okrasa
Solution Specialist,
Hikvision Poland

Korzyści zapewniane przez systemy dozoru wizyjnego w przestrzeniach miejskich to nie tylko przeciwdziałanie przestępczości, ale także wpływ na jakość życia i rozwój infrastruktury miejskiej. To także wyzwania związane zarówno z odpowiednią ochroną zróżnicowanych obiektów użytku publicznego, jak i koniecznością obserwowania otwartych przestrzeni. Właściwe zabezpieczenie obszarów miejskich wymaga także integracji wielu

systemów, takich jak kontrola dostępu, telewizja dozorowa czy sygnalizacja włamania i napadu.

Kamery stosowane w systemie monitoringu miasta mają za zadanie umożliwić operatorom realizację dwóch podstawowych celów: identyfikację zagrożenia oraz identyfikację ewentualnych sprawców. Cele te, z technicznego punktu widzenia, są niejako ze sobą sprzeczne, ponieważ wymogiem w przypadku pierwszego jest zastosowanie kamery o jak najszerszym polu obserwacji, natomiast drugiego – uzyskanie obrazu o jak najlepszej jakości (wyrażanej np. liczbą pikseli na metr). Ponadto przestrzeń miejska charakteryzuje się dynamicznymi zmianami oświetlenia, występowaniem jednocześnie intensywnych źródeł światła oraz fragmentów słabo oświetlonych, a także pozbawionych oświetlenia. Wyzwaniom tym sprostają kamery serii PanoVu oferowane przez firmę Hikvision. Połączenie w jednej obudowie kamery panoramicznej z ka-

merą obrotową PTZ otwiera nowe możliwości obserwacji stref objętych dozorem. Poza oczywistą zaletą wynikającą z realizacji podglądu obrazu w zakresie 180 lub 360 stopni w czasie rzeczywistym takie rozwiązanie ma jeszcze jedną, być może najistotniejszą cechę. Obie jednostki zostały ze sobą sprzężone programowo w sposób umożliwiający szybkie ustawienie pozycji poprzez zaznaczenie myszą interesującego obszaru na obrazie panoramicznym. Panorama zapewnia widok ogólny, pozwalający ocenić sytuację i podjąć decyzję o wyborze obserwowanego obiektu, a uzyskanie dzięki modułowi PTZ obrazu o wysokiej rozdzielczości trwa chwilę. Co więcej, takie rozwiązanie znacznie ułatwia śledzenie wielu celów jednocześnie, nawet gdy znajdują się one po przeciwnych stronach punktu kamerowego. Standardem w urządzeniach tej klasy są funkcje analityczne zawartości obrazu, takie jak wykrywanie przekroczenia linii lub detekcja intruza.

Spośród rozwiązań przeznaczonych dla miast wartę uwagi są systemy parkingowe, nie rzadko sprzężone z systemami telewizji dozorowej. Algorytmy rozpoznające numery rejestracyjne pojazdów, zaimplementowane w kamerach Hikvision, w połączeniu z funkcjami wykrywania wolnych miejsc parkingowych pozwalają zbudować system umożliwiający zarządzanie miejscami parkingowymi. Po wprowadzeniu numeru rejestracyjnego w interaktywnym kiosku system wskaże, gdzie został zaparkowany pojazd, a detektory zintegrowane z kamerami ułatwią znalezienie wolnego miejsca. Jedna kamera jest w stanie objąć polem działania kilka miejsc parkingowych, nadzorem wizyjnym można objąć każdy pojazd, a zarejestrowany materiał będzie pomocny w przypadku różnego rodzaju nieprzyjemnych zdarzeń, takich jak kradzież, zarysowanie drzwi lub innych „niespodzianek” charakterystycznych dla dużych, wielopoziomowych parkingów.

Bezpieczne miasto – wyzwania stawiane systemom dozorowym



Jakub Sobek
certyfikowany trener techniczny,
Linc Polska

Systemy monitoringu wizyjnego na stałe wpisały się w krajobraz wielu polskich miast. Nie budzą sprzeciwu mieszkańców, a wielokrotnie to na ich prośbę miasta lub mniejsze lokalne społeczności decydują się na zakup kolejnych kamer. Miejskie systemy monitoringu kojarzą się z klasycznymi systemami CCTV, z kamerami PTZ i kamerami stałopozycyjnymi. Główną zmianą, jaka zaszła w nich w ostatnich latach, jest jakość

obrazu trafiającego do centrum monitoringu. Dużo częściej stosuje się kamery o rozdzielczości kilku megapikseli, które oferują wyższą jakość obrazu. Kamery PTZ, dzięki coraz lepszej optyce i dostępnemu zoomowi, pozwalają także na monitorowanie większych obszarów. Patrząc jednak od „kuchni” na funkcjonowanie tych systemów, trzeba mieć świadomość, że wielu zdarzeń, które dzieją się w obszarze widzenia kamer, operator stacji monitorowania często nie zauważa. Kiedy musi jednocześnie obserwować wiele obrazów, jego percepcja i skuteczność dostrzegania zagrożeń znacznie spada już po kilkunastu minutach. Z pewnością wzrośnie w kolejnych latach znaczenie analizy wideo w systemach monitoringu. Tylko dzięki wsparciu dedykowanych algorytmów można poprawić skuteczność wykrywalności zdarzeń. Już teraz są dostępne rozwiązania pozwalające np. na detekcję osób pozo-

stających zbyt długo w zdefiniowanych obszarach lub pozostawionych przedmiotów. W przyszłości na popularności zyskają algorytmy behawioralne, które będą miały za zadanie wykrywać nietypowe zachowania lub identyfikować poszukiwane osoby na podstawie danych biometrycznych, takich jak twarz lub cech indywidualnych, np. rodzaj chodu. Coraz częściej, gdy słyszymy, że miał miejsce jakiś atak terrorystyczny lub wypadek, po chwili to samo zdarzenie możemy prześledzić w Internecie z wielu różnych ujęć. Część filmów pochodzi rzeczywiście z kamer miejskiego systemu monitoringu, niektóre z kamer zamontowanych na obiektach prywatnych, przeważają jednak filmy z telefonów komórkowych czy rejestratorów wideo zainstalowanych w prywatnych pojazdach. Wszystkie te „dodatkowe” kamery wypełniają luki w systemach monitoringu miejskiego. Bardzo kosztowne jest przecież objęcie dozorem całego miasta. W ten

trend wpisują się coraz popularniejsze kamery nasobne, czyli niewielkie kamery mocowane na mundurach policjantów czy strażników miejskich. Dzięki wbudowanym systemom transmisji wideo operator stacji monitoringu widzi na mapie lokalizację każdego z funkcjonariuszy i w razie potrzeby może obejrzeć obraz z jego kamery. Zapewne systemy będą dodatkowo uzupełniane kamerami z metra, autobusów i tramwajów, a w przyszłości także z dronów wykorzystywanych w trakcie działań obserwacyjnych, patrolowych czy pościgowych. Wyzwaniem, z którym już teraz przychodzi się zmierzyć, jest integracja obrazów z tych wszystkich kamer w jednym oprogramowaniu po stronie centrum monitoringu. Ze względu na ilość danych, jaka tu będzie spływać, tylko profesjonalne i dedykowane rozwiązania pozwolą operatorom na wygodną i skuteczną pracę. Dla nas wszystkich będzie to oznaczać bezpieczniejsze miasto.



Grzegorz Ćwiek
prezes,
Schrack Seconet Polska

Bezpieczeństwo pożarowe obiektów

Nie ma jednego właściwego zestawu wytycznych czy obowiązujących aktów prawnych, w pełni odpowiadających budynkom, w których przebywają ludzie, a także norm oraz zaleceń specjalnych, np. związanych z infrastrukturą krytyczną (choćby dla budynków rządowych). Zarówno projektanci, jak i wykonawcy instalacji ppoż. muszą naj-

pierw odnieść się do przepisów ogólnych, a następnie ocenić możliwość ich zastosowania w konkretnym przypadku. Potrzeby szczegółowe w zakresie doboru odpowiedniego systemu zabezpieczenia wynikają z indywidualnych potrzeb użytkowników i charakterystyki użytkowej obiektu – jego wyposażenia stałego lub tymczasowego. Ponadto ze względu na to, że obiekty

biurowe należą do obiektów użyteczności publicznej należy uwzględniać odpowiednie wymagania dla danej klasy (kategorii ZL) zagrożeń zidentyfikowanych dla danego budynku, a także jego wysokość – co również wpływa na zakres ochrony przeciwpożarowej, jaką musi lub może zostać objęty. Budynek biurowy może być również usytuowany (i naj-

biurowych

częściej tak się dzieje) w sąsiedztwie innych obiektów o podobnym lub różnym przeznaczeniu, co wpływa na zakres i wymagania dotyczące zastosowania koniecznych (minimalnych) lub dodatkowych zabezpieczeń przeciwpożarowych. Można jednak wyróżnić dwie istotne cechy obiektów biurowych, które powinny być podstawą analizy zagrożeń

i doboru odpowiednich środków przeciwdziałania zagrożeniom (pożarom) w takich budynkach. Po pierwsze są to obiekty, w których ludzie przebywają czasowo, w sposób powtarzalny (w przeciwieństwie np. do obiektów mieszkalnych, w których uznaje się, że ludzie przebywają w nich „na stałe”), ale jednak ich wymienność (fluktuacja) i dynamika przemieszczania się są znacznie mniejsze niż w przypadku obiektów np. handlowo-usługowych czy sportowych. Po

drugie są to budynki biurowe, w których zwykle są ulokowane siedziby firm lub organizacji mających własne, odrębne kultury organizacyjne, regulaminy, przepisy i normy zachowań indywidualnych oraz zespołowych. Mogą one także posiadać własne wytyczne i procedury związane z zachowaniem pracowników i ich gości w warunkach zagrożenia życia (wytyczne korporacyjne, branżowe itp.). Wpływają one w bardzo istotny sposób na organizację ewakuacji ludzi

w przypadku wystąpienia zjawiska kryzysowego wywołanego pożarem rzeczywistym lub nawet fałszywym alarmem. Zasygnalizowane pokrótce czynniki determinujące zakres i sposób zapewnienia bezpieczeństwa osobom przebywającym w budynku biurowym powinny skłonić do głębszej refleksji na temat problematyki bezpieczeństwa pożarowego w obiektach biurowych w odniesieniu do budynków o innym przeznaczeniu.



Bezpieczeństwo pożarowe obiektów biurowych

Według Polskiej Klasyfikacji Obiektów Budowlanych (PKOB) budynki biurowe to obiekty budowlane *wykorzystywane jako miejsca pracy dla działalności biura, sekretariatu lub innych prac o charakterze administracyjnym, np. budynki banków, urzędów pocztowych, urzędów miejskich, gminnych, ministerstw*, przeznaczone dla wydziałów administracyjnych. Grupa 122 (PKOB) wymienia także budynki centrów konferencyjnych, kongresów, sądów i parlamentów.

Grzegorz Ćwiek
prezes, Schrack Seconet Polska

Klasyfikacja PKOB¹⁾ do budynków biurowych nie zalicza pomieszczeń biurowych w budynkach przeznaczonych głównie do innych celów. W związku z tym obiekty handlowo-usługowe, produkcyjne czy sportowe stanowią oddzielną grupę klasyfikacyjną.

Mimo wymienionych wyłączeń kształtuje się całkiem pokaźna i różnorodna grupa obiektów budowlanych z całym wachlarzem zagadnień i problemów związanych z obszarem bezpieczeństwa pożarowego konstrukcji budowlanych. Z punktu widzenia przepisów i norm powiązanych z ochroną przeciwpożarową (również z systemami zabezpieczeń elektronicznych) znajdują tu zastosowanie zarówno akty prawne przyjmowane zwy-

czajowo jako podstawowe dla budynków, w których przebywają ludzie²⁾, jak i wiele norm oraz zaleceń specjalnych, np. związanych z infrastrukturą krytyczną (choćby dla budynków rządowych).

Z tego też względu nie ma jednego właściwego zestawu wytycznych czy obowiązujących aktów prawnych, w pełni odpowiadających tego typu budynkom. Zarówno projektanci, jak i wykonawcy instalacji bezpieczeństwa pożarowego muszą najpierw odnieść się do przepisów ogólnych, a następnie ocenić możliwość ich zastosowania w konkretnym przypadku. Potrzeby

szczegółowe w zakresie doboru odpowiedniego zabezpieczenia wynikają z indywidualnych potrzeb użytkowników i charakterystyki użytkowej obiektu – jego wyposażenia stałego lub tymczasowego. Ponadto ze względu na to, że obiekty biurowe należą do obiektów użyteczności publicznej należy uwzględniać odpowiednie wymagania dla danej klasy (kategorii ZL) zagrożeń zidentyfikowanych dla danego budynku, a także jego wysokość – co również wpływa na zakres ochrony przeciwpożarowej, jaką musi lub może zostać objęty.

Budynek biurowy może być również usytuowany (i najczęściej tak się dzieje) w sąsiedztwie innych obiektów o podobnym lub różnym przeznaczeniu, co wpływa na zakres i wymagania dotyczące zastosowania koniecznych (minimalnych) lub dodatkowych zabezpieczeń przeciwpożarowych.

Można jednak wyróżnić dwie istotne cechy obiektów biurowych, które powinny być podstawą analizy zagrożeń i doboru odpowiednich środków przeciwdziałania zagrożeniom (pożarom) w takich budynkach:

1) Przede wszystkim są to obiekty, w których ludzie przebywają czasowo, w sposób powtarzalny (w przeciwieństwie np. do obiektów mieszkalnych, uznaje się, że ludzie przebywają w nich na stałe), ale jednak ich wymienność (fluktuacja) i dynamika przemieszczania się są znacznie mniejsze niż w przypadku obiektów, np. usługowo-handlowych czy sportowych.

2) W budynkach biurowych zwykle są ulokowane siedziby firm lub organizacji mających własne, odrębne kultury organizacyjne, regulaminy, przepisy i normy zachowań indywidualnych oraz zespołowych. Mogą one także posiadać własne wytyczne i procedury związane z zachowaniem

Zarówno projektanci, jak i wykonawcy instalacji bezpieczeństwa pożarowego muszą najpierw odnieść się do przepisów ogólnych, a następnie ocenić możliwość ich zastosowania w konkretnym przypadku.

pracowników i ich gości w warunkach zagrożenia życia (wytyczne korporacyjne, branżowe itp.). Wpływają one w bardzo istotny sposób na organizację ewakuacji ludzi w przypadku wystąpienia zjawiska kryzysowego wywołanego rzeczywistym pożarem lub nawet fałszywym alarmem. Zasygnalizowane pokrótce czynniki determinujące zakres i sposób zapewnienia bezpieczeństwa osobom przebywającym w budynku biurowym powinny skłonić do głębszej refleksji na temat problematyki bezpieczeństwa pożarowego w obiektach biurowych w odniesieniu do budynków o innym przeznaczeniu. ■



Nie ma jednego właściwego zestawu wytycznych czy obowiązujących aktów prawnych, w pełni odpowiadających specyfice budynków biurowych.

¹⁾ PKOB – Polska Klasyfikacja Obiektów Budowlanych. Podstawa prawna: Rozporządzenie Rady Ministrów z 30.12.1999 r. w sprawie Polskiej Klasyfikacji Obiektów Budowlanych.
²⁾ Ustawa Prawo budowlane (Dz.U. z 2006 r., nr 156, poz. 1118 z późn. zm.); Ustawa z 24 sierpnia 1991 r. O ochronie przeciwpożarowej (Dz.U. z 2009 r., nr 178, poz. 1380 z późn. zm.); Rozporządzenie Ministra Infrastruktury z 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz.U. z 2002 r., nr 75, poz. 690 z późn. zm.); Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 16 czerwca 2003 r. w sprawie przeciwpożarowego zaopatrzenia w wodę oraz dróg pożarowych (Dz.U. nr 121, poz. 1139 z późn. zm.) i inne.

Ciągłość zasilania urządzeń przeciwpożarowych w zapewnieniu bezpieczeństwa pożarowego obiektów biurowych

Budynki biurowe należą do grupy obiektów użyteczności publicznej i jako takie wymagają ochrony przeciwpożarowej w zależności od ich wysokości i powierzchni. Najczęściej obiekty te lub ich części – stanowiące odrębne strefy pożarowe – są kwalifikowane do kategorii ZLIII zagrożenia ludzi.

Edward Skiepmo
rzeczoznawca do spraw zabezpieczeń przeciwpożarowych

Jeżeli mogą w nich przebywać ludzie w grupach większych niż 50 osób, niebędący ich stałymi użytkownikami, wówczas strefę tę należy zakwalifikować do kategorii ZLI zagrożenia. Przykładem może być budynek biurowy z restauracją na parterze, w której są organizowane przyjęcia okolicznościowe dla osób niebędących pracownikami biurowca. Będzie on posiadał co najmniej dwie różne strefy pożarowe. Budynki w zależności od ich wysokości dzielimy na:

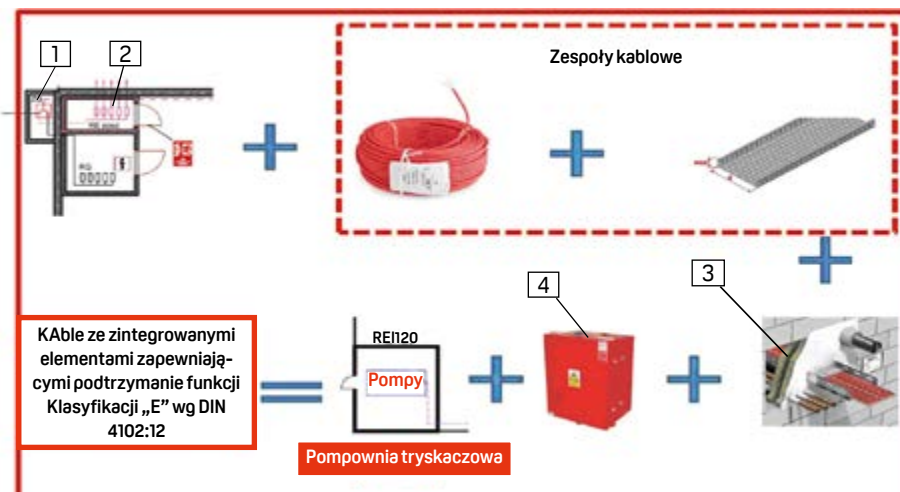
- niskie – o wys. do 12 m,
- średnio wysokie – od 12 do 25 m,
- wysokie – od 25 do 55 m,
- wysokościowe – powyżej 55 m.

Wysokość budynków jest mierzona zgodnie z rozporządzeniem Ministra Infrastruktury [1]. Im większa wysokość budynku i jego powierzchnia, tym większe wymagania związane z wyposażeniem go w techniczne systemy zabezpieczeń. W tabeli 1 przedstawiono (w uproszczeniu) wymagania w tym zakresie dla części naziemnej budynków biurowych o zbliżonej powierzchni zabudowy.

W tabeli wyróżniono – kolorem żółtym – instalacje przeciwpożarowe, którym stawia się szczególne wymagania, jeśli chodzi o sposób i źródło zasilania. Przed rozpoczęciem projektowania i wykonania instalacji należy rozważyć, czy mają one pracować również w warunkach pożaru, czy tylko do momentu jego wykrycia. Jeżeli dany obwód czy instalacja mają funkcjonować w warunkach pożaru, to generalną zasadą za-

pewniającą poprawność działania jest ich prawidłowe zasilanie i sterowanie. Należy skoncentrować się na tym, aby osiągnąć efekt końcowy, czyli zapewnić ich normalne, bezawaryjne działanie w warunkach pożaru. W praktyce zachowanie się instalacji można sprawdzić tylko w jeden sposób – podczas pożaru, ale jest to metoda destrukcyjna, nie do wykonania w normalnych warunkach. Pożar jest zdarzeniem wyjątkowym, ale

Rys. 2. Idea zachowania funkcjonalności zasilania w warunkach pożaru: 1 – złącze główne z przeciwpożarowym wyłącznikiem prądu, 2 – rozdzielnia stanowiąca odrębną strefę pożarową zasilającą urządzenia ppoż., 3 – przepusty ogniowe w elementach oddzielenia przeciwpożarowych, 4 – szafa w klasie E zachowania ciągłości zasilania



dla większości urządzeń ppoż. – stanem ich normalnej pracy. Muszą więc zostać zaprojektowane i wykonane z dużą rezerwą obejmującą ewentualne nieprzewidziane zdarzenia, które mogą wystąpić w trakcie eksploatacji. Dlatego wiele z nich jest objętych badaniami określającymi ich przydatność do stosowania w ochronie przeciwpożarowej [3]. Szczególne wymagania dotyczą zasilania urządzeń i sterowania w dwóch stanach ich pracy – do momentu wykrycia pożaru i pracę w warunkach pożaru. W zależności od nich dobiera się rozwiązania techniczne zapewniające ich funkcjonowanie. Obejmują one:

- źródła zasilania urządzenia,
- sposób ich zasilania,
- dobór elementów rozdzielczych i łączniowych,
- zastosowanie odpowiednich kabli,
- właściwe usytuowanie – bezpieczne z punktu widzenia ochrony przeciwpożarowej,
- odpowiedni moment ich uruchomienia,
- odporność na zakłócenia.

W literaturze często spotyka się sformułowanie doskonale oddające ideę takich

	Niski [N]	Średnio wysoki [SW]	Wysoki [W]	Wysokościowy [WW]
	Ppoż. wyłącznik prądu	Ppoż. wyłącznik prądu	Ppoż. wyłącznik prądu	Ppoż. wyłącznik prądu
	Oświetlenie awaryjne ¹⁾	Oświetlenie awaryjne ¹⁾	Oświetlenie awaryjne	Oświetlenie awaryjne
	Hydranty wewnętrzne (średnica 25) ²⁾	Hydranty wewnętrzne (średnica 25) ³⁾	Hydranty wewnętrzne (średnica 25)	Hydranty wewnętrzne (średnica 25)
		System oddymiania klatek schodowych	Zabezpieczenie przed zadymieniem klatek schodowych	Zabezpieczenie przed zadymieniem klatek schodowych
			Zabezpieczenie przed zadymieniem poziomych dróg ewakuacyjnych	Zabezpieczenie przed zadymieniem poziomych dróg ewakuacyjnych
			Pompownia pożarowa ze zbiornikiem wody	Pompownia pożarowa ze zbiornikiem wody
			Instalacja sygnalizacji pożarowej SSP	Instalacja sygnalizacji pożarowej SSP
			Instalacja DSO: dźwiękowego systemu ostrzegawczego	Instalacja DSO: dźwiękowego systemu ostrzegawczego
			Dźwigi dla ekip ratowniczych ⁴⁾	Dźwigi dla ekip ratowniczych
			Zawory (śred. 52)	Zawory (śred. 52)
				Instalacja tryskaczowa

¹⁾ O ile występują kryteria wskazane w § 181 [1].

²⁾ O powierzchni strefy pożarowej >1000 m².

³⁾ O powierzchni strefy poż. >200m² lub 1000 m².

⁴⁾ Jeżeli poziom posadzki najwyższej kondygnacji użytkowej znajduje się na wys. >25 m.

rozwiązań – mowa o kablach ze zintegrowanymi elementami zapewniającymi podtrzymanie funkcji. Z punktu widze-

nia działania systemów to bardzo dobre określenie obejmujące całościowo kwestie związane z zasilaniem w budyn-

CENTRALA STERUJĄCA urządzeniami przeciwpożarowymi



Urządzenie modułowe przeznaczone do sterowania i nadzorowania pracy wszystkich urządzeń w budynku, które będą uruchomione na wypadek zagrożenia pożarem. Ułatwia kontrolę i zarządzanie urządzeniami ppoż.

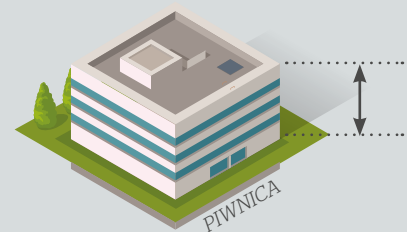


ela compil

Ela-compil sp. z o.o., ul. Szczepanowskiego 8, 60-541 Poznań, tel.: +48 61 869 38 50, -60 www.ela.pl

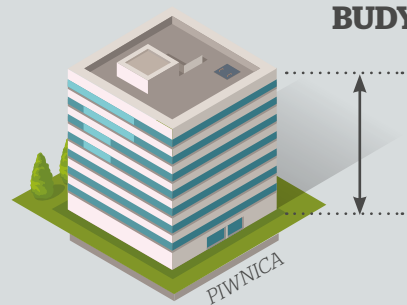
Bezpieczne obiekty biurowe

Rys. 1. Sposób klasyfikacji budynków w zależności od ich wysokości



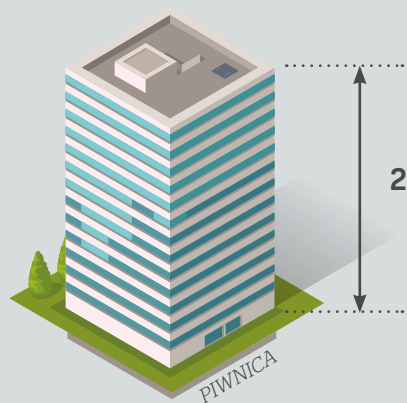
BUDYNKI NISKIE

$$H \leq 12 \text{ m}$$



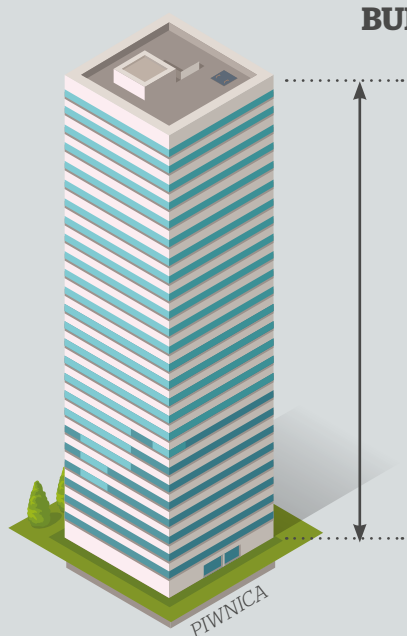
BUDYNKI ŚREDNIO WYSOKIE

$$12 \text{ m} < H \leq 25 \text{ m}$$



BUDYNKI WYSOKIE

$$25 \text{ m} < H \leq 55 \text{ m}$$



BUDYNKI WYSOKOŚCIOWE

$$H > 55 \text{ m}$$

ku, począwszy od miejsca usytuowania złącza, przeciwpożarowego wyłącznika prądu i rozdzielni elektrycznej, poprzez sposób prowadzenia i rodzaje kabli oraz ich mocowanie, skończywszy na innych elementach wpływających na ich działanie (rys. 2).

Niezależne zasilanie

Część urządzeń przeciwpożarowych powinna funkcjonować także wówczas, kiedy awarii ulega podstawowe źródło zasilania. Zasilanie urządzeń ppoż. można wówczas uzyskać, spełniając wymagania opisane wcześniej. Największym problemem jest zapewnienie dwóch źródeł zasilania. Przepisy RMI [1] nakazują stosowanie zasilania z dwóch niezależnych źródeł: podstawowego i rezerwowego. Definicja niezależnych źródeł zasilania znajduje się w normach dotyczących projektowania instalacji tryskaczowej oraz w normie PN-HD 60364-5-56.

Zgodnie z zapisami w dokumentach:

- PN-M-51540 *Ochrona przeciwpożarowa. Urządzenia tryskaczowe. Zasady projektowania i instalowania oraz odbioru i eksploatacji* (norma nieobowiązująca traktowana na zasadzie wiedzy technicznej),
- VDS CEA 4001:2003-01(01) za dwa „niezależne zasilania” w energię elektryczną uznaje się takie dwa „ciągi zasilania” (linie, aparaty rozdzielcze), które nie mają żadnego wspólnego elementu systemu rozdziału energii do poziomu napięcia rozdzielczego 110 kV.

Również w normie PN-HD 60364-5-56:2010+A1:2011 (PN-IEC 60364-5-56:1999) *Instalacje elektryczne w obiektach budowlanych – Dobór i montaż wyposażenia elektrycznego – Instalacje bezpieczeństwa* znajduje się definicja „niezależności zasilania”, jednak nieco inna od przywoływanej. Rozróżnia ona następujące źródła elektryczne do stosowania w instalacji bezpieczeństwa: – akumulatory, a także wszelkiego rodzaju zasilacze, – ogniwa galwaniczne (baterie), – zespoły prądotwórcze niezależne od zasilania podstawowego, – oddzielna linia sieci zasilającej, która skutecznie uniezależnia od podstawowej linii zasilającej.

Ponadto norma określa, że *oddzielne niezależne linie sieci zasilającej nie powinny służyć jako elektryczne źródła instalacji bezpieczeństwa, chyba że można zagwarantować (zapewnić – oryg.), że nie jest*

możliwe, aby te dwa źródła zasilania jednocześnie uległy uszkodzeniu.

Ważne!

Doboru poszczególnych źródeł dokonuje się na podstawie tego, co mają zasilać w przypadku zaniku napięcia zasilania podstawowego. Powyższe wymaganie nie dotyczy instalacji sygnalizacji pożarowej i dźwiękowych systemów ostrzegawczych – których zasady zasilania rezerwowego są określone w normie EN-54-4 oraz systemów oddymiania – których zasady zasilania rezerwowego są określone w normie serii EN-12101-10. Podobnie jest z instalacjami gaśniczymi.

Przytoczone akty prawne w sposób ogólny odnoszą się do kwestii związanych z zasilaniem, pozostawiając do decyzji projektantów i rzeczoznawców ds. zabezpieczeń ppoż. szeroki zakres urządzeń, które „logika” nakazuje zasilić z dwóch źródeł, ale przepisy nie wskazują wprost takiej potrzeby. Należą do nich:

- zasilanie napowietrzania w systemach oddymiania,
- zasilanie elementów przeciwpożarowych wyłączników prądu,
- przeciwpożarowe klapy odcinające EN 15650,

- klapy odcinające wentylacji pożarowej EN 12101-8,
- obwody bezpiecznego zasilania urządzeń.

Przy projektowaniu i wykonywaniu instalacji elektrycznych nie można zapomnieć również o bezpieczeństwie ludzi, a także konstrukcji obiektu i znajdujących się tam urządzeń. Często to właśnie one decydują o tym, jak szybko w krytycznym momencie zostanie wykryte zagrożenie i jak szybko się o nim dowiemy. Tylko właściwie zasilana, wykonana i eksploatowana instalacja zasilająca systemy bezpieczeństwa może to zapewnić. ■

- [1] Rozporządzenie Ministra Infrastruktury z 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz.U. nr 75/2002, poz. 690 z późn. zm.).
- [2] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 2 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. nr 109/2010, poz. 719).
- [3] Rozporządzenie MSWiA 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 z 2007 r., poz. 1002, zm.; Dz.U. nr 85 z 2010 r., poz. 553).
- [4] PN-B-02877-4 – instalacje grawitacyjne do odprowadzania dymu i ciepła.
- [5] Skiepkó E., Instalacje przeciwpożarowe, DW. MEDIUM 2010 r.
- [6] DIN 4102-12 Zachowanie się materiałów i elementów budowlanych pod działaniem ognia. Podtrzymanie funkcji urządzeń w czasie pożaru. Wymagania i badania.
- [7] PN-HD 60364-5-56:2013 – Instalacje elektryczne niskiego napięcia. Część 5-56: Dobór i montaż wyposażenia elektrycznego. Instalacje bezpieczeństwa.
- [8] PN-EN 12101-10:2007+AC:2007 – Systemy kontroli rozprzestrzeniania dymu i ciepła. Część 10: Zasilacze.
- [9] PN-EN 54-4:2001+A1:2004+A2:2007 Systemy sygnalizacji pożarowej. Część 4. Zasilacze.
- [10] Cygankiewicz D., Skiepkó E., Gwarantowane zasilanie urządzeń przeciwpożarowych napięciem przemiennym 230 V „Systemy Alarmowe” nr 4/2014.

ZETO-PROJEKT



BEZPIECZEŃSTWO POŻAROWE DO WYNAJĘCIA

Wbrew pozorom obiekty w fazie budowy są bardziej narażone na niebezpieczeństwo pożaru, niż obiekty oddane do użytku. Wychodząc naprzeciw potrzebom ochrony obiektów w fazie budowy, oferujemy wynajem bezprzewodowych Systemów Sygnalizacji Pożarowej. Dysponujemy pełną gamą urządzeń: czujki punktowe (optyczne, temperatury i multisensoryczne), ręczne ostrzegacze pożarowe, moduły wejścia/wyjścia, moduły linii bocznej oraz sygnalizatory. Brak okablowania ułatwia zmianę konfiguracji w zależności od postępu budowy.

Dla każdej budowy wykonujemy projekt SSP, a wypożyczone od nas urządzenia dostarczamy na budowę, montujemy i uruchamiamy. Proponowane urządzenia są produkowane przez firmę Advanced Electronics Ltd pod marką Axis EN, a przedstawicielem firmy na Polskę jest ZETO-PROJEKT.

P.U.I. ZETO-PROJEKT Sp. z o.o.,
55-075 Bielany Wrocławskie, ul. Kolejowa 20,
tel. 71 311 05 91, biuro@zeto-projekt.com.pl zeto-projekt.com.pl



dobre zaprojektowane BEZPIECZEŃSTWO

SYSTEMY SYGNALIZACJI POŻAROWEJ

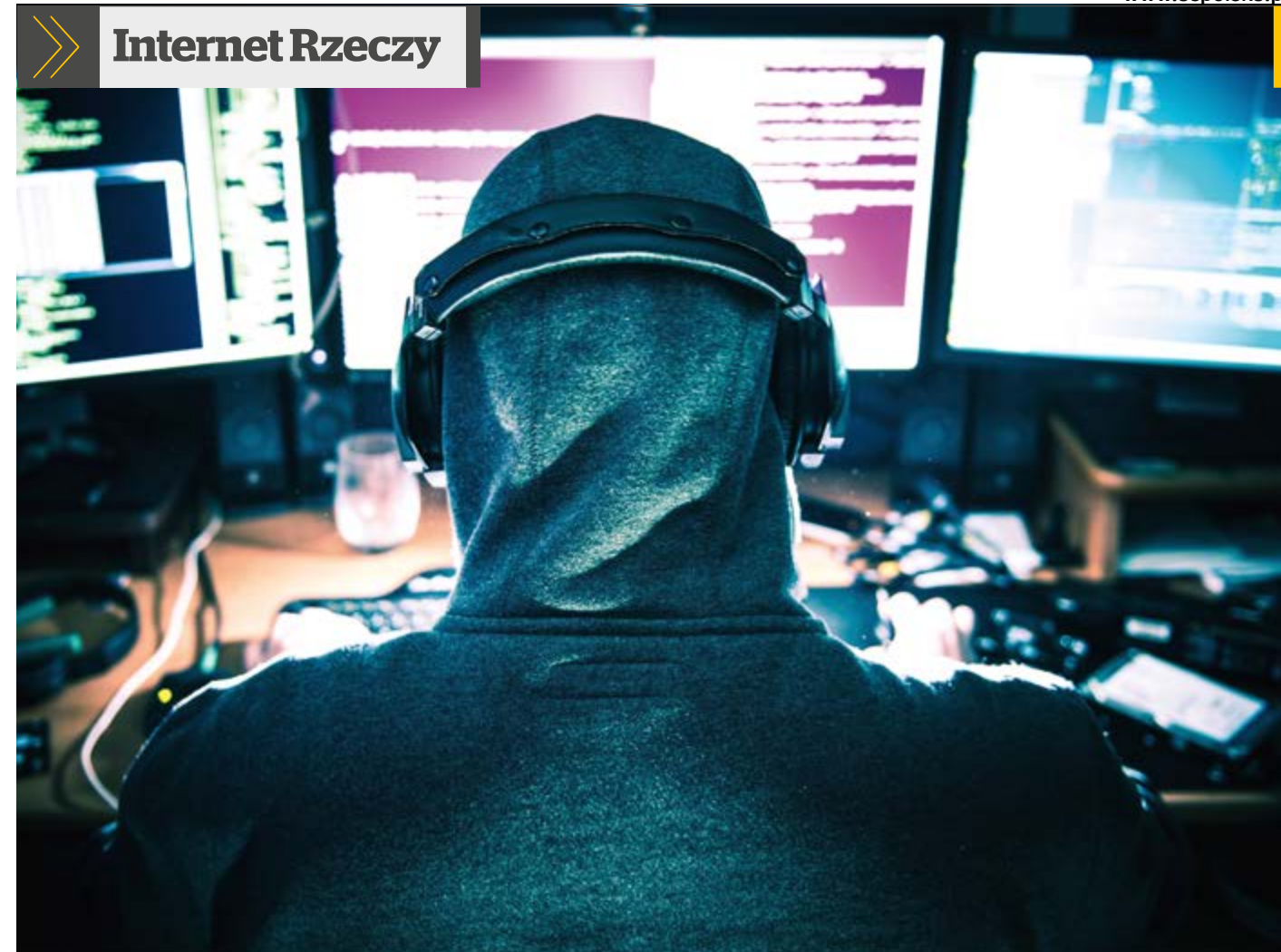
- innowacyjnie rozproszony POLON 6000
- interaktywny POLON 4000
- konwencjonalny IGNIS 1000/2000

oraz

UNIWERSALNE CENTRALE STERUJĄCE UCS 6000

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.

85-861 Bydgoszcz, ul. Glinki 155 | www.polon-alfa.pl



Bezpieczeństwo IoT - zagrożenia i przeciwdziałanie im

Typowe dla Internetu Rzeczy luki w zabezpieczeniach zostały wykorzystane w cyberataku typu DDoS, dokonanym 21 października 2016 r. w Stanach Zjednoczonych. W piątek o godzinie 7.00 czasu wschodniego popularne serwisy Twitter, Spotify, Netflix i Reddit przestały działać. Wszystkie z nich korzystały z usług DNS firmy Dyn.

SMAhome
a&s International

Jak poinformowali przedstawiciele firmy Dyn, do przeciążenia i zablokowania ich serwerów wykorzystano dziesiątki milionów urządzeń z całego świata. Według analityków ds. bezpieczeństwa hakerzy użyli urządzeń IoT, które przejęli i połączyli w rozbudowaną sieć botnet sterowaną przez *malware* Mirai. Powstanie i rozprzestrzenianie się złośliwego oprogramowania Mirai umożliwił niski poziom zabezpieczeń wielu urządzeń tworzących tzw. inteligentny dom. Poziom ochrony elementów IoT nierzadko jest bardzo słaby, co sprawia, że staje się łatwym celem hakerów. Wiele urządzeń korzysta np. z domyślnych nazw użytkowni-

ka i haseł. Gdy Mirai dotrze do ich danych uwierzytelniających, przejmuje je i włącza do botnetu.

Pokaźna liczba uczestniczących w ataku urządzeń pochodziła od chińskiego producenta XiongMai Technologies. Oferuje on komponenty IoT dostawcom, którzy instalują je we własnych produktach. Umożliwiło to przejście milionów urządzeń IoT korzystających z ustawień XiongMai, z kamerami dozоровymi, urządzeniami inteligentnego domu czy elektronicznymi nianiami włącznie.

Użytkownicy nie zauważyli, że ich sprzęt został wykorzystany jako broń w cyberataku. Ponieważ użytkownik końcowy zwykle nie jest w stanie zmienić danych uwierzytelniających, ochrona tego typu urządzeń jest trudna. Z informacji Flashpoint Security, opublikowanych 6 października 2016 r.,

wynika, że w ten sposób można było przejąć 515 tysięcy urządzeń. Serwery Dyn trzykrotnie zaatakowano metodą DDoS. Firma ta jest dostawcą domen dla setek dużych stron internetowych, dlatego popularne portale internetowe zostały do końca dnia wyłączone. Zmasowany atak wzbudził obawy o bezpieczeństwo urządzeń IoT. Tradycyjne cyberataki koncentrują się na stronie internetowej i mają na celu jej zablokowanie. W związku z tym, że liczba urządzeń IoT rośnie, w przyszłości takie ataki, jak ten na serwery Dyn, mogą zdarzać się częściej. Spowoduje to zagrożenie większej liczby sektorów, ponieważ każdy kolejny atak jest potężniejszy od poprzedniego.

PHILIPS HUE z protokołem ZIGBEE jako platforma dla hakerów

Inteligentne systemy oświetleniowe Philips Hue nie po raz pierwszy stały się celem cyberataków. Niedawno opublikowano wyniki badań, których autorzy włamali się do inteligentnych żarówek Philips Hue za pomocą protokołu Zigbee. Badania te dowodzą, że hakerzy mogą wykorzystać wady Philips Hue i protokół Zigbee do wgrania złośliwej aktualizacji *firmware'u*. Gdy program zainfekuje jedną żarówkę, automatycznie przeniesie się na kolejne. Po włamaniu się haker będzie mógł z przejeżdżającego w pobliżu samochodu albo z drona latającego na zewnątrz budynku włączyć i wyłączać światła. W opisywanym przypadku badacze kontrolowali działanie żarówek Philips Hue z odległości 400 m, gdy system był zainstalowany na zewnątrz budynku, i 70 m, gdy był ukryty wewnątrz. Włamań dokonywali z jadącego samochodu albo z drona wyposażonego w podzespoły dostępne na rynku. Badanie to ujawniło, że tego typu zagrożenie – gdy dotyczy urządzeń połączonych – wywołuje reakcję łańcuchową, momentalnie rozprzestrzenia się na duże obszary i infekuje kolejne elementy. Gdyby nastąpił atak na dużą skalę, haker mógłby sterować oświetleniem miasta, zainfekować je na stałe lub wykorzystać w zmasowanym ataku DDoS. Firma Philips w październiku minionego roku poinformowała o wprowadzeniu łaty, której instalację za pośrednictwem aplikacji Hue zaleca się wszystkim użytkownikom. Zdaniem specjalistów biorących udział w badaniu zapobiega ona

Poziom ochrony elementów IoT nierzadko jest bardzo słaby, co sprawia, że staje się łatwym celem hakerów. Wiele urządzeń korzysta np. z domyślnych nazw użytkownika i haseł.

jednak tylko włamaniom na odległość. Luka związana ze złośliwą aktualizacją nie została usunięta. Innymi słowy, hakerzy nadal są w stanie zainfekować urządzenia i wykorzystać je do ataków DDoS. W ostatnim raporcie Gartner Group podano, że do końca 2016 r. na świecie będzie ponad 6,4 miliarda urządzeń IoT, a w roku 2020 liczba ta ma wzrosnąć do 20,8 miliarda. Wraz z dynamicznie rosnącą liczbą urządzeń zwiększają się związane z nimi zagrożenia. Zabezpieczenie urządzeń IoT staje się koniecznością, by nasze domy nie zmieniły się w broń cyberprzestępców.

Luki w zabezpieczeniach IoT są bezwzględnie wykorzystywane do skoordynowanych międzyplatformowych ataków DDoS

Według firmy Symantec słabe zabezpieczenie wielu urządzeń IoT, zwłaszcza niezintegrowanych z komputerem PC, czyniło z nich łatwe cele. Z powodu wątpliwej struktury ich systemów operacyjnych i niskiej mocy obliczeniowej rzadko są wyposażane w programy chroniące. Złośliwe oprogramowanie wykorzystuje zarówno te luki, jak i łączność urządzeń z Internetem.

Do ataków zachęcają również hasła o niskiej sile. Z raportu firmy Symantec wynika, że większość użytkowników nie zmienia haseł domyślnych. Najczęściej spotykana nazwa użytkownika i hasło to „root”, „admin”, „123456” lub „test”, które zazwyczaj są ustawiane fabrycznie. W ten sposób użytkownicy nieświadomie sami narażają się na niebezpieczeństwo. Większość ataków nie jest jednak wymierzona przeciwko ofierze, twierdzą specjaliści z firmy Symantec. Ich główny cel to zazwyczaj przejęcie urządzenia i włączenie go do botnetu, aby wykonać atak typu rozproszona odmowa usługi (DDoS). Przejmując urządzenia IoT, hakerzy potrafią przeprowadzać ataki DDoS jednocześnie z wielu platform IoT, co dotychczas było rzadkością. Symantec przewiduje, że takie sytuacje będą się zdarzać coraz częściej, ponieważ liczba urządzeń podłączonych do sieci nieustannie rośnie.

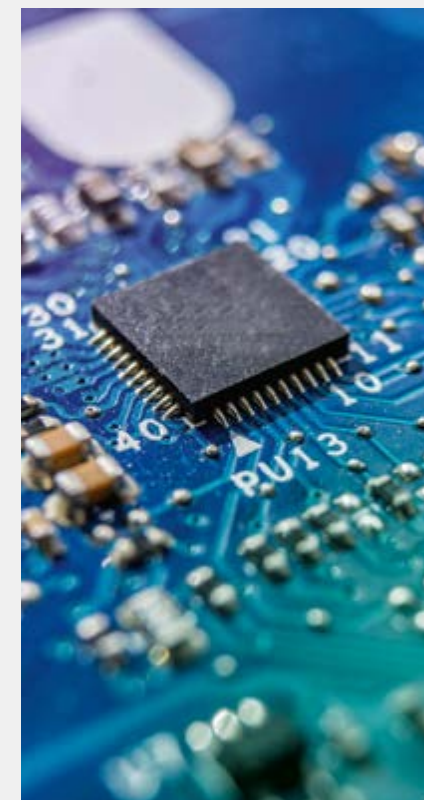
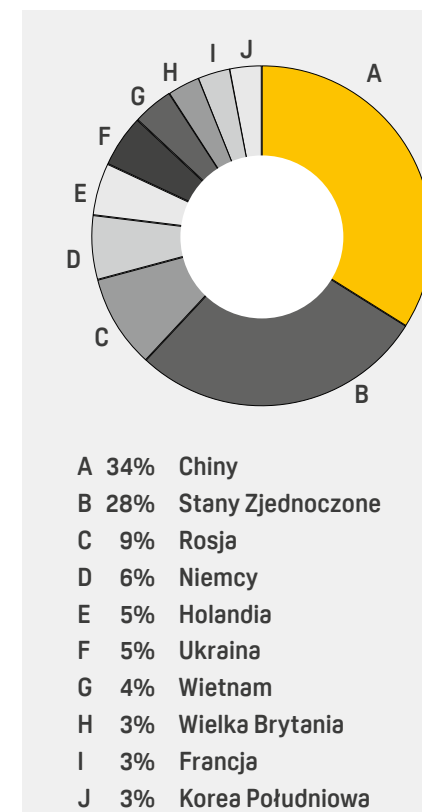
Rośnie też liczebność złośliwego oprogramowania zdolnego przenosić się między platformami. Hakerzy bez problemów tworzą wirusy malware na różne architektury. Jak podaje Symantec, najczęściej atakowane platformy to x86, ARM MIPS oraz MIPSSEL. Szybko włączane są kolejne, w związku z czym liczba potencjalnych celów rośnie i obejmuje serwery, routery, modemy, urządzenia NAS, systemy telewizji dozorowej oraz systemy ICS. Symantec zastosował system *honeypot*, który pozwolił na sporządzenie globalnego zestawienia *malware* atakującego IoT. Wynika z niego, że w 2016 r. najwięcej ataków na urządzenia IoT pochodziło z Chin (34%) i Stanów Zjednoczonych (28%). Następne były Rosja (9%), Niemcy (6%), Holandia (5%), Ukraina (5%), Wietnam (4%), Wielka Brytania (3%), Francja (3%) i Korea Południowa (3%).

NOWE WYMAGANIA BEZPIECZEŃSTWA CERTYFIKOWANYCH URZĄDZEŃ IOT STOWARZYSZENIA Z-WAVE

Z-Wave Alliance wprowadziło nowe wymagania bezpieczeństwa do swojego długoletniego programu certyfikowania interoperacyjności. Rada stowarzyszenia zdecydowała, że wszystkie produkty certyfikowane przez Z-Wave po 2 kwietnia 2017 r. muszą mieć zaimplementować Security framework S2. Dodanie tego zapisu

do programu certyfikującego nałoży na producentów konieczność wdrożenia najsilniejszego poziomu ochrony IoT w branży. Według stowarzyszenia S2 zapewnia najbardziej zaawansowany na rynku poziom bezpieczeństwa urządzeń i sterowników inteligentnego domu, bram sieciowych i hubów.

Źródła ataków na IoT



Giganci technologiczni zalecają poprawę bezpieczeństwa IoT

Techniczna grupa doradcza ds. Internetu szerokopasmowego (BITAG – Broadband Internet Technical Advisory Group) wspierana przez takich gigantów technologicznych, jak Google, AT&T, Cisco, T-Mobile, Intel i Microsoft opublikowała w listopadzie 2016 r. raport na temat bezpieczeństwa i prywatności IoT. Zawierał on obserwacje dotyczące luk w zabezpieczeniach urządzeń IoT. Przedstawiał także sugestie dotyczące poprawy bezpieczeństwa i zapobiegania włamaniom za pośrednictwem *malware*. Doradcy BITAG wskazali, że przestarzałe oprogramowanie, nieszyfrowana komunikacja, brak uwierzytelniania i wzajemnych autoryzacji, a także nieodizolowanie sieci to podstawowe niedociągnięcia w bezpieczeństwie IoT. W związku z tym, że aktualizacja oprogramowania, która mogłaby usunąć krytyczne luki bezpieczeństwa, nie jest czynnością prostą, a konsumenci nie są skłonni do aktualizowania swoich urządzeń, problemy zabezpieczeń i prywatności nie znikają. Według BITAG, aby uniknąć opisanych sytuacji, użytkownicy powinni korzystać z urządzeń IoT posiadających najnowsze

oprogramowanie, używać silnych metod uwierzytelniania, które nie korzystają z łatwych do odgadnięcia nazw użytkowników i haseł, a także przestrzegać najlepszych praktyk bezpieczeństwa i szyfrowania. Co ważne, dostawcy urządzeń IoT powinni stosować politykę prywatności, której zasady są dla użytkownika łatwe do odszukania i zrozumiały. Branża IoT natomiast powinna rozważyć wdrożenie całościowego programu ochrony przed cyberprzestępczością. BITAG, jako organizacja non profit, nie ma mocy kształtowania obowiązujących przepisów. Niemniej raport pokazał, że do bezpieczeństwa IoT przywiązuje się coraz większą wagę, a zarazem przekazał impuls

By korzystać z urządzeń IoT, trzeba mieć najnowsze oprogramowanie, używać silnych metod uwierzytelniania i przestrzegać najlepszych praktyk bezpieczeństwa i szyfrowania.

do działania rządom i urzędowi, gdyż liczba urządzeń IoT stale będzie się zwiększać.

Wytyczne dla producentów IoT

Departament Bezpieczeństwa Krajowego USA (DHS – Department of Homeland Security) wydał publikację *Strategic Principles for Securing the Internet of Things (IoT), Version 1.0* (Strategiczne zasady zapewnienia bezpieczeństwa w Internecie Rzeczy – IoT, wersja 1.0), która może stanowić zestaw wytycznych dla producentów sektora IoT. Nie definiują one zasad korzystania z urządzeń, zwracają raczej uwagę, by to projektanci i producenci kierowali się względami bezpieczeństwa i przestrzegali zalecanych procedur. Dokument ten miał na celu uświadomienie producentom zagrożeń i ochronę przed nimi. Publikacja DHS obejmuje włączenie w fazę projektowania zagadnień bezpieczeństwa, umożliwienie wprowadzania aktualizacji zabezpieczeń i zarządzania lukami, korzystanie ze sprawdzonych najlepszych praktyk bezpieczeństwa, nadawanie priorytetów zabezpieczeniom w zależności od ryzyka i propagowanie przejrzystości w kontaktach deweloperów z producentami. Zwraca też uwagę na zachowanie ostrożności i celowości przez klientów IoT przy włączaniu do sieci.

W kluczowych dla życia czynnościach w coraz większym stopniu polegamy na sieciach funkcjonalnych, od autonomicznych samochodów po systemy dostarczające wodę i prąd do naszych domów. Bezpieczeństwo Internetu Rzeczy stało się sprawą bezpieczeństwa kraju – podkreślił w opublikowanym oświadczeniu Jeh Johnson, sekretarz bezpieczeństwa krajowego. – *Wydany dzisiaj przewodnik stanowi ważny krok w dostarczaniu firmom informacji, aby ich decyzje wpływające na bezpieczeństwo były oparte na wiedzy.*

Po ataku DDoS Federalna Komisja Łączności (Federal Communications Commission) nie wydała nowych zaleceń, oświadczając, że zarządzenie *Open Internet Order* bez dodatkowych przepisów zapewnia usługodawcom internetowym wystarczające pole do działań chroniących sieci przed niezabezpieczonymi podłączonymi urządzeniami.

Amerykański rynek IoT jest częścią globalnego ekosystemu, toteż wszelkie przepisy krajowe będą w dużym stopniu oddziaływać na inne kraje i standardy międzynarodowe. ■

Tylko dla a&s

INTERNET RZECZY i jego konsekwencje dla branży

zabezpieczeń technicznych

Rozmowa z
Perem Björkdahlem,
przewodniczącym komitetu
wykonawczego ONVIF

Pierwsze pytanie nasuwa się samo: czym jest Internet Rzeczy?

Paradoksalnie, dyskusje na temat technologii Internetu Rzeczy (IoT) skupiają się zazwyczaj na poszukiwaniu odpowiedzi na pytanie, co IoT może oznaczać dla przyszłych technologii, rozwoju urządzeń i ich sprzedaży – bez jej faktycznego zdefiniowania. Jedni twierdzą, że Internet Rzeczy jest już obecny w naszym życiu w postaci licznych zintegrowanych ze sobą aplikacji mobilnych, sieciowych i internetowych. Inni z kolei uważają, że o pojęciu IoT można mówić tylko wtedy, gdy urządzenia są połączone z innymi urządzeniami. W ogólnym rozumieniu IoT oznacza, że wiele różnych przedmiotów i systemów jest ze sobą połączonych i zarządzanych przez pojedynczy interfejs użytkownika. Urządzenia działające w ramach IoT korzystają zazwyczaj ze wspólnej infrastruktury, którą wykorzystują do komunikowania się. Zaletą koncepcji IoT jest jednocześnie, w czasie rzeczywistym, dostęp do danych z różnych urządzeń i/lub systemów za pomocą jednego interfejsu

użytkownika. Oprócz monitorowania w czasie rzeczywistym oprogramowanie IoT umożliwia analizę wielu strumieni danych do celów operacyjnych i analityki biznesowej.

Czy można wskazać istotne obawy związane z Internetem Rzeczy?

Generalnie obawy dotyczą bezpieczeństwa informacji, które wymieniają pomiędzy sobą urządzenia i sieci – właśnie wymiana danych stanowi sedno idei IoT. Zgodnie z koncepcją Internet Rzeczy łączy ze sobą zdalnie wiele urządzeń i systemów. Powstają wtedy nowe punkty dostępu, które mogą nie mieć odpowiedniej ochrony. Skoro informacja wychodzi poza obręb ograniczonej bezpiecznej sieci, zabezpieczenie integralności danych staje się wielkim wyzwaniem. Integralność to brak niekontrolowanych zmian. Istotne obawy sektora technologicznego dotyczą też ryzyka stosowania słabych zabezpieczeń urządzeń IoT i danych wrażliwych, utraty kontroli nad urządzeniami czy naruszenia prywatności.

Jakie stanowisko w tej kwestii zajmuje branża zabezpieczeń technicznych? Czy podziela obawy dotyczące bezpieczeństwa IoT?

W przypadku branży zabezpieczeń technicznych temat IoT jest postrzegany nie tylko przez pryzmat bezpieczeństwa informatycznego sieci IT. Podstawowym zadaniem naszej branży jest zapewnianie bezpieczeństwa ludziom, obiektom oraz mieniu. Zatem wyposażając nasze produkty w możliwości komunikacji w ramach IoT, musimy zachować szczególną ostrożność, by utrzymać wysokie branżowe standardy zabezpieczeń. Integracja urządzeń i systemów security nie może i nie powinna stanowić kompromisu ze względu na IoT. Ponieważ intensywność wymiany danych między urządzeniami a klientami rośnie, zabezpieczenie integralności danych staje się ważniejsze niż dotychczas.

Dlaczego standardy, takie jak ONVIF, są ważne dla rozwoju i przyszłości IoT?

Większość przedstawicieli świata technologii IT uważa – podobnie jak ONVIF – że rozwój IoT powinien opierać się na odpowiednich standardach. Internet Rzeczy bazuje na przyjęciu zdefiniowanej i uniwersalnej zasady współdzielenia danych w komunikacji sieciowej. Aby IoT mógł działać, różne czujniki i źródła danych muszą być w stanie komunikować się z serwerem lub oprogramowaniem. Specyfikacje ONVIF spełniają tę samą rolę odnośnie do sieciowych urządzeń zabezpieczeń technicznych – definiują standardy komunikacji. To zrozumiałe, że standardy ONVIF np. ułatwiają komunikację pomiędzy kamerami różnych producentów za pomocą kompatybilnego oprogramowania zarządzającego VMS, PSIM lub innego sieciowego (IP) systemu zarządzania. To tak, jakby ONVIF i inne standardy ustanawiały wspólny język porozumiewania się dla różnych krajów.

Co ważne, specyfikacje ONVIF dotyczące systemów dozoru wizyjnego i kontroli dostępu zo-

stały przyjęte przez IEC. Oznacza to, że specyfikacje ONVIF stają się de facto standardami w przypadku tych systemów takich organizacji normalizacyjnych, jak IEC. Jeśli zatem IoT zostanie w danej lokalizacji wdrożony zgodnie z wymaganiami IEC i będzie zawierać urządzenia telewizji dozorowej oraz kontroli dostępu, będzie korzystał ze specyfikacji ONVIF.

Jakie konkretne wyzwania związane z IoT czekają branżę?

Największym wyzwaniem jest zapewnienie wysokiej funkcjonalności i łatwości obsługi przy zachowaniu odpowiedniego zabezpieczenia integralności danych. Przypomina to spacer po linie. Producenci i integratorzy systemów coraz więcej uwagi poświęcają problemom bezpieczeństwa, ale nadal jest mnóstwo pracy do wykonania. Musimy jeszcze lepiej chronić dostęp do sieciowych urządzeń, takich jak kamery czy kontrolery wejść, a to wymaga poprawy zabezpieczenia całej sieci oraz urządzeń. Pytaniem nie jest, czy Internet Rzeczy zmaterializuje się właśnie w takim kontekście, ponieważ to już się dokonało. Branża zabezpieczeń technicznych musi zwiększyć tempo rozwoju środków ochrony oraz zwrócić uwagę na poprawę edukacji użytkowni-

Korzystając z IoT, musimy zachować szczególną ostrożność, by utrzymać wysokie standardy zabezpieczeń. Integracja urządzeń i systemów security nie może i nie powinna stanowić kompromisu ze względu na IoT.

ków końcowych i pracowników działów IT w zakresie bezpieczeństwa systemów zabezpieczeń technicznych w ich codziennej pracy.

Czy ONVIF pracuje nad standardem IoT?

Nad standardem IoT pracują już inne organizacje normalizacyjne. IEEE – największe na świecie stowarzyszenie profesjonalistów z różnych dziedzin technologii – rozwija standardy IoT w odniesieniu do kilku branż technologicznych. Złożona z przedstawicieli różnych sektorów grupa robocza IEEE o nazwie P2413 jest odpowiedzialna za ograniczenie rozdrobnienia branżowego poprzez rozwój wspólnego szkieletu i oparcie przyszłych działań na identyfikowaniu cech wspólnych pomiędzy segmentami IoT. Takie porozumienia, jak Open Internet Consortium (OIC), grupy THREAD Group, ZigBee i Z-Wave opracowują specyfikacje do certyfikacji, biorąc pod uwagę także standardy IoT. Sukces IoT jest oparty na wspólnym dążeniu producentów i działów rozwoju do opracowania standardów bazowych, które pozwolą systemom zabezpieczeń technicznych współpracować z innymi urządzeniami zabezpieczeń, a także z urządzeniami spoza obszaru security. Zapewniona w ten sposób współpraca pomiędzy wieloma systemami stanowi fundament IoT.

ONVIF przyczynia się do realizacji tego celu, zwiększając w strefie zabezpieczeń technicznych zgodność wśród sieciowych (IP) urządzeń zabezpieczeń technicznych, co może być istotne dla rynku IoT i jego rozwoju. Moim zdaniem kolejny etap działań ONVIF może dotyczyć problemu wzajemnej kompatybilności pomiędzy systemami zarządzania strumieniami wideo. Stanowi to zaledwie element bardziej złożonego problemu IoT. ■



Per Björkdahl

Od 2012 r. jest przewodniczącym Komitetu Sterującego ONVIF. Uczestniczy w inicjatywach ONVIF i reprezentuje organizację na targach i innych wydarzeniach branżowych. Od ponad 25 lat pracuje w branży zabezpieczeń technicznych, obecnie jako dyrektor ds. rozwoju biznesu Axis Communications.

Internet Rzeczy

Rok 2016 był rekordowy pod względem liczby ataków na urządzenia Internetu Rzeczy. Routery znalazły się na celowniku cyberprzestępców ponad 25 miliardów razy. Kolejne miejsca zajmują sieciowe rejestratory wizyjne i kamery. Przyczyną są poważne luki w zabezpieczeniach tych urządzeń, które do dziś nie zostały naprawione.

Routery i sieciowy sprzęt wideo

najczęściej atakowanymi urządzeniami IoT

Internet Rzeczy jest dziś jednym z obszarów najbardziej narażonych na cyberzagrożenia. Producenci tego typu rozwiązań często nie dbają o odpowiednie zabezpieczenia, cyberprzestępcy natomiast bezlitośnie wykorzystują każdą wykrytą podatność urządzeń działających w ramach IoT. Niestety producenci naprawiają je zbyt późno, w związku z czym hakerzy mają sporo czasu na działania. Nierzadko też opracowanie i dostarczenie łat jest trudne, ponieważ urządzenia te nie mają automatycznych mechanizmów aktualizacji *firmware'u*.

Fale nowych ataków na IoT nie ustają. W zeszłym roku botnet o nazwie Mirai wykorzystał urządzenia IoT do przeprowadzenia jednego z największych w historii ataków DDoS. Ataki na sprzęt będący elementem systemów medycznych, przemysłowych czy infrastruktury krytycznej mają poważne konsekwencje. Zainfekowany Internet Rzeczy może zostać użyty do szpiegowania, wyłudzenia okupów *ransomware* czy też posłużyć jako furtka do głębiej osadzonych zasobów sieciowych.

Domowe routery najczęstszym celem

Analitycy z zespołu FortiGuard Labs firmy Fortinet zebrali dane dotyczące ataków na Internet Rzeczy z 2016 r. z podziałem na określone kategorie urządzeń.

Jak się okazało, w ubiegłym roku nastąpił gwałtowny wzrost liczby ataków na routery stosowane zazwyczaj w domowych sieciach. Odnotowano ich ponad 25 mld w porównaniu do 820 tys. w 2015 r. Tak ogromna liczba ataków wiązała się z luką odkrytą w routerach Netco-

re/Netis polegającą na zamieszczeniu hasła dostępu do panelu zarządzania routerem w kodzie oprogramowania. Na razie nie opublikowano łatki usuwającej ten błąd, toteż można się spodziewać dalszych zmasowanych ataków na te urządzenia. W Polsce routery tego producenta nie należą do najpopularniejszych. Z ogólnej liczby 25 mld ataków w naszym kraju zano- towano około 90 tys. Przejęcie dostępu do zarządzania routerem pozwala na przechwycenie ruchu pochodzącego ze wszystkich urządzeń podłączonych do domowej sieci.

Hakerzy-podglądacze

Drugą najczęściej atakowaną w 2016 r. kategorią urządzeń IoT były sieciowe rejestratory wizyjne (DVR/NVR). Rejestrują one nagrania z kamer IP systemu monitoringu wizyjnego. Analitycy Fortinet wykryli w minionym roku 1,5 mln ataków na tego typu urządzenia. W Polsce odnotowano ich około 1800. Za zdecydowaną większość naruszeń stoi odkryta w marcu ubiegłego roku podatność na zagrożenia dotycząca urządzeń 79 producentów rejestratorów. Również ten *backdoor* nie został do dziś naprawiony.

Na trzecim miejscu w zestawieniu znalazły się kamery IP. Za większość ubiegłorocznych ataków na te urządzenia odpowiada *backdoor* odkryty w kamerach firmy LinkSys. Należy jednak zwrócić uwagę na fakt, że w porównaniu do 2015 r. liczba ataków na kamery sieciowe spadła 10-krotnie. Można to tłumaczyć tym, iż coraz częściej kamery wykorzystują do zdalnego dozoru rozwiązania chmurowe lub P2P, w którym komunikacja jest szyfrowana. Najbardziej narażone na ataki są kameryki

Zestawienie najczęściej atakowanych urządzeń IoT w 2016 r.

Routery	25 172 757 940
Kamery IP	36 790
Systemy telefoniczne	19 289
NAS	29 993
DVR/NVR	1 514 484
Smart TV	1 354
Drukarki	16

Porównanie liczby ataków na IoT w 2015r. i 2016 r.

	2015	2016
Routery	821 504	25 172 757 940
Kamery IP	363 550	36 790
Systemy telefoniczne	117 156	19 289
NAS	43 823	29 993
DVR/NVR	749	1 514 484
Smart TV	520	1 354
Drukarki	28	16

Zainfekowany Internet Rzeczy może zostać użyty do szpiegowania, wyłudzenia okupów *ransomware* czy też posłużyć jako furtka do głębiej osadzonych zasobów sieciowych.

internetowe, nad którymi kontrola odbywa się bezpośrednio przez Internet. Na kolejnych miejscach zestawienia przygotowanego przez Fortinet znalazły się rozwiązania NAS, systemy telefoniczne (VoIP), telewizory Smart TV i drukarki sieciowe.

Jak bezpiecznie korzystać z Internetu Rzeczy?

Dobierając urządzenia powiązane i działające w ramach Internetu Rzeczy, szczególną uwagę należy zwrócić na to, jak do problemu bezpieczeństwa podchodzi ich producent – czy stosuje jakiegokolwiek mechanizmy ochronne i jak wygląda kwestia aktualizacji *firmware'u*. Trzeba również sprawdzić, czy dany sprzęt nie jest obciążony rozpoznaną luką bezpieczeństwa. Wprowadzając rozwiązania Internetu Rzeczy do sieci firmowej, najlepiej skonsultować się ze specjalistą i upewnić, czy stosowany system bezpieczeństwa IT zapewnia skuteczną ochronę. Może się bowiem okazać, że system będzie wymagał aktualizacji. ■

INFORMACJE O FIRMIE FORTINET

Fortinet oferuje rozwiązania do ochrony firmom, dostawcom usług i podmiotom administracji publicznej na całym świecie. Świadczy pełną i inteligentną ochronę w dobie wzrostu zagrożeń i rosnących oczekiwań wobec wydajności rozszerzających się sieci.

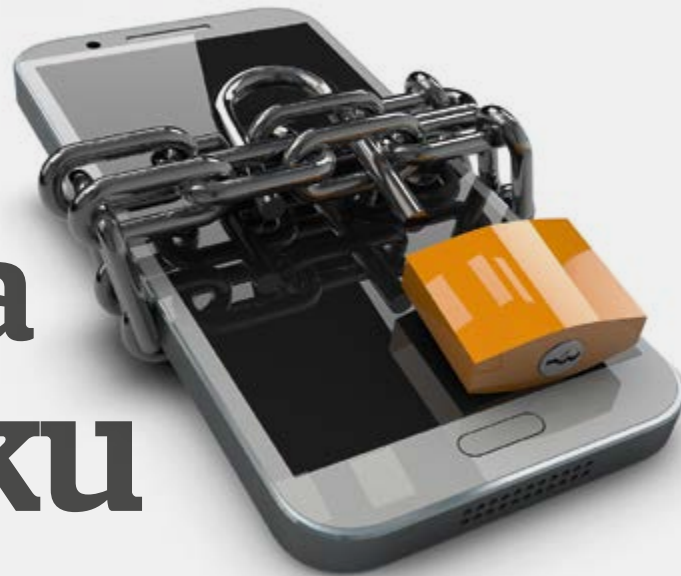
Architektura Fortinet Security Fabric zapewnia skuteczne zabezpieczenia spełniające kluczowe wyzwania bezpieczeństwa środowisk sieciowych, aplikacji, chmury oraz urządzeń mobilnych. Zabezpieczenie swoich firm powierzyło Fortinetowi ponad 300 tys. klientów na całym świecie.



CYBERBEZPIECZEŃSTWO

RAPORT CERT ORANGE POLSKA

Wyzwania i zagrożenia w 2017 roku



Na podstawie raportu
CERT Orange 2016

W tym roku nie można oczekiwać zmniejszenia liczby ataków *malware*, *ransomware* czy *phishingu*. Mimo zakrojonych na szeroką skalę prób podniesienia świadomości zagrożeń internetowych, wielu internautów wciąż pozwala się oszukać, otwierając podejrzaną wyglądające załączniki czy klikając linki w e-mailach podszywających się pod znane marki.

Odwagi hakerom dodają niska skuteczność wykrywania sprawców oraz mała liczba zgłoszeń do organów ścigania. Ich działalność ułatwia również to, że nie muszą już pisać złośliwego oprogramowania od podstaw i planować kampanii. *Malware* i narzędzia do jego dystrybucji można kupić i skonfigurować na własne potrzeby.

W ubiegłym roku Orange Polska przewidywał też dynamiczny wzrost liczby ataków za pośrednictwem Internetu Rzeczy, czyli na połączone z siecią urządzenia niebędące komputerami czy smartfonami. Ta diagnoza była trafna. Do odnotowanego w 2016 r. największego w historii ataku DDoS (prawie 1 terabit na sekundę) wykorzystano głównie zainfekowane wcześniej kamery internetowe oraz rejestratory obrazu. Taki atak zablokowałby w tym samym czasie dostęp do bankowości elektronicznej przeszło tysiąca dużych banków!

W roku 2017 nastąpi dalszy wzrost znaczenia ataków z wykorzystaniem IoT. Producenci coraz większej liczby urządzeń implementują w nich funkcjonalności umożliwiające zdalne zarządzanie, zbyt często wprowadzając je na rynek bez przeprowadzenia testów bezpieczeństwa. W efekcie rozwiązania te stają się łatwym

celem dla atakujących, zwłaszcza przy braku zaleceń zmiany domyślnych haseł, które nie stanowią tajemnicy.

Ataki w mediach społecznościowych

Nie zanosi się też na to, by przestępcy zrezygnowali z najpopularniejszej metody rozpowszechniania złośliwego oprogramowania, czyli za pośrednictwem mediów społecznościowych. Tam rządzą i będzie rządzić socjotechnika. Jeszcze długo będziemy otrzymywali dziwnie brzmiące wiadomości w Messengerze albo np. znajomy polubi jakiś dziwny status. W takich przypadkach – gdy nie zachowamy czujności – nasze konto przestanie należeć do nas.

W ostatnich miesiącach coraz częściej na Facebooku zaczęły się pojawiać fanpage z fałszywymi konkursami, wykorzystującymi znane marki lub osoby. Niestety okazały się wyjątkowo skuteczne. Ich działanie polega na utworzeniu fałszywego profilu z konkursem firmowanym przez znaną markę lub osobę. Nagrodą są rzekomo bezpłatne zakupy czy nawet wysokiej klasy samochód. Wystarczy polubić post, udostępnić go na swoim profilu i zamieścić pod nim komentarz o wskazanej treści. Pozwala to przestępcom dotrzeć

do kolejnych osób, tj. znajomych ofiar. Następnie na profilu pojawia się informacja, że w celu sprawdzenia listy zwycięzców należy wypełnić udostępniony formularz i potwierdzić tożsamość numerem PIN otrzymanym w SMS-ie weryfikującym numer telefonu „zwycięzcy”. Jak można się domyślić, nie potwierdzamy tożsamości, ale subskrypcję wysokopłatnej usługi Premium SMS. Za zbędne wiadomości można zapłacić nawet do 30 zł za każdą! Paradoksalnie przestępcy postępują zgodnie z prawem, pod formularzem bowiem jest umieszczony link (drobnym drukiem) prowadzący do regulaminu, który opisuje usługę i koszty. Pytanie jednak, jak wiele osób czyta regulaminy? O wysokich opłatach ofiary dowiadują się dopiero z rachunku telefonicznego.

Warto także pamiętać o świadomym udostępnianiu informacji o sobie w różnych serwisach społecznościowych, w szczególności odnoszących się do pracy zawodowej. Wiele wskazuje na to, że 2017 r. okaże się rokiem *phishingu* przygotowywanego pod kątem konkretnych grup zawodowych, co może znacznie wpłynąć na jego skuteczność. Księgowy z większym prawdopodobieństwem otworzy odpowiednio nazwany plik Excela, a jeśli przestępca usiłujący zaatakować naszą firmę znajdzie wcześniej na Facebooku czy LinkedIn odpowiednich kandydatów, szanse jego powodzenia wyraźnie wzrosną.

Co robić, by się bronić?

Bezpieczeństwo teleinformatyczne wymaga ochrony proaktywnej. Reagowanie na zagrożenia, które i tak już wyrządziły szkodę, pozwoli jedynie zmniejszyć skalę strat. Lepiej więc zapobiegać, niż leczyć. Odwołując się do branży transportowej, nie trzeba kupować samochodu, żeby przemieścić się z punktu A do B. Podobnie jest z rozwiązaniami bezpieczeństwa IT. Można je kupić jako usługę, zamiast nabywać na własność. To wariant znacznie tańszy, a dzięki temu można korzystać w tym samym czasie z ochrony przed kilkoma zagrożeniami, nie wydając całego budżetu na jedną platformę. Oczywiście wszystko zależy od profilu firmy i jej potrzeb, ale większość przedsiębiorstw, decydując się na inwestycje w rozwiązania cyberbezpieczeństwa,

Do odnotowanego w 2016 r. największego w historii ataku DDoS (prawie 1 terabit na sekundę) wykorzystano głównie zainfekowane wcześniej kamery internetowe i rejestratory obrazu.

dużą wagę przywiązuje do kosztów. To zupełnie naturalne, tym bardziej że rozwiązania tej klasy to forma ubezpieczenia, i to przed zjawiskiem wirtualnym. Najczęściej stosowaną ochroną danych w polskich firmach jest oprogramowanie antywirusowe. Jest podstawą podstaw, która chroni biznes przynajmniej przed częścią zagrożeń z sieci. Jednak antywirus to za mało. Inną kwestią jest samokontrola. Z raportu Integrated Solutions „Cyberzagrożenia według polskich firm” wynika, że nieprzestrzeganie przez pracowników procedur bezpieczeństwa jest jedną z głównych przyczyn incydentów. Oprócz budowania świadomości wśród personelu firmy powinny pamiętać o bieżących aktualizacjach rozwiązań. W przeciwnym razie istnieje ryzyko, że korzystając ze „starego” oprogramowania, padniemy ofiarą ataku.

Poziom bezpieczeństwa polskiej cyberprzestrzeni

CZYM GROZI FIRMIE IGNOROWANIE CYBERBEZPIECZEŃSTWA?

Wśród ekspertów od bezpieczeństwa IT panuje przekonanie, że nie ma bezpiecznych sieci, są tylko źle zeskanowane przez włamywacza. Inni z kolei sugerują, że kluczowe pytanie nie powinno dotyczyć tego, „czy mnie zaatakują?” ani „kiedy mnie zaatakują?”, ale „kiedy zostałem zaatakowany?”. W czasach, gdy dla większości firm normą jest bycie online, niezależnie czy wykorzystują ten kanał do komunikacji z klientami, partnerami, czy tylko wewnątrz organizacji, ignorowanie cyberzagrożeń jest swego rodzaju prośbą o biznesową tragedię. I nie chodzi tu

wyłącznie o ataki celowe, gdzie cyberprzestępca skrupulatnie wybiera konkretną ofiarę. Włamywacze skanują sieć regularnie, w sposób automatyczny, szukając luk w zabezpieczeniach i wykorzystując je do swoich celów. Konsekwencje natomiast kosztują. Trudno oszacować wartość strat, bo firmy niechętnie przyznają się do tego, że z ich kont bankowych wyprowadzono pieniądze lub straciły cenne dane na skutek ataku.

Sektor MŚP w Polsce dostrzega potrzebę podjęcia inicjatyw, które ochronią ich działalność przed zagrożeniami z Internetu. 51 proc. określa cyberbezpieczeństwo jako bardzo ważne dla ich firmy, 34 proc. uznaje je za kluczowe. To pokazuje systematyczny wzrost świadomości polskich przedsiębiorstw na temat konsekwencji potencjalnych ataków. Wśród zagrożeń, które w opinii małych i średnich firm mogą spowodować największe straty finansowe, znalazły się *malware* (złośliwe oprogramowanie) oraz ataki odmowy dostępu (DDoS). Najwięcej, bo aż 66 proc. wskazań, dotyczyło złośliwego oprogramowania. Co więcej, właśnie ataki z wykorzystaniem *malware* zostały określone także jako najtrudniejsze do wykrycia.

Te dane wynikają ze specyfiki złośliwego kodu, który jest coraz bardziej skomplikowany, a wobec takich zagrożeń, jak APT czy *zero-day* oprogramowanie antywirusowe jest bezbronny. Są to ataki, które nie mają przypisanych sygnatur i nie figurują w bazach producentów antywirusów. Bez specjalistycznej ochrony mogą bezkarnie wykradać dane lub pieniądze firm nawet przez kilka lat.

Dynamika zmian w cyberprzestrzeni, rozwijające się złośliwe oprogramowanie i zmienne cele przestępców powodują, że ocena poziomu zagrożeń i prognozowanie zmian stanowią duże wyzwanie. Ubiegły rok jest doskonałym przykładem dynamiki zmian wektorów ataku i metod infekcji. Prezentowane dane pochodzą z systemów Orange Polska analizujących ruch sieciowy pod względem złośliwego oprogramowania, z próbką odpowiadającą ok. 1% ruchu użytkowników usług szerokopasmowego dostępu do Internetu.

MALWARE W POLSCE

Zidentyfikowane ataki można podzielić na trzy typy:

- *malware object* – dostarczenie do stacji końcowej złośliwego oprogramowania,
 - *web infection* – infekcja w czasie rzeczywistym i instalacja złośliwego oprogramowania na urządzeniu ofiary,
 - *malware callback* – potwierdzenie skutecznego uruchomienia złośliwego kodu poprzez zestawienie komunikacji sieciowej z serwerem zdalnego zarządzania (w celu pobrania dalszych instrukcji bądź przekazania wykradzionych informacji).
- Sposobów na dostarczenie złośliwego oprogramowania na stacje robocze jest wiele. Coraz więcej z nich unika wykrycia w warstwie sieciowej, wykorzystując mechanizm szyfrowania komunikacji TCP. Zdecydowaną większość zdarzeń stanowi komunikacja zwrotna do centrum sterowania, co wynika z mechanizmów działania współczesnych infekcji, a także podkreśla niski stan bezpieczeństwa użytkowników Internetu. Przeważająca część złośliwego oprogramowania po uruchomieniu na stacji użytkownika w drugiej fazie działania będzie infekować urządzenia.

Ataki na bankowość elektroniczną

Sektor finansowy od lat znajduje się w centrum zainteresowania cyberprzestępców. Rok 2016 przyniósł falę ataków na systemy bankowości internetowej. Były one wycelowane zarówno w infrastrukturę techniczną, jak i bezpośrednio w klientów banków. Dowiodły, że linia kontaktu bank-klient – coraz częściej to e-mail lub SMS – jest bardzo podatna na zagrożenia i dlatego skutecznie wykorzystywana. Wśród metod dominują ataki *phishingowe*, w których wyniku klienci są narażani na wyłudzenia danych logowania i numerów kart płatniczych.

Co gorsza, treść wiadomości e-mailowych jest coraz lepiej dostosowana pod konkretne banki i klientów, a fałszywe serwisy bankowe są dopracowane i wiarygodnie imitują prawdziwe. Jedną z kluczowych kwestii nadal pozostaje udoskonalenie zabezpieczeń i monitorowanie styku usług bankowych i telekomunikacyjnych wykorzystywanych w komunikacji banku z klientem. W ubiegłym roku instytucji z sektora bankowego nie

ATAKI, PRZED KTÓRYMI CERT ORANGE POLSKA CHRONIŁ UŻYTKOWNIKÓW SWOJEJ SIECI

- ataki *phishingowe* związane z programem 500+ (podszywające się pod portale umożliwiające złożenie wniosku),
- subskrypcja usług Premium SMS,
- ataki *phishingowe* na bankowość elektroniczną,
- kampanie *phishingowe* polegające na podszywaniu się pod bankowość elektroniczną,
- wyłudzenie danych umożliwiających wykonanie operacji w systemach bankowości elektronicznej lub wyłudzenie danych z kart płatniczych,

- ataki *phishingowe* na klientów Poczty Polskiej,
- kampanie złośliwego oprogramowania,
- przesyłanie wiadomości podszywającej się pod powiadomienie wysłane przez Poczta Polska, zawierającej link do oprogramowania,
- *cryptolocker* (rodzaj *ransomware*),
- okup za odszyfrowanie danych: 1299 zł na krótki okres, później 2399 zł,
- ataki *phishingowe* na klientów PGE pod pozorem wysyłki faktury.

Podsumowanie roku 2016

Pierwszy kwartał 2016 r. z najmniejszą liczbą zagrożeń w porównaniu do pozostałych był dość spokojny dla użytkowników. Główny udział w zdarzeniach miał Trojan. ZeroAccess, *dropper* pobierający m.in. aplikacje, wykorzystujący moc obliczeniową komputera ofiary do „wykopywania” kryptowaluty bitcoin lub wymuszający na użytkownikach kliknięcia w reklamy typu *pay-per-click*. Podobne funkcje ma drugi z *dropperów*, Diple, pobierający m.in. *malware* ZeroAccess oraz kod wykradający dane wrażliwe ze stacji ofiary. W pierwszym kwartale, zwłaszcza w lutym, zidentyfikowaliśmy wzmożoną aktywność bota Jorik, również wykorzystującego zasoby zainfekowanych urządzeń do wydobywania bitcoinów. Na przełomie lat 2015 i 2016 CERT Orange Polska zaobserwował intensywną kampanię rozprzestrzeniania oprogramowania *ransomware* Cryptowall. Infekuje on witryny WWW, by następnie wykorzystując podatności w systemie ofiary, bez jej wiedzy pobrać i zainstalować złośliwy kod na jej komputerze. Pierwszą piątkę pierwszego kwartału zamyka hybrydowy trojan Sality wykradający dane wrażliwe ze stacji i wykorzystujący przejęte urządzenie do ukierunkowanych ataków bądź kampanii spamowych. W drugim kwartale zanotowano rozwój infekcji opartych na paczkach *exploit kitów*, wykorzystujących podatności w aplikacjach sieciowych i zabezpieczeniach antywirusowych. *Malvertising* – jak wskazuje nazwa – to złośliwe reklamy spotykane najczęściej w serwisach oferujących

pirackie wersje oprogramowania bądź umożliwiających obejrzenie najnowszych filmów i seriali bez ponoszenia opłat w zamian za uruchomienie w tle kilku mało uciążliwych reklam.

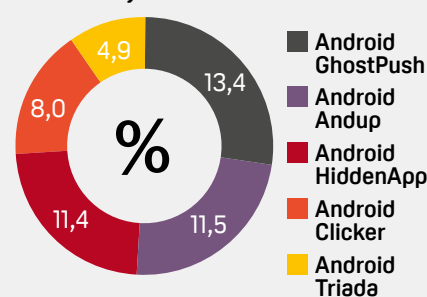
Trzeci kwartał wyróżnił się najmniejszą liczbą anomalii, utrzymując trend z pierwszej połowy roku. W skrzynkach e-mailowych regularnie pojawiały się kampanie *phishingowe*, a tą drogą najczęściej był rozpowszechniany *ransomware* Locky (skrypt, który ukrywa się zazwyczaj w makrach dokumentów aplikacji MS Excel czy MS Word). Obserwowano także natężenie infekcji trojanami bankowymi, w tym Ursnif, którego kolejne wersje nauczyły się rozpoznawać, czy plik zawierający gotowy do wykonania kod jest otwierany przez użytkownika, czy przy życiu procesów charakterystycznych dla rozwiązań bezpieczeństwa, uruchamiając faktyczny *malware* tylko w tym pierwszym przypadku. Najczęściej występujące złośliwe oprogramowanie w czwartym kwartale ubiegłego roku było zarówno efektem nowych podatności i rodzin złośliwego oprogramowania (Mirai), jak i początku roku akademickiego oraz przedświątecznych zakupów. W kolejnych kampaniach „faktur” cyberprzestępcy umieszczali *ransomware* TorrentLocker, czyli nową odmianę znanego

go Cryptolockera, komunikującą się z C&C w celu wymiany kluczy zaszyfrowanym kanałem. Działanie Nymaima z kolei było ukierunkowane na infekcję przeglądarek prowadzącą do ataku *man-in-the-browser* – modyfikację danych zawartych w poleceniach przelewów bankowych w momencie wykonywania płatności elektronicznych.

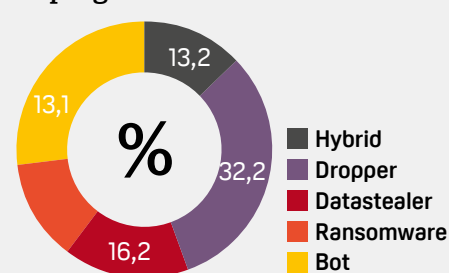
Ostatnie miesiące 2016 r. zdominował *backdoor* atakujący urządzenia Internetu Rzeczy działające pod kontrolą systemu Linux – bot Mirai. Botnet składający się z urządzeń zainfekowanych tym oprogramowaniem został po raz pierwszy użyty 20 września 2016 r. Jego efektem był należący do największych ataków DDoS w historii dochodzący do 620 Gb/s.

Ze względu na stosunkowo niski poziom zabezpieczeń urządzeń Internetu Rzeczy (hasła domyślne, nieaktualne oprogramowanie) oraz ich rosnącą powszechność Mirai rozprzestrzenił się także w Polsce, dominując wśród największych *botnetów* zidentyfikowanych w badanej przez CERT Orange Polska próbkę. III

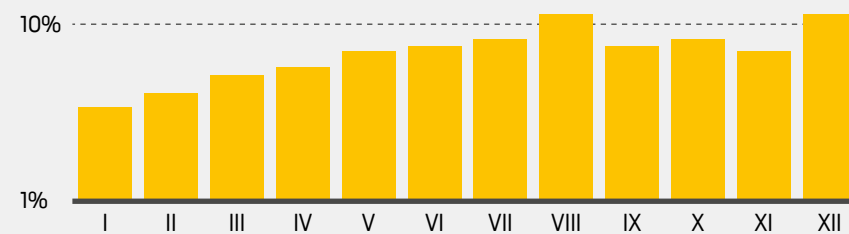
Top 5 zagrożeń mobilnych 2016 roku



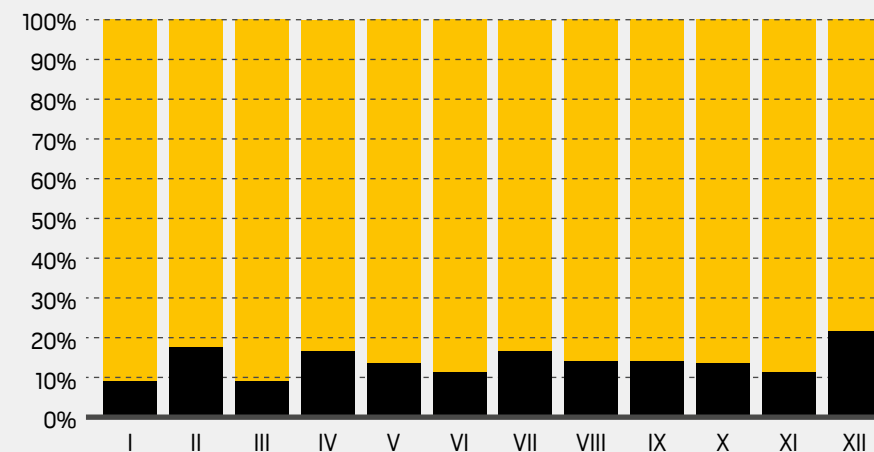
Rodzaje złośliwego oprogramowania



Użytkownicy zainfekowani złośliwym oprogramowaniem na urządzenia mobilne (średnia miesięczna z roku 2016)



Użytkownicy zainfekowani złośliwym oprogramowaniem (dane dla poszczególnych miesięcy roku 2016)



RAPORT

Boom na rynku IoT i inteligentnego domu niezbędna standaryzacja

Internet Rzeczy (IoT) wywołał niemałe zamieszanie i przyspieszył rozwój wielu branż. Raporty czołowych firm badawczych pokazują, że szybko rosną wydatki i przychody związane z IoT w krajach Europy Środkowo-Wschodniej. Chiny i Stany Zjednoczone to kolejne duże rynki inteligentnego domu. Rozpowszechnianie się IoT pociąga problemy związane z ochroną prywatności i cyberbezpieczeństwem, co wymusza opracowanie standardów ochrony danych osobowych.

a&s International

1 Wydatki na IoT w Europie Środkowo-Wschodniej za 4 lata wyniosą 24 mld USD

Nakłady na urządzenia, oprogramowanie, usługi i komunikację związane z IoT w krajach Europy Środkowo-Wschodniej w 2016 r. wyniosły 11 mld USD. Według prognoz firmy analitycznej IDC przychody związane z IoT w tym rejonie w latach 2016–2020, przy średnim wskaźniku CAGR na poziomie 21,5% zamkną się kwotą 24 mld USD. Pod względem inwestycji w IoT w 2016 r. pierwsze miejsce zajmowała branża transportu, generując wydatki rzędu 2,3 mld USD. Tuż za nią znalazł się sektor produkcyjny (2,1 mld USD), trzecie miejsce (1,2

mld USD) przypadło sektorowi *utilities*. Według IDC w najbliższych pięciu latach na prowadzenie pod względem obrotów w obszarze IoT wysunie się rynek konsumenta. Ubezpieczenia, budownictwo (inteligentne budynki), transport, samochody podłączone do sieci oraz inwestycje międzybranżowe będą stanowiły główne obszary zastosowań IoT. Wzrosną też nakłady użytkowników indywidualnych na inteligentne domy – według IDC do 2020 r. przekroczą 1,1 mld USD. Firmy oraz instytucje rządowe w Europie Środkowo-Wschodniej, podobnie jak konsumenci, dobrze znają ideę Internetu Rzeczy i są skłonni do poważnych inwestycji w rozwijanie IoT – wyjaśnia Milan Kalal, Program Manager ds. Internetu Rzeczy w IDC CEMA. Według IDC największe obro-



ty przyniosą usługi, następnie sprzęt, oprogramowanie i komunikacja. Wydatki na usługi w ciągu najbliższych pięciu lat mają się podwoić, osiągając w 2020 r. poziom 7 mld USD. Na razie szybszy wzrost będzie dotyczył sprzętu (moduły i czujniki) oraz oprogramowania, aplikacje natomiast mogą stanowić ponad połowę wydatków na oprogramowanie.

2 Chiny i Stany Zjednoczone – największe rynki rozwiązań inteligentnego domu

Firma analityczno-konsultingowa Ovum w ostatnim raporcie prognozuje, że największymi odbiorcami rozwiązań inteli-

gentnego domu będą Chiny i USA, a sprzedaż urządzeń inteligentnych do 2021 r. przekroczy 1,4 mld sztuk. Według jej analityków za wzrost od 224 mln w 2016 r. do 1,4 mld w roku 2021 będą odpowiadać głównie urządzenia z branż security i *utilities*, takie jak kamery, zamki do drzwi, inteligentne termostaty i żarówki. Liczba inteligentnych gospodarstw domowych w 2021 r. wzrośnie do 463 mln, w każdym będzie się znajdować średnio 8,7 urządzeń inteligentnych, co łącznie – jak podaje Ovum – zwiększy ich liczbę do 1,4 mld sztuk.

Stany Zjednoczone i Chiny uznano za największe rynki rozwiązań inteligentnych domów ze względu na podaż

produktów i duże zainteresowanie konsumentów. Pozostałe rejony Azji Wschodniej i Południowo-Wschodniej także będą miały istotne znaczenie dla rynku. Opracowana przez Ovum dla sektora inteligentnych domów mapa przedstawiająca nasycenie rynku w 2021 r. pokazuje, że w adaptacji technologii prowadzenie obejmą Stany Zjednoczone (69%). Za nimi znajdą się Kanada (54%), Korea Południowa (48%), Japonia (41%) i Wielka Brytania (40%). W raporcie przedstawiono podział urządzeń inteligentnego domu na pięć kategorii: *utilities*, AGD, security, interaktywne głośniki audio i pozostałe. Uwagę zwraca osobna kategoria interaktywnych głośników audio (takich jak Amazon Echo czy Google Home). Zdaniem Ovum ich sprzedaż będzie rosła najszybciej – w 2021 r. osiągając 192 mln sztuk.

Raport wskazuje też na lukę między systemami „zrób to sam” a dedykowanymi usługami dla inteligentnego domu. Na przykład do 2021 r. 15,5% gospodarstw zaadaptuje inteli-

gentne systemy zabezpieczeń, a jedynie 6,2% zamierza skorzystać z płatnych profesjonalnych usług branży ochrony. Ta luka może oznaczać dla firm nowe możliwości rozwoju modeli biznesowych skupionych wokół technologii inteligentnego domu.

3 Standardy bezpieczeństwa produktów IoT

Wydawnictwo Consumer Reports zapowiedziało wykreowanie standardu, który umożliwiłby sprawdzenie odpowiedniego poziomu zabezpieczeń i prywatności użytkowników korzystających z urządzeń IoT. Impulsem do opracowania standardu były wyniki niedawnej ankiety CR Consumer Voices, według której 65% Amerykanów nie ma pewności, czy ich dane osobo-

we są bezpieczne podczas korzystania z komunikujących się ze sobą urządzeń IoT. Zdaniem Consumer Reports producenci nie powinni przerzucać na użytkowników odpowiedzialności za bezpieczeństwo urządzeń sieciowych. Branża powinna zainteresować się proponowanym standardem ochrony prywatności i bezpieczeństwa, wdrażając odpowiednie mechanizmy podczas projektowania i tworzenia produktów cyfrowych – urządzeń IoT, oprogramowania i aplikacji. Naszym celem jest pomoc konsumentom w zorientowaniu się, które z produktów cyfrowych najlepiej chronią ich prywatność i bezpieczeństwo oraz umożliwiają im kontrolę nad ich danymi osobowymi – podkreślono w komunikacie.

Przy opracowaniu wskazówek

i rozwiązań standardów jak najbardziej uniwersalnych Consumer Reports współpracowało z kilkoma partnerami. Wśród nich znaleźli się np. dostawca aplikacji blokujących śledzenie danych Disconnect, organizacja non profit Ranking Digital Rights (RDR) zajmująca się badaniami polityki prywatności oraz Cyber Independent Testing Lab (CITL) testująca bezpieczeństwo oprogramowania. Spółka przedstawiła wskazówki dotyczące tego standardu. Przykładowo podczas pierwszego uruchomienia nowego urządzenia IoT użytkownik powinien zostać zapytany o ustanowienie unikatowej nazwy użytkownika i hasła, podobnie jak to się dzieje w przypadku zakładania konta bankowego. Ponadto polityka firm powinna obejmować praktyki usuwania z serwera danych konsumenta na jego prośbę o ochronę prywatności.

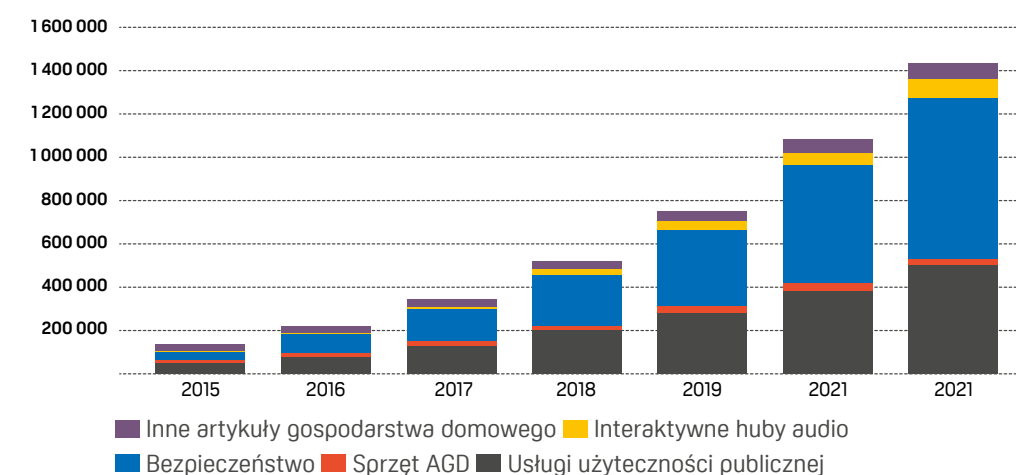
Standard ten może być wykorzystywany jako pomoc w rozwijaniu specyficznych i powtarzalnych procedur testowych. Będziemy wówczas mogli oceniać produkty i umożliwiać konsumentom ich wzajemne porównywanie na podstawie np. stopnia ochrony prywatności, podobnie jak robimy to obecnie w innych aspektach działania produktów – podkreśla Consumer Reports.

65%

mieszkańców Stanów Zjednoczonych nie ma pewności, czy ich dane osobowe są bezpieczne podczas korzystania z urządzeń skomunikowanych.

Liczba sprzedanych urządzeń dla inteligentnego domu wg kategorii

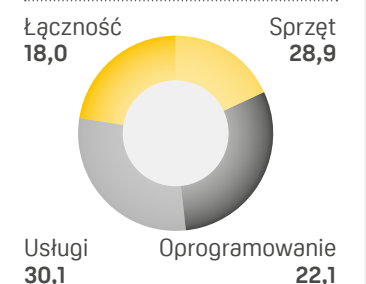
Liczba sprzedanych sztuk



Źródło: Prognoza Ovum dotycząca urządzeń inteligentnego domu 2016–2021

Udziały w rynku IoT w 2016

[%] poszczególnych segmentów technologii w Europie Środkowo-Wschodniej



INTELIGENTNY DOM trendy na 2017 rok

a&s International

1

OFERTA FIRM TELEKOMUNIKACYJNYCH DLA INTELIGENTNEGO DOMU

Główni dostawcy usług telekomunikacyjnych, np. AT&T, Deutsche Telekom, Orange, od kilku lat są aktywni w biznesie *smart home*. Biorąc pod uwagę, że inteligentny dom stanowi „ciekawą dodatek” dla stałych klientów, operatorzy z różnych krajów, np. Telstra (Australia), Singtel (Singapur), True (Tajlandia), MobiPhone (Wietnam), SK (Korea Południowa),

O2 (Wielka Brytania) KP (Holandia), wprowadzili w 2016 r. nowe usługi inteligentnego domu oparte na własnych aplikacjach. W roku 2017 zestaw i usługi dla inteligentnego domu zamierza wprowadzić więcej operatorów telefonii i telewizji kablowej z rynków wschodzących, m.in. z południowej Afryki, krajów ASEAN, Ameryki Południowej i Europy Wschodniej.

2

KONTROLA I STEROWANIE GŁOSEM

Raporty firm analitycznych dowodzą, że w ciągu ostatniego półtora roku sterowanie głosem stało się kategorią dominującą w sektorze urządzeń inteligentnego domu. ABI Research podaje, że kontrolowane głosem urządzenia inteligentnego domu, reprezentowane przez Amazon Echo, do 2021 r. będą generować 30% obrotów na rynku *smart home*, mimo że ta kategoria sprzętu dwa lata temu dopiero zaczynała się rozwijać. Możliwość wykorzystania funkcji cyfrowego asystenta na smartfony stanowi realną wartość dla klientów. *Zdolność do integracji i poszerzania zakresu zastosowań kontroli głosem w domach będzie oczywiście wymagać o wiele większej liczby urządzeń z funkcją sterowa-*

nia głosowego – mówi Jonathan Collins, dyrektor ds. badań w ABI Research. – *W ciągu najbliższych pięciu lat dystrybutorzy urządzeń dla domu i AGD, a także instalatorzy i dostawcy systemów inteligentnego domu podejmą współpracę prowadzącą do integracji w ramach platform sterowania głosem.* Niemiecki operator Deutsche Telekom potwierdził, że jego otwarta platforma dla domów włączonych do sieci (QIVICON) została zintegrowana z aplikacją Alexa (Amazon) we wrześniu 2016 r. W swoim komunikacie podaje: *Współpraca z Amazonem pozwala oferować klientom jeszcze więcej rozwiązań innowacyjnych. Wierzymy w przyszłość inteligentnych domów sterowanych głosem.*

W ślad za popularnością Amazon Echo na rynkach zachodnich z możliwości komunikacji w różnych językach skorzystali też konkurenci Echo, tacy jak NUGU od SK Telecom w Korei Płd. czy DingDong w Chinach. NUGU początkowo oferowało urządzenie w kształcie walca o średnicy 21,9 cm z planowaną funkcjonalnością głośnika i oświetlenia LED. Koreański operator potwierdził, że w pierwszej połowie 2017 r. zamierza uruchomić funkcję *Application Programming Interfaces* (APIs), która pobudzi rozwój ekosystemu wokół NUGU poprzez bliską współpracę ze start-upami, małymi i średnimi przedsiębiorstwami oraz ekspertami z dziedziny sztucznej inteligencji w celu udostępnienia usług powiązanych.

4

WIĘCEJ PLATFORM IOT GOTOWYCH DO WYKORZYSTANIA

Platformy IoT są kluczowe dla takich zastosowań i usług, jak inteligentne domy, które łączą rzeczywiste i wirtualne światy przedmiotów, systemów i ludzi. W 2016 r. na rynku było co najmniej 300 platform IoT, wśród nich Predix (GE), Watson (IBM) czy SAP (Hana). Ich liczba wciąż rośnie. Rozwój ułatwiają liczne start-upy, producenci sprzętu, urządzeń sieciowych, twórcy oprogramowania biznesowego i zarządzania mobilnego, tacy jak IBM, Amazon, Ayla Networks, Exosite, Orbweb itd. Ze względu na różne strategie biznesowe dostawców usług IoT zyski z potencjału Internetu Rzeczy zapewni partnerstwo. Amerykański Qualcomm Technologies przedstawił plany współpracy z Google mającej na celu wspieranie przez procesory Qualcomm Snapdragon

nowego systemu operacyjnego Android Things. Jak podają przedstawiciele Qualcomm, jest to nowe rozwiązanie wertykalne do urządzeń IoT. Programiści mogą wykorzystać swoją wiedzę na temat Androida i procesorów Snapdragon, aby przyspieszyć rozwój rozwiązań IoT. Grupa Alibaba zadebiutowała w branży IoT w Chinach systemem YunOS. Ponad 10 milionów telewizorów smart i modułów TV box chińskich marek Lenovo i Skyworth sprzedawano z zainstalowanym oprogramowaniem YunOS. W ten system wyposażono ponadto podłączone do sieci wentylatory kuchenne firmy Haier i inteligentne lodówki Midea. Poza granicami Chin system ten zainstalowano w robotach Pepper japońskiej firmy SoftBanks oraz samochodach SAIC Motor.

Jak podano w rocznym komunikacie z 2016 r. wysłanym do udziałowców Alibaby przez Jacka Ma, założyciela i prezesa, firma aktywnie inwestuje w usługi przetwarzania we własnej chmurze, Alibaba Cloud, ponieważ środowisko e-commerce już wkrótce stanie się powszechne. Plany firmy skupiają się na możliwościach wykorzystania jej systemu handlowego i stworzenia środowiska dla nowych technologii, takich jak sztuczna inteligencja, VR (*Virtual Reality* – rzeczywistość wirtualna) AR (*Augmented Reality* – rzeczywistość rozszerzona) oraz Internet Rzeczy. W walce o IoT najlepszą bronią ma być system YunOS. Oprócz strategii i modeli biznesowych kluczowe dla podkreślenia wartości IoT jest generowanie złożonych danych. Umożliwia to zasadniczo już sama platforma.

INTELIGENTNE DOMY OPARTE NA SZTUCZNEJ INTELIGENCJI

Technologie sztucznej inteligencji (AI – *Artificial Intelligence*) umożliwiają urządzeniom inteligentnego domu rozpoznawanie sygnałów odbieranych z urządzeń zdalnie sterowanych, takich jak urządzenia *wearable* (które można nosić na sobie), w celu sterowania urządzeniami AGD, urządzeniami i systemami zabezpieczeń. Oprócz Amazona i Google również Apple, Samsung i Microsoft mają potencjał do wprowadzenia na rynek podobnych urządzeń i funkcji. Według Technavio rynek AI ma wiele do zaoferowania dystrybutorom i producentom OEM z sektora inteligentnego domu, takim jak Samsung Electronics. W listopadzie 2016 r. ten gigant technologiczny z Korei Płd. przedstawił plan wdrożenia technologii AI w urządzeniach AGD Samsung. Firma ma taką możliwość dzięki dokonaniu w październiku przejęcia Viv. Start-up Viv został założony przez twórców Siri, wirtualnego asystenta Apple. W 2012 r. odeszli oni z Apple i powołali Viv. Ma on odmienną budowę niż Siri, a różnica polega na tym, że jego system

back-end ma charakter programowy. Platforma sztucznej inteligencji Viv potrafi sama tworzyć nowe kody, by wykonać nawet takie zadania, dla których nie istnieją instrukcje w oryginalnie napisanym kodzie. Wszystkie te firmy planują inwestycje w rozwiązania AI i tworzenie inteligentnych urządzeń nowej generacji. Także największy dystrybutorzy przetwarzania w chmurze – Amazon Web Services i Microsoft – inwestują w rozwiązania AI i technologie uczenia maszynowego. Przetwarzanie w chmurze stało się kluczowym elementem technologii inteligentnego domu, ponieważ w chmurze znajdują się zarówno aplikacje, jak i magazyn danych. Ponadto inwestycje w AI, wspomagane przez przetwarzanie w chmurze, zwiększają konkurencyjność głównych producentów. Kolejnym elementem sprzyjającym rozwiązaniom AI w aspekcie technologicznym jest wykrywanie i rozpoznawanie emocji. Najszybszy wzrost analitycy przewidują w technologii biosensorów. Instytut badawczy MarketsandMar-

kets szacuje, że rynek wykrywania i rozpoznawania emocji wzrośnie z 6,7 mld USD w 2016 r. do 36,1 mld USD w 2021, przy wskaźniku CAGR 39,9%. Z kolei gigant technologiczny IBM poinformował, że w listopadzie 2016 r. udostępni swoją wiedzę na temat przetwarzania kognitywnego wszystkim producentom oprogramowania. Przedstawiciele IBM upublicznili ten eksperymentalny projekt pod nazwą Project Intu. Jest to platforma pozwalająca na wbudowanie w urządzenia funkcji Watson, takich jak umiejętności uczenia kognitywnego czy podstawy uczenia maszynowego i oferowanie architektury nowej generacji do budowania rozwiązań opartych na podejściu kognitywnym. Ten otwarty projekt pozwoli twórcom oprogramowania skupić się na innych funkcjach.

5



POPRAWA BEZPIECZEŃSTWA IOT

W erze automatyki domowej i szybkiego wzrostu liczby skomunikowanych urządzeń IoT dla domu wielu dystrybutorów i duża liczba nowych start-upów chce nadążyć za tym trendem. ABI Research przewiduje, że do roku 2020 liczba sprzedanych urządzeń inteligentnego domu wyniesie 360 mln.

Przy rosnącej liczbie urządzeń domowych podłączonych do sieci pojawia się coraz więcej luk związanych z użytkowaniem urządzeń IoT. Przykładem jest zmasowany atak DDoS w USA przeprowadzony w październiku 2016 r. Hakerzy wykorzystali luki urządzeń IoT, przejęli serwery dostawcy DNS i zakłócili działanie takich serwisów jak Netflix, Airbnb czy Spotify.

Obserwujemy alarmujący rozwój złośliwego ransomware w telewizorach smart i kamerach IP, ataki typu code injection, dowody na istnie-

nie zagrożeń typu zero-day, a także wykradanie haseł inteligentnych zamków i urządzeń podłączonych do sieci – mówi Dimitrios Pavlakis, analityk branżowy w ABI Research. Stan zabezpieczeń w środowisku inteligentnego domu jest niewystarczający. Producenci urządzeń smart home muszą zadbać o mechanizmy cyberbezpieczeństwa już na etapie projektowania produktów. Techniczna Grupa Doradcza ds. Internetu Szerokopasmowego (Broadband Internet Technical Advisory Group) wspierana przez gigantów technologicznych, m.in. Google, AT&T, Cisco, T-Mobile, Intel i Microsoft, zaleca posiadanie ostatniej aktualizacji oprogramowania, używanie silnego uwierzytelniania poprzez domyślne, a zarazem trudne do odgadnięcia nazwy użytkownika i moce hasła, przestrzeganie najlepszych praktyk bezpieczeństwa

i szyfrowania. Przestrzeganie tych zaleceń zwiększy poziom bezpieczeństwa. Ponadto dostawcy usług IoT powinni dystrybuować produkty w ramach prostej polityki prywatności, cały sektor IoT natomiast powinien rozważyć opracowanie branżowego programu cyberbezpieczeństwa.

Już na etapie projektowania producenci OEM muszą myśleć przede wszystkim o bezpieczeństwie i oceniać ryzyko – podkreśla D. Pavlakis. – Kolejny krok stanowi zapewnienie odpowiednich testów bezpieczeństwa, zanim produkt wejdzie na rynek. W kolejnej fazie producenci powinni oferować stałe wsparcie bezpieczeństwa przez cały okres życia produktu. Bez podjęcia tych podstawowych kroków konsekwencją ataków na produkty inteligentnego domu będą wysokie koszty finansowe i wizerunkowe producentów.

6



OPIEKA ZDROWOTNA W DOMU

Urządzenia typu *wearable* i *smart-watche*, integrowane z innymi aplikacjami IoT, są coraz bardziej powszechnym narzędziem opieki medycznej. Skupienie usług i urządzeń opieki medycznej na konsumencie przyczynia się do integracji ze środowiskiem inteligentnego domu i nowymi modelami biznesowymi. Spośród urządzeń smart home w obszarze opieki medycznej w kręgu zainteresowania w 2016 r. znalazły się rozwiązania poprawiające jakość snu i czystość powietrza.

Nowe rozwiązania, takie jak Sense, czujniki snu SleepExpert firmy Beurer, Sleepace Nox, materace oferowane przez Eight, żarówki C Sleep Smart Bulb firmy General Electric i inne, zostały opracowane pod kątem poprawy jakości snu. Łączy Bluetooth, wsparcie IFTTT czy sterowanie głosem są w tych produktach powszechne i poprawiają zarówno integrację w ramach inteligentnego domu, jak i wrażenia użytkowników. Przykładowo czujnik wykrywa, że użytkownik się budzi. Wtedy Sense

przekazuje wiadomość inteligentnemu termostatowi, aby ustawił wybraną temperaturę w pomieszczeniu lub stopniowo zapalał światła. Wersja Sense with Voice współpracuje z termostatem Learning Thermostat firmy Nest i inteligentnym oświetleniem Hue Philipsa. Czujniki wbudowane w materac Eight śledzą nagłe ruchy, zmianę pozycji, szybkość oddechu, czas i jakość snu oraz warunki w sypialni, w tym temperaturę łóżka i powietrza. Dane mogą być eksportowane do innych aplikacji związanych ze zdrowiem, np. Apple'a czy Google'a. Na podstawie zebranych danych aplikacja mobilna może budzić użytkowników alarmem dostosowanym do ich cyklu snu.

Zanieczyszczenie powietrza to nie tylko problem na zewnątrz budynków. Powietrze wewnątrz może być skażone pleśnią, formaldehydem czy radem. Zagrożenia mogą wynikać również z braku wentylacji, wycieków gazu, unoszącego się w powietrzu pyłu z domu czy spoza niego, a także z VOC (lotne związki organiczne) z mebli, dekoracji czy

produktów gospodarstwa domowego. Inteligentne czujniki informują użytkowników o jakości powietrza i przekazują dane niezbędne do utrzymania zdrowej atmosfery. Powszechnie mierzone parametry obejmują temperaturę, wilgotność, stężenie tlenu, dwutlenku węgla, zapylenie, w tym PM2,5 i PM10, a także lotne związki organiczne VOC.

Firmy takie jak Withings (przejęta przez Nokię), Awair, iBaby Air, Koto Air czy EQL wykorzystują zaawansowane technologie, np. przetwarzanie w chmurze, przetwarzanie Big Data i sztuczną inteligencję do zaawansowanych zastosowań ułatwiających podejmowanie decyzji dotyczących czystości powietrza. Rok 2017 z pewnością przyniesie więcej inteligentnych produktów zapewniających poprawę jakości życia.



7



INTELIGENTNE OŚWIETLENIE W PRZYSTĘPNEJ CENIE

Inteligentne oświetlenie nie jest rozwiązaniem nowym na rynku inteligentnego domu. Wiele firm oferuje produkty, którymi można sterować przy użyciu smartfonów. Strategia cenowa producentów spowolniła jednak ich upowszechnianie na większą skalę. Szwedzki gigant meblowy IKEA chce, żeby stały się one przystępne cenowo. We wrześniu ub.r. firma wprowadziła drugą linię produktów dla inteligentnego domu. Zaoferowała klientom inteligentną żarówkę LED, którą można regulować zdalnie. Kolekcja obejmuje żarówki LED, panele oświetleniowe, drzwi i funkcję zdalnego sterowania. IKEA podaje, że żarówka

może współpracować ze wszystkimi standardami gniazd, gdyż posiada własny wbudowany moduł zasilający. Także we wrześniu TP-Link udostępnił nową rodzinę inteligentnych żarówek Wi-Fi. Podobnie jak zwykłe żarówki, żarówki Wi-Fi nie potrzebują do pracy huba czy mostka, dzięki czemu są tanie i łatwe w użytkowaniu. Konsumenci mogą ściągnąć aplikację i połączyć się z żarówką poprzez Wi-Fi w kilka sekund, mogą też łatwo dodawać urządzenia i komunikować się z inteligentnym domem. W perspektywie globalnej rynek tradycyjnych systemów oświetleniowych wyposażonych w funkcjo-

nalność rozwiązań inteligentnych najszybciej rozwija się obecnie w Europie. W kolejnych latach palną pierwszeństwa przejmie region Azji i Pacyfiku ze względu na szybko rosnące zapotrzebowanie na ekonomiczne i energooszczędne oświetlenie w krajach rozwijających się, np. Chinach czy Indiach.

8



PRZEJĘCIA NA RYNKU AUTOMATYKI DOMOWEJ

W październiku podano informację o największej w historii transakcji w branży półprzewodników. Holenderska firma NXP została kupiona przez amerykańskiego giganta Qualcomm, który zapłacił za nią 47 mld USD. Kwota ta przyćmiła 37 mld USD, jakie Avago zapłaciło za Broadcom, czy 30 mld przeznaczonych przez SoftBank na nabycie ARM Holdings. Transakcje takie jak Qualcomm-NXP, Qorvo-Greenpeak itp. odzwierciedlają pilną potrzebę poprawy konkurencyjności w dojrzewającym świecie półprzewodników.

Na targach CES 2016 NXP pokazał zestaw do rozwoju inteligentnego domu. Firma oferuje gotowe do produkcji moduły i projekty do inteligentnego oświetlenia, detekcji dymu, detekcji ruchu i urządzenia pełniące funkcję domowej bramy sieciowej. Połączenie Qualcomm z NXP ma zapewnić organizacji pierwszą pozycję na rynku IoT. *Jeśli mówimy o wsparciu dla klientów w obliczu dynamicznego rozwoju rynku IoT, to nie istnieje rozwiązanie uniwersalne. Potrzebna jest elastyczna platforma pozwalająca na innowacje* – uważa Stephen DiFranco, wiceprezes ds. IoT w Cypress i były dyrektor general-

ny w Broadcom IoT. Na początku lipca firma Cypress ogłosiła przejęcie oddziału IoT i związanych z nim udziałów firmy Broadcom w ramach transakcji wycenianej na 550 mln USD. Przejęcie Cypress umożliwiło włączenie do oferty linii produktów IoT wspierających protokoły Wi-Fi, Bluetooth oraz ZigBee, wraz z powiązanim know-how, a także zestaw narzędzi programowania WICED, środowisko i społeczność deweloperskie. Obawy o elastyczność ofert były siłą napędową także dla innych przejęć z branży automatyki domowej w 2016 r., m.in. Leviton-ConTech Lighting, Bosch-Skyline Automation, Nokia-Withings czy Legrand-Luxul Wireless.





9 STARCIE GIGANTÓW

Rok 2016 przyniósł wiele innowacyjnych urządzeń IoT, nowości dla inteligentnego domu i możliwość współpracy pomiędzy protokołami komunikacji. Czwórka gigantów, czyli Amazon, Apple, Google, Microsoft, dokłada wszelkich starań, aby tworzyć nowe obszary na rozwijającym się rynku *smart home*. Wraz z premierą nowej wersji systemu operacyjnego iOS 10, która odbyła się 13 września, uniwersalna aplikacja do sterowania inteligentnym domem pod nazwą Home, opracowana przez Apple'a, wkroczyła w fazę testów beta na iPhone. Kilka dni później Amazon przedstawił Echo Dot w cenie nieprzekraczającej 50 USD, dzięki czemu z Alexy można korzystać w dowolnym pomieszczeniu domu. Z kolei 4 października ub. roku Google zaprezentowało swoje debiutanckie urządzenie w stylu Echo, czyli Google Home. Zapowiada się walka, ale na razie trudno powiedzieć, kto uzyska do-

minację w świecie inteligentnego domu. Apple oferuje coś, czego inne firmy nie mają: plan ekosystemu inteligentnego domu, który pozwoli producentom urządzeń i osobom o wiedzy technologicznej tworzyć produkty zdolne do zintegrowanej komunikacji z użytkownikiem i peryferiami, nie wspominając o ogromnej bazie użytkowników i dużych udziałach w rynku. Ten stan odzwierciedla rzeczywisty potencjał rynkowy. Poważnym czynnikiem zniechęcającym twórców do związania się z tym ekosystemem może być natomiast koszt i czas oczekiwania na licencję *Made For iPhone* (MFi), certyfikacja *HomeKit* i obowiązkowy zakup wszystkich kluczowych elementów od nieujawnionych dostawców.

Platforma Google Home, która integruje różne usługi Google – *Google Calendar*, *Google Keep* i *Google Maps* – próbuje dorównać kroku usługom Amazon Alexa, która przez dwa lata rozwinęła tysiące funkcji dla inteligentnego domu. Podobno Google buduje swój ekosystem, zachęcając twórców do tworzenia własnych sterowanych głosem urządzeń z wbudowanym wirtualnym asystentem Google. Miesiąc po wejściu Google Home na rynek uruchomił program *Actions on Google*, który pozwala deweloperom rozwijać środowisko poleceń wydawanych podczas rozmowy dla Google Home. Otwarte narzędzia zostaną udostępnione niezależnym deweloperom na początku 2017 r., natomiast współpracujący z Google partnerzy – IFTTT, Nest, Samsung SmartThings i Philips Hue – już ogłosili nowe funkcje dla Google Home.

Inaczej niż Amazon proponujący użytkownikom Alexę, w przypadku Google Assistant Google stosuje inny system deweloperski. Nie zamierza np. tworzyć strony, na której użytkownik będzie wybierał funkcjonalności dla swojego Google Home. Planuje natomiast zatwierdzanie i wprowadzanie słowa kluczowego z innych usług w ramach

dostępu otwartego. Aby to osiągnąć, Google opracuje odpowiednią politykę i systemy filtrujące, aby zapobiegać *campingowi* słów kluczowych, tj. praktyce deweloperów polegającej na używaniu w funkcji poleceń słów czy haseł innych marek lub firm. Google przygotowuje się także do włączenia Google Assistant do swojej usługi czatowania Allo i smartfonów Pixel. Deweloperzy mogą więc poprzez *Actions on Google* zacząć tworzyć nowe aplikacje także dla tych dwóch zastosowań. Amazon Echo obchodził 6 listopada ub.r. drugie urodziny, a firma wprowadził już Amazon Echo 2. Nowa wersja premium została wyposażona w siedmiocalowy ekran dotykowy. Nie licząc nowych udoskonaleń, takich jak ładowanie bezprzewodowe i lepsza jakość dźwięku, Amazon Echo 2 ma za zadanie upowszechnić zastosowania inteligentnego domu przy użyciu usprawnionej komunikacji sieciowej i ulepszonej usługi głosowej.

Współpraca Amazona z Intelem zdecydowanie pomogła w rozwoju ekosystemu inteligentnego domu. Intel w ramach partnerstwa zainicjował dwa kierunki rozwoju. Pierwszy z nich polega na umożliwieniu usługi Alexa zdalnego sterowania i koordynowania urządzeń za pośrednictwem huba opartego na technologii Intel. Drugi dotyczy przyspieszenia rozwoju sprzętowego dla urządzeń głosowych za pomocą usług głosowych Alexa i platformy Intel. Aby zrealizować tę drugą inicjatywę, Intel podejmuje współpracę z Amazonem nad dostarczaniem oferty Alexa producentom. W grudniu Amazon udostępnił kody w celu zwiększenia inteligencji usługi Alexa. W ostatnim komunikacie Amazon potwierdził wdrożenie biblioteki kilkuset nowych intencji (intent) i slotów (slot) jako część środowiska Alexa Skill Kit.

W języku kodowania Alexa intencje należy rozumieć jako podstawowe komendy, a sloty są używane do identyfikowania informacji, takich

KAMIEŃ MIŁOWY NA RYNKU INTELIGENTNEGO DOMU W 2016 R.

CORTANA/HOME HUB

MICROSOFT implementuje funkcje Home Hub do Windows 10 – to oprogramowanie zmieni komputer osobisty w domową centralę.



a

ALEXA/ECHO

ALEXA, usługa głosowa będąca podstawą Echo, zapewnia rozwiązania do intuicyjnego domu inteligentnego.

SIRI/HOMEKIT

HOMEKIT to platforma firmy Apple służąca do komunikacji i sterowania podłączonymi do sieci peryferiami w domu użytkownika.



ASSISTANT/HOME

GOOGLE HOME bazuje na Google Assistant. Zadawaj pytania, wydawaj polecenia, asystent chętnie ci pomoże.

jak daty czy liczby. Do niedawna Alexa obsługiwała około 15 intencji i 10 rodzajów slotów. Amazon wprowadza nowe intencje i sloty jako elementy wbudowane, aby deweloperzy nie musieli używać asercji do uczenia Alexy rozumienia intencji użytkownika. Ma to ułatwić integrację i przyspieszyć wprowadzanie produktów na rynek.

Nie chcąc przejmować się konkurencją i wyróżnić spośród innych firm, Microsoft wchodzi na rynek inteligentnego domu z urządzeniem Home Hub. W odróżnieniu od Google czy Amazonu, Home Hub nie jest sprzętem, lecz oprogramowaniem. Home Hub zostanie zintegrowany z Windows 10, aby użytkownicy uzyskali możliwość korzystania z rozwiązań inteligentnego domu od razu na komputerze. Wirtualny asystent Microsoftu, Cortana, wyświetli się na ekranie blokady, gotowy do pomocy użytkownikom. Cortana

Amazon, Apple, Google i Microsoft – czwórka gigantów dokłada wszelkich starań, by stworzyć nowe obszary na rozwijającym się rynku *smart home*.

będzie się łączyć z innymi aplikacjami, dzięki czemu komputer będzie miał funkcjonalność Google Home czy Amazon Echo. Firma stawia sobie za cel uczynić z Windows 10 centralę dla wszystkich podłączonych do sieci urządzeń w domu. Home Hub będzie wtedy stanowił uniwersalny panel kontrolny do sterowania domowym sprzętem. Microsoft pracuje także nad innymi aplikacjami dla Windows 10, które ułatwią komunikację z urządzeniami inteligentnego domu.

Gigant zachęca swoich partnerów OEM do rozwijania urządzeń kompatybilnych z Home Hub i Cortaną. Podobno trwają rozmowy z Lenovo i HP. Producent głośników Harman Kardón, którego właścicielem jest Samsung Electronics, zapowiedział udostępnienie w 2017 r. niewielkiego głośnika zdolnego do interakcji głosowej z Cortaną. Microsoft opublikował zestaw narzędzi programowania dla urządzeń Cortana (Cortana Devices SDK), aby zachęcić deweloperów do udostępniania urządzeń z zaimplementowaną usługą Cortana. SDK wspiera różne platformy, m.in. Windows IoT, Android i Linux. Oznacza to, że Cortana będzie mogła działać na sprzęcie nienależącym do Microsoftu, np. Apple TV czy urządzeniach z Androidem. Na horyzoncie inteligentnego domu nieustannie pojawiają się nowe rozwiązania. Pozostaje więc czekać na nowinki technologiczne roku 2017. ■

Zapowiada się walka gigantów, ale na razie trudno powiedzieć, kto uzyska dominację w świecie inteligentnego domu.

NASZE DANE

e-SPOŁECZNOŚĆ A PROBLEM OCHRONY DANYCH WRAŻLIWYCH

ROZWÓJ PRZESTĘPCZOŚCI W OBSZARZE DANYCH OSOBOWYCH CZ. 3

Marek Blim

Etapy rozwoju społecznego

Żyjemy w okresie dynamicznej zmiany stosunków społecznych wywołanych dostępnością do środków bezpośredniej komunikacji – w tzw. III fali rozwoju społeczeństwa. Przejście od rozproszonych grup zbieracko-myśliwskich do osiadłego społeczeństwa agrarnego¹⁾ zajęło kilkanaście wieków, a nawet obecnie część świata, np. regiony Afryki, zatrzymała się na tym etapie²⁾. Wynalezienie maszyny parowej przez Jamesa Watta w 1769 r. rozpoczęło II etap rozwoju społecznego – industrializację³⁾. Trwał on dwa stulecia, zastąpiony III etapem – informatycznym. W literaturze jest wiele propozycji wyznaczenia jego początku: rozwój techniczny i technologiczny po II wojnie światowej (od 1945 r.), wynalezienie pierwszego komputera (ABC – 1942 r.; ENIAC – 1943 r.), stworzenia podstaw internetu (konceptcja Paula Barana – 1962 r.) czy zdominowanie gospodarki przez sektor usług, gdy w 1968 r. po raz pierwszy przekroczyły one magiczną granicę 50% PKB w USA⁴⁾. Przykładem uzależnienia się od techniki informatycznej stała się kwestia dwucyfrowego zapisu roku w systemach komputerowych XX w. oraz przejścia przez datę 1 stycznia 2000 r. Żartobli-

wym odniesieniem do rozwoju społecznego człowieka jest rys. 1 (od małpy i *homo erectus* do *homo computerus*). Społeczeństwo III etapu rozwoju pojawi się wtedy, gdy podstawą funkcjonowania gospodarki stanie się informacja, a więc gdy człowiek uniezależni się od węgla, ropy i gazu jako nieodnawialnych źródeł energii. Szybki postęp techniczny jednocześnie zrewolucjonizował życie. Pojawiła się telewizja, telewizja cyfrowa, telefonia komórkowa, Internet, komputery osobiste. Możliwości technicznych nie można jednak przekładać na zmiany struktur społecznych. Wręcz przeciwnie, wydaje się, że postęp techniczny jest szybszy niż społeczne możliwości adaptacyjne. W konsekwencji pojawia się „podział cyfrowy”, który oznacza nie tylko dywersyfikację technicznych możliwości dostępu do informacji i nowych technologii, ale też możliwości ich codziennego wykorzystywania. Analfabetyzm informatyczny (niezdolność do korzystania z komputera, telefonu komórkowego, Internetu) może być taką samą przeszkodą w upowszechnianiu społeczeństwa informacyjnego jak niedostatecznie rozwinięta infrastruktura informatyczna. Nie należy również zapominać o dodatkowym czynniku – braku zainteresowania nowoczesnymi technologiami części obywateli, co nie zmienia faktu, że przez znaczny okres życia i tak są oni integralnie związani z systemami informacyjnymi (państwowymi

i środowiskowymi). Społeczeństwo nie w pełni postrzega rolę i nie zawsze rozumie znaczenie informacji jako waloru i zasobu materializującego się w obszarze codziennego funkcjonowania. Mamy za sobą pierwsze wojenne operacje informacyjne (Desert Storm – sierpień 1990 r.) i rozwijające się asymetryczne działania walki informatycznej⁵⁾ (Iran 2010 r. – wirus Stuxnet, użycie szkodliwego oprogramowania w PLC przeprogramowującego zainfekowane systemy automatyki przemysłowej). Trend ten przenosi się do obszarów i działań szkodliwych nie tylko w postaci przechwycenia czy zaboru informacji (kradzież tożsamości – cz. 2 cyklu, „a&s” nr 1/2017), ale także jako element rozpoznania socjotechnicznego atakowanej osoby (*spearphishing* – trojan BlackEnergy) w odniesieniu do jej stanowiska służbowego oraz posiadanych tajemnic przedsiębiorstwa⁶⁾. Przechwycenie chronionych informacji wrażliwych pozwala na manipulowanie zarówno nimi, jak i osobą, której one dotyczą.

Informacja według norm i ustawowe dane wrażliwe

Przedsiębiorca zajmujący się systemami ochrony fizycznej i technicznej coraz większą wagę powinien przykładać do przestrzegania sformalizowanych zapisów informacji: w umowie usługi, projekcie ochrony, dokumentacji powykonawczej i konserwatorskiej systemu, zwłaszcza gdy

jego działanie jest związane z zabezpieczeniem i ochroną zasobów informacji nie tylko biznesowych, ale także wrażliwych danych osobowych. Warto poznać definicje normatywne, by uniknąć ewentualnych nieporozumień.

Informacja (w ujęciu encyklopedycznym)

– dane przetworzone (poukładane, prze-filtrowane, pogrupowane itd.), by na ich podstawie można było wyciągać wnioski i podejmować decyzje biznesowe. Jest składnikiem aktywów (wartości) i musi być odpowiednio zabezpieczona. Informacja istnieje w wielu postaciach. Może być wydrukowana lub zapisana na papierze, przechowywana w formie elektronicznej, przesyłana pocztą lub za pomocą środków elektronicznych, pokazana na filmach i zdjęciach albo przekazywana słownie. Niezależnie od formy informacji i sposobów jej przetwarzania, przesyłania lub przechowywania powinna być ona zawsze odpowiednio zabezpieczona⁷⁾.

Przytoczone pojęcia mają charakter podstawowy, w praktyce natomiast są używane w różnym znaczeniu.

Informacja (pojęcie ogólne) – wiedza dotycząca obiektów, takich jak fakty, pojęcia, przedmioty, zdarzenia i dane (PN-I-02000:2002).

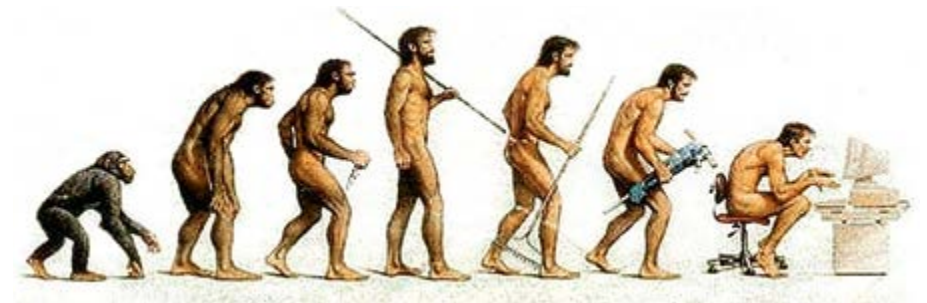
Informacja (w przetwarzaniu informacji) – wiedza o obiektach, takich jak fakty, pojęcia, przedmioty, procesy lub idee, zawierające koncepcje, o określonym znaczeniu w ustalonym kontekście (PN-ISO/IEC 2382-1:1996; PN-N-01602:1997).

Informacja (w teorii informacji) – wiedza redukująca lub usuwająca niepewność, dotycząca wystąpienia określonego zdarzenia z danego zbioru zdarzeń możliwych (PN-ISO 2382-16:2000).

Informacja wrażliwa – informacja, którą (jak ustalił właściwy organ) należy chronić, ponieważ jej ujawnienie, modyfikacja, zniszczenie lub utrata spowoduje zauważalną szkodę dla kogoś lub czegoś (PN-I-02000:2002).

Dane – reprezentacja informacji przedstawiona w sposób sformalizowany, dogodny do komunikowania się, interpretowania, przechowywania w pamięci lub przetwarzania (PN-ISO/IEC 2382-1:1996).

Dane (w przetwarzaniu informacji) – reprezentacja informacji mająca interpretację, właściwa do komunikowania się, interpre-



tacji lub przetwarzania (PN-ISO/IEC 2382-1:1996; PN-N-01602:1997).

Dane osobowe – wszelkie informacje dotyczące osoby fizycznej o ustalonej tożsamości albo dającej się zidentyfikować (PN-I-02000:2002).

Zbiór danych terminologicznych – zbiór danych zawierający informacje o pojęciach z zakresu określonych dziedzin (PN-ISO 1087-1:2004).

System informatyczny – system przetwarzania informacji oraz związany z nim ludzie oraz zasoby techniczne (sprzęt) i finansowe (środki), który dostarcza i rozprowadza informację (PN-ISO 2382-1:1996).

Atrybuty informacji – określone właściwości informacji, znaczące dla jej dalszego wykorzystania systemowego (PN-ISO/IEC 13335-1:1999; PN-ISO/IEC 27005:2010; PN-ISO Guide 73:2012; PN-ISO/IEC 27000:2014-11).

Atrybut bezpieczeństwa – informacja dotycząca użytkownika, podmiotu, zasobu i/lub obiektu określana przez funkcje bezpieczeństwa przedmiotu oceny, która jest wykorzystywana w celu zapewnienia realizacji polityki bezpieczeństwa przedmiotu oceny (PN-I-02000:2002).

Bezpieczeństwo informacji – zachowanie poufności, integralności i dostępności informacji; mogą być brane pod uwagę inne właściwości, np. autentyczność, rozliczalność, niezaprzeczalność i niezawodność (PN-ISO/IEC 27000:2014-11; PN-ISO/IEC 27001:2014-12; PN-ISO/IEC 27002:2014-12; PN-ISO/IEC 27005:2010).

System Zarządzania Bezpieczeństwem Informacji (SZBI) – część całościowego systemu zarządzania oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymania i doskonalenia bezpieczeństwa informacji (system zarządzania zawiera strukturę organizacyjną, polityki, planowane działania, zakresy odpowiedzialności, zasady,

procedury, procesy i zasoby) (PN-ISO/IEC 27001:2014-12).

Ponadto funkcjonuje wiele pojęć wynikających z przyjętych zobowiązań międzynarodowych (konwencje prawne i deklaracje ONZ), rozstrzygnięć ustawowych oraz rozporządzeń resortowych. Dane osobowe szczególnie chronione to – zgodnie z art. 27 ust. 1 ustawy z 27 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 2016 r. poz. 922) – zabronione do przetwarzania i podlegające odrębnym rygorom ochronnym:

- ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową,
- o stanie zdrowia, kodzie genetycznym, nałogach i/lub życiu seksualnym,
- dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Bezpieczeństwo danych to również zachowanie trzech podstawowych atrybutów informacji: poufności, integralności i dostępności, przy zapewnieniu niezawodności systemów użytych do jej przetwarzania.

Dane wrażliwe i ich systemy ochrony

Są definiowane zgodnie z ustawą o ochronie danych osobowych⁸⁾, ale należy także pamiętać o innych rozstrzygnięciach⁹⁾ firmowych i resortowych¹⁰⁾ oczekujących nas w trakcie posługiwania się własnymi danymi osobowymi zaliczanymi do grupy wrażliwych (umowa o pracę, postępowania mandatowe, administracyjne, karno-skarbowe itp.). Przedsiębiorca zajmujący się projektowaniem zabezpieczeń, ochroną fizyczną i techniczną oraz konserwacją systemów ochronnych/alarmowych powinien

⁷⁾ Na podstawie *Encyklopedia Gubernica*.

¹⁾ Pierwsze narzędzia wykorzystywane przy obróbce zbóż pochodzą sprzed 12,5 tys. lat (*Encyklopedia Britannica*).

²⁾ M. Luterek, *Zmiany w strukturze społecznej i modelu życia jednostki od społeczności opartych na łowiectwie i zbieractwie do społeczeństwa informacyjnego*, materiały Instytutu Informacji Naukowej i Studiów Bibliologicznych, Uniwersytet Warszawski, Warszawa 2005.

³⁾ B. Orłowski, *Technika*, Wydawnictwo Zakład Narodowy im. Ossolińskich, Wrocław-Warszawa-Kraków, 1999.

⁴⁾ J. Hreen, *Nowa era komunikacji*, wyd. Prószyński i S-ka, Warszawa 1999.

⁵⁾ M. Lakomy, *Cyberwojna jako rzeczywistość XXI wieku*, „Stosunki Międzynarodowe – International Relations”, rocznik 2011, nr 3-4.

⁶⁾ http://securelist.pl/blog/7348,ataki_apl_blackenergy_na_ukrainie_wykorzystuja_spearphishing_z_dokumentami_worda.html (dane Kaspersky Lab, 27.01.2016).

każdorazowo upewnić się co do wymagań zlecającego daną usługę oraz szczegółowego przeznaczenia chronionego zasobu, pomieszczenia czy obiektu. Szczególną uwagę należy zwrócić na pomieszczenia przeznaczone do długotrwałego (B50) przechowywania dokumentacji niearchiwalnej zawierającej dane osobowe:

- dokumentacja finansowa – rachunki i faktury osób fizycznych – okres BE5 od zakończenia roku finansowego, w którym zostały zbilansowane (5 lat wg art. 74 ustawy o rachunkowości)¹⁰;
- dokumentacja administracyjno-odszkodowawcza: protokoły powypadkowe, postępowania odszkodowawcze – okres BE3/BE10 (art. 118 kodeksu cywilnego)¹²;
- dokumentacja pracownicza – 50 lat (B50) od zakończenia przez ubezpieczonego pracy u danego płatnika (dotyczy okresów zatrudnienia i wynagrodzenia za pracę oraz innych dokumentów, na których podstawie następuje ustalenie podstawy wymiaru emerytury lub renty), co wynika z art. 125a ust. 4 ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych¹³. Identyfikacyjny okres przechowywania – B50 – obowiązuje w stosunku do akt osobowych, co wynika z art. 51u ustawy o narodowym zasobie archiwalnym i archiwach¹⁴. W grupie dokumentacji pracowniczej należy wymienić dokumentację związaną z bezpieczeństwem i higieną pracy – zgodnie z kodeksem pracy¹⁵ dokumentację związaną z wypadkami zbiorowymi, śmiertelnymi i powodującymi inwalidztwo należy przechowywać 25 lat (B25), związaną z innymi wypadkami – 10 lat (B10). Analizę wypadków i chorób zawodowych należy przechowywać 10 lat (B10). Obie analizy zawierają (wg uodo¹⁶) wrażliwe dane osobowe.

Ze względu na poufność zbiorów danych osobowych i związanych z nimi dokumentów (ich nośników) należy zwrócić uwagę na funkcjonowanie systemów ochrony – w okresie pozostawiania zbioru bez nadzoru osobowego uprawnionego personelu, tzn. w czasie długotrwałego przechowywania w magazynie bądź składnicy akt danego przedsiębiorstwa. Warto zapoznać się z wymaganiami zawartymi w Rozporządzeniu Prezesa Rady Ministrów z 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów

akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz.U. z 2011 r., nr 14, poz. 67) obowiązującymi administrację publiczną (państwową i samorządową), ale zarazem przydatną dla osób odpowiedzialnych za organizację i przechowywanie zbiorów danych.

Telemedycyna i e-zdrowie

Hermeticznosc wiedzy medycznej w kulturze Zachodu i powszechnosc wiedzy medycznej w społeczeństwie polskim powodują zróżnicowane odniesienia do potrzeby zarządzania wiedzą medyczną w warunkach e-społeczeństwa XXI wieku. W praktyce mamy sytuację, gdy rozwój ICT (*Information & Communication Technology*) staje się fundamentem zarządzania wiedzą w sektorze opieki zdrowotnej, gdyż to dzięki nowoczesnej technologii i poprawnej organizacji systemowej¹⁷ można z tych zasobów w pełni korzystać. Ze względu na wrażliwość danych medycznych ich zbieranie, wykorzystywanie i przechowywanie podlega szczególnej ochronie. Należy wyjaśnić, z czym współcześnie jest kojarzone pojęcie telemedycyna i „o co chodzi” w jej żywiołowym rozwoju w Polsce, istota tej sprawy bowiem tylko w części leży po stronie lekarzy. Funkcjonuje wiele definicji telemedycyny. Najprostsza określa ją m.in. jako praktykę lekarską oraz edukację medyczną odbywającą się za pośrednictwem interaktywnej komunikacji wykorzystującej teleinformatyczne urządzenia przesyłające dźwięk i obraz, a nie poprzez bezpośrednią fizyczną interakcję lekarz – pacjent. Polega na przesyłaniu danych medycznych przez sieć telekomunikacyjną czy teleinformatyczną z miejsca, gdzie zostały one uzyskane (np. klinika) lub są składowane (np. baza danych) do miejsca, gdzie zostaną poddane analizie (np. w celu diagnostycznym), jak również na przesyłaniu ich w kierunku odwrotnym (np.

przeprowadzanie operacji na odległość). Zastosowanie narzędzi telemedycznych przyspiesza postawienie diagnozy, gdy dostęp do specjalisty w danej dziedzinie jest utrudniony. Ponadto jest jedną z mniej kosztownych i oszczędnych czasowo metod monitorowania pacjentów na potrzeby prewencji. Nadaje się do archiwizacji i przepływu danych medycznych. Najbardziej szeroką kategorią związaną z usługami telematycznymi, czyli łączącymi technologie obliczeniowe z technologiami komunikacyjnymi, jest teleZdrowie i eZdrowie (*telehealth, eHealth*) – zdalna prewencja i leczenie chorób oraz zdalna opieka medyczna (*telecare*) lub wszelkie działalności informacyjne, diagnostyczne, konsultacyjne, terapeutyczne i naukowe związane z przesyłaniem obrazu, dźwięku i innych danych elektronicznych związanych z problematyką zdrowia, określane ogólnie terminem e-zdrowie. Wprowadzając systemy ochrony technicznej (szczególnie bezprzewodowe), należy się upewnić, czy pasma i wielkości sygnałów ICT nie zakłóca pracy urządzeń telemedycznych istotnych dla życia oraz zdrowia pacjenta.

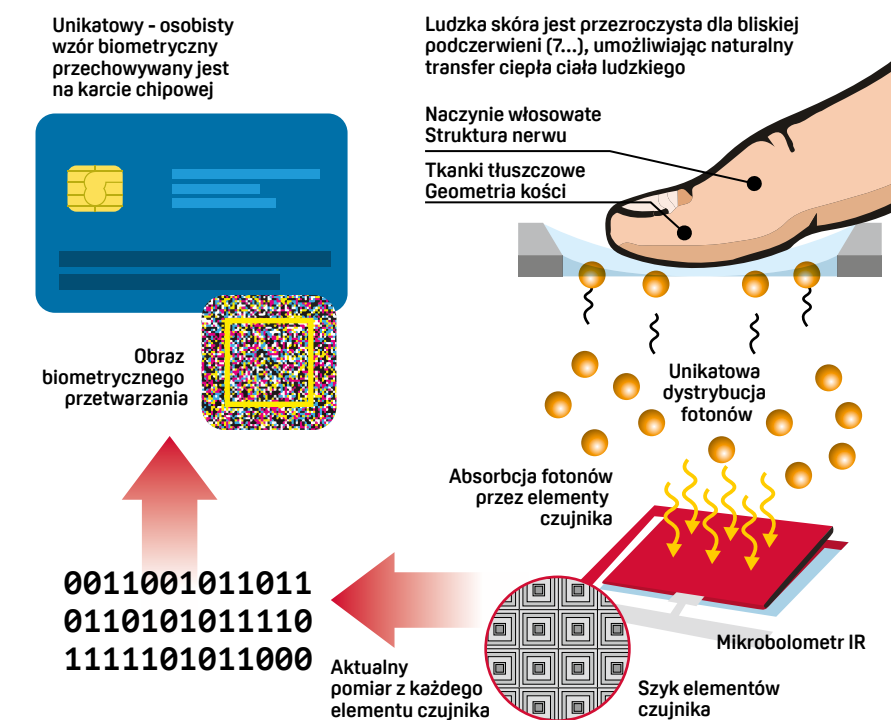
Ochrona danych w systemach dostępu

Rozporządzenia Unii Europejskiej powodują, że do 24 maja 2018 r. obowiązuje *va-catio legis* dokumentu UE nr 679/2016 z 27 kwietnia 2016 r.¹⁸ określonego jako RODO/GDPR (Rozporządzenie o Ochronie Danych Osobowych/*General Data Protection Regulation*). Dokument ten kończy prace nad doskonaleniem zasad ochrony mających istotne znaczenie dla Europejskiego Obszaru Gospodarczego, szczególnie w kwestii ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia obowiązującej dy-

BIOMETRA

cechy fizyczne					cechy behawioralne
linie papilarne	kształt	tęcza	struktura naczyń	twarz	podpis
palce, kostki, dłoń	dłoń, ucho		palce, dłonie, siatkówka	wykorzystanie kamer monitoringu wizyjnego	motoryka
				urządzenia z kamerą na podczerwień	głos

Rys. 2. Cechy osobowe wykorzystywane w biometrii systemów ochrony



Rys. 3. Przeniesienie wzorca biometrycznego na nośnik indywidualny (security ID Card)



Rys. 4. Analiza obrazu żył napięstka w ramach technik biometrycznych w systemach KD

rektywy 95/46/WE Ogólne rozporządzenie o ochronie danych (art. 99 ust. 2 RODO/GDPR wyznacza termin promulgacji aktu na 25 maja 2018 r.). Przedsiębiorca zajmujący się projektowaniem zabezpieczeń, ochroną fizyczną i techniczną oraz konserwacją systemów ochronnych i alarmowych opartych na biometrii powinien przeanalizować art. 4 ust. 14 RODO/GDPR definiujący „dane biometryczne” jako dane osobowe (takie jak wizerunek twarzy lub dane daktylo-

skopijne), które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjonomicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby. Oznacza to, że groma-

Tabela skuteczności technologii biometrycznych stosowanych w SKD/ESKK

TECHNOLOGIA	U	T	M	W	O
odciski palców	++	++	0	+	++
tęcza	++	++	+	++	++
siatkówka	++	+	--	++	++
DNA	++	++	--	++	--
geometria ucha	+	++	0	0	0
geometria dłoni	+	0	++	0	0
podpis (styl i dynamika)	0/+	--	0/++	0	--/+
twarze	-	-	++	-	0
głos	-	-	++	--	+
naczynia (palec)	++	++	-	++	++
wielomodalna (wideo)	0	-	++	+	++

dzone na potrzeby SKD lub ESKK dane biometryczne użytkowników tych systemów od 25 maja 2018 r. muszą być szczególnie chronione jako wrażliwe i poufne dane osobowe pod rygorem odpowiedzialności, zgodnie z wymogami zawartymi w rozdz. II, art. 9 RODO/GDPR. Niektóre dane można powierzyć zainteresowanemu, np. zapis na chipie przepustki (rys. 3), choć zbiory danych biometrycznych należy przechowywać w LCN/SMA.

W przypadku zapewnienia dużej przepustowości systemu kontroli dostępu wykorzystuje się np. systemy analizy żył napięstka (rys. 4) wymagające szybkiego dostępu do licznej bazy danych wzorcowych uzależnionych od użytej technologii (tab. 5), chronionych w ramach bazy w LCN/SMA. W art. 42 RODO Unia Europejska zachęca do dobrowolnej certyfikacji wprowadzonych systemów bezpieczeństwa w ramach audytu ochrony danych przez krajowe akredytowane (art. 43 ust. 1 pkt b) jednostki certyfikujące¹⁹, co ma potwierdzić wzmocnienie kontroli podmiotu nad własnymi danymi oraz promować wdrażanie mechanizmów zwiększających ochronę prywatności (tzn. *privacy by design* – na etapie projektowania – oraz *privacy by default* – jako ustawienia domyślne). Wnikliwe zapoznanie się przedsiębiorcy z treścią RODO/GDPR pozwoli na uniknięcie wielu kłopotliwych sytuacji. ■

¹⁰ <https://uodo.pl/dane-wrażliwe/wykładnia-GIODO-z-dnia-21.07.2014>.

¹¹ Art. 22 ustawy Kodeks Pracy (Dz.U. z 2014 r. poz. 1502 z późn. zm. – ostatnia Dz.U. 2016 r. poz. 1053).

¹² Zarządzenie Ministra Sprawiedliwości z dnia 27 czerwca 2012 r. w sprawie Polityki Bezpieczeństwa Informacji w Ministerstwie Sprawiedliwości i sądach powszechnych (Dz.Ur. MS z 2012 r. poz. 93).

¹³ Ustawa o rachunkowości z dnia 29 września 1994 r. (Dz.U. z 2013 r. poz. 330 z późn. zm. – ostatnia Dz.U. z 2016 r. poz. 615).

¹⁴ Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. z 2016 r. poz. 380 z późn. zm.).

¹⁵ Ustawa z dnia 17 grudnia 1998 r. o emeryturach i rentach z FUS (Dz.U. z 2015 r. poz. 248 z późn. zm.).

¹⁶ Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2015 r. poz. 1446 z późn. zm. – stan na 2017-02-20, Rdz. 4b, art. 51u) oraz orzecznictwo NSA).

¹⁷ Ustawa Kodeks pracy (Dz.U. z 2014 r. poz. 1502 z późn. zm. – ostatnia zmiana Dz.U. 2016 r. poz.1053).

¹⁸ Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922).

¹⁹ A. Frąckiewicz-Wronka, A. Austen, *Od zarządzania informacją do tworzenia wiedzy – zastosowanie ICT w organizacjach sektora zdrowotnego*.

Z. Wróbel (red.), *Zarządzanie i technologie informacyjne. Technologie informacyjne w medycynie*, t. 3. Wydawnictwo Uniwersytetu Śląskiego, Katowice 2006, s. 53–82.

¹⁸ Euro-Lex, edycja polska OJEU z 4.05.2016, poz. L119/1.

¹⁹ Wymagania normy PN-EN ISO/IEC 17065:2013-03

NIE DAJ SIĘ PODSŁUCHAĆ

W BEZPIECZNYM MIEŚCIE

Po każdym zamachu terrorystycznym w Europie czy na świecie specjaliści jak mantrę powtarzają, co powinno się robić w przypadku ataku. Oczywiście zagrożeń terrorystycznych nie wolno bagatelizować, ale na szczęście żyjemy w kraju, który nie został zaatakowany. Dlatego chciałbym, w myśl zasady „koszula bliższa ciału”, skupić się na innych zagrożeniach, z jakimi spotykamy się na co dzień. To ważne, gdyż mogą nam czy naszej firmie przynieść katastrofalne skutki.

Sebastian Błażkiewicz
prezes SASMA Europe

Nie tak dawno, realizując pewien projekt, przez kilka miesięcy podróżowałem PKP na linii Warszawa-Kraków-Warszawa. Starałem się przy okazji tych podróży wybierać tzw. otwarte przedziały. Trudno się tam nudzić, słysząc różne opowieści. Nie trzeba się specjalnie starać, by (zwłaszcza od pracowników korporacji) uzyskać informacje. Wystarczy słuchać, by dowiedzieć się o:

- kondycji finansowej firmy,
- zarządzie firmy,
- prowadzonych rozmowach czy negocjacjach (ze szczegółami strategii),
- przygodach towarzyskich,
- hasłach do laptopów (wpisywanych publicznie),
- innych problemach, także prywatnych.

Należy wyraźnie podkreślić, że konkurencja uwielbia takie środowisko jak pociąg. Płaci duże pieniądze firmom doradczym z mojej branży, by zdobywać informacje, które mogą

mieć duży wpływ na ich biznes. Nadal dla większości Polaków brzmi to wirtualnie, ale informacja stała się dzisiaj dobrem, za które płaci się potężne pieniądze. Kolejny przykład – warszawiancy na pewno wiedzą, gdzie leży tzw. Mordor – dzielnica biznesowa w okolicy Galerii Mokotów. Wystarczy wybrać się w porze lunchu do okolicznych barów i słuchać... Dowiemy się tam wszystkiego na temat interesujących nas firm. A gdy trochę „pociągniemy za język”, to nawet uda się nam zdobyć dane o wartościach milionów euro w ciągu 30 minut. W cenie spaghetti carbonara... Opisane przykłady pokazują typowe wyzwania, przed jakimi stawiają nas ośrodki miejskie czy komunikacja zbiorowa. Kierujące się modą firmy i korporacje wydają znaczne kwoty na szkolenia antyterrorystyczne, a zapominają o czymś, co może je doprowadzić na skraj przepaści.

Kierujące się modą firmy i korporacje wydają znaczne kwoty na szkolenia antyterrorystyczne, zapominając o zagrożeniach, które mogą je doprowadzić na skraj przepaści.

Kolejny przykład wyzwań miejskich w aspekcie bezpieczeństwa biznesu – socjotechnika. Zdradzę pewien scenariusz – nie odkrywczy, ale działający niezawodnie od lat. Wystarczy wejść do biurowca, w którym mieści się nasz cel, i w męskiej toalecie zostawić jakiś świetnie wyglądający pendrive. Ponieważ 99% mężczyźni to miłośnicy gadżetów, jest duże prawdopodobieństwo, że „szczęśliwy” znalazca będzie chciał go szybko sprawdzić, podłączając do komputera w firmie, a wtedy... zyskujemy prawie nieograniczony dostęp do komputera i sieci interesującej nas firmy. Przykłady scenariuszy można by mnożyć. Przeprowadzając

fizyczne testy penetracyjne na zlecenie klientów, wielokrotnie udowadniamy, że nie trzeba wysublimowanych metod, by zdobyć interesujące informacje. Zdaję sobie sprawę, że opisane „zagrożenia miejskie” są trochę inne niż te, do których przywykliśmy – mam na myśli terroryzm czy też przestępczość przeciwko mieniu. Jednak porównajmy skutki dwóch zdarzeń:

- kradzież portfela (częsta w mieście) – tracimy dokumenty, pieniądze i karty. Pomijając stratę pieniędzy (raczej nikt nie nosi już dużych sum), stracimy głównie czas na blokowanie kart, zastrzeganie starych dokumentów, a także wyrabianie nowych;
- zdobycie informacji na temat romansu dyrektora finansowego firmy X (np. w sytuacji opisanej powyżej, tzn. w pociągu). Pan dyrektor prawdopodobnie

nie będzie chciał, by ujawniono jego rodzinie szczegóły i zgodzi się na współpracę. Dzięki temu firma Y, główny konkurent firmy X, będzie miała zapewnioną przewagę informacyjną na lata.

W mieście może nas dopaść jeszcze wiele innych zagrożeń, które mogą mieć duży wpływ na nasz biznes. Chciałem jednak zaszczylić w czytelnikach pewną myśl, by kierowali się zdrowym rozsądkiem, a nie modą. Wprost nie mogłem się nadszwić, gdy pewna duża firma poprosiła mnie o szkolenie, które miało polegać tylko na ochronie przed tzw. *active shooter* i sytuacjami zakładniczymi (jakby były one w Polsce na porządku dziennym). Na moje pytanie o inne problemy stwierdzono, że nie są one „trendy”, a pracownicy chcą się poczuć jak w filmie. Na zakończenie – warto po prostu przestać kierować się modą, a włączyć zdrowy rozsądek, bo miasto jest znakomitym środowiskiem, w którym na ludzi biznesu czeka mnóstwo zagrożeń. ■

BIO

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



PIERWSZE TAKIE WYDANIE
NA RYNKU POLSKIM

NOWOCZESNE I PRAKTYCZNE SPOJRZENIE
DOŚWIADCZONYCH EKSPERTÓW

POZNAJ WYZWANIA BRANŻY
BEZPIECZEŃSTWA BIZNESU

Więcej informacji na stronie www.sas-ma.org

**Bezpieczeństwo
biznesu
w XXI wieku**

PRACA ZBIOROWA

INCYDENTY WYBUCHOWE W OBSZARACH MIEJSKICH

W miastach w Polsce mieszka ponad 23 mln ludzi, gęstość zaludnienia w nich natomiast przekracza 1000 osób na km². Społeczność miejska jest bardziej narażona na zagrożenia o charakterze masowym: wydarzenia związane z materiałem wybuchowym czy groźby jego użycia, które potencjalnie zagrażają życiu i zdrowiu wielu osób.

Tomasz Goleniowski

Istotna z punktu widzenia zapobiegania zagrożeniom i ograniczania ich skutków jest świadomość ich wystąpienia. Improvizowane urządzenia wybuchowe, zwane też „bombami”, zawierają materiał wybuchowy oraz elementy inicjujące wybuch. Nie sposób opisać, jak wygląda „bomba”, gdyż jej rodzaj, działanie, wielkość i stopień zaawansowania technologicznego są wypadkową wielu czynników. Do najważniejszych należą: budżet, jakim dysponuje jej konstruktor, jego możliwości intelektualne, dostęp do tech-

nologii, przeszłość, wykształcenie, wykonywany zawód itd. Konstruktor czy też sprawca podłożenia „bomby” decyduje o sposobie użycia urządzenia – czy będzie ono sterowane radiowo, przewodowo, czy też uruchamiane przez ofiarę (pułapka), zostanie podłożone pod samochodem czy może przymocowane do komercyjnego drona i rzucone w konkretnym miejscu, np. podczas imprezy masowej w plenerze. Improvizowane urządzenie może znajdować się w plecaku (Madryt 2004 r.), w torbie na zakupy (Sosnowiec 2010 r.) lub w garnku (Wrocław 2016 r.) bądź umieszczone na drzewie (Sosnowiec 1959 r.) – wszystkich możliwych scenariuszy nie sposób przewidzieć.

Potencjalną ofiarą może być każdy. Moje wieloletnie obserwacje wskazują, że nawet gdy sprawca podłożenia „bomby” wybrał konkretną ofiarę, często w wybuchu były też poszkodowane inne osoby znajdujące się w pobliżu. Wybuch urządzenia wybuchowego nigdy nie ma skutku lokalnego – bomba rurowa wypełniona stosunkowo słabym prochem czarnym może skutecznie rażać w promieniu 200 m. Odnotowywano przypadki, gdy „bombę” przeznaczoną dla konkretnej osoby uruchamiała inna osoba – sąsiad czy członek rodziny (Myszków 2008 r.). Dobór ofiar wybuchu może też być przypadkowy. Motywem tego rodzaju działań bywa m.in. chęć zwrócenia na siebie

uwagi czy zastraszenie świadka. Niektórzy sprawcy cierpią na zaburzenia psychiczne, a wtedy trudno mówić o konkretnym motywie. Jak zapobiegać zagrożeniom związanym z „bombami”? Należy mieć świadomość, że „bomba” i wybuch nie są narzędziem jedynie terrorystów. Używają ich także pospolic przestępcy, a materiał wybuchowy nietrudno pozyskać lub wyprodukować. W 2016 r. policja zabezpieczyła w Polsce 1570 kg materiałów wybuchowych w związku z nielegalnym ich posiadaniem (CBŚP). Motyw działania przestępcy może być przyziemny, wręcz banalny, a czasem niezrozumiały. W 2016 r. zanotowano w Polsce 28 wybuchów ma-

teriałów i urządzeń wybuchowych, zginęło siedem osób, a piętnaście zostało rannych (CBŚP). Jednym z działań, które może zminimalizować skutki potencjalnego ataku bombowego, jest uświadamianie społeczeństwu powszechności takich zjawisk, konieczności i sposobów reagowania na zagrożenia związane z porzucenymi w przestrzeni miejskiej przedmiotami o niewiadomym pochodzeniu. Informacja o podłożeniu materiału lub urządzenia wybuchowego jest bardzo często notowanym incydentem związanym z materiałami wybuchowymi. Niewiele osób zastanawia się nad tym, dlaczego sprawca miałby informować osobę, czy instytucję o podłożeniu „bomby”. Wydaje się to nielogiczne. Sprawca, który informuje o podłożeniu, ryzy-

kuje, że jego plan spali na panewce, a „bomba” zostanie zabezpieczona przez policję i dostarczy niezbędnych śladów umożliwiających identyfikację konstruktora. By wyjaśnić to zjawisko, należałoby się przenieść do Wielkiej Brytanii i cofnąć do połowy lat 90. XX wieku. W trakcie walki IRA o przyłączenie Irlandii Północnej do Irlandii „bomba” była dość popularnym narzędziem. W wybuchach, oprócz żołnierzy i policjantów, ginęli także przypadkowi ludzie. Powodowało to spadek poparcia społecznego dla IRA. Dlatego organizacja zmieniła taktykę prowadzenia walki. Nadal podkładano „bomby”, jednak w większości przypadków kilkanaście minut przed wybuchem informowano o jej podłożeniu. Ten czas wystarczał do ewakuacji osób z zagrożonego obiektu. Ewakuacja oraz wybuch i zniszczenie miały być wystarczającą demonstracją siły. Nie wiadomo kiedy plaga powiadomień, głównie fałszywych, pojawiła się w Polsce. Każde z nich należy jednak traktować poważnie, a potwierdzanie lub wykluczanie zagrożenia pozostawić służbom. Motywów działania po-

Należy mieć świadomość, że „bomba” i wybuch nie są narzędziem jedynie terrorystów. Używają ich także pospolic przestępcy.

tencjalnego sprawcy jest tak dużo, że nie można z góry zakładać, iż to wybryk lub głupi żart. Polskie prawo nie dopuszcza angażowania pracowników (w tym ochrony) zaatakowanego obiektu do poszukiwań urządzenia wybuchowego. Ci, którzy zostali dotknięci takim incydentem, zetknęli się na pewno z tzw. rekomendacją CBŚP – ewakuować lub nie ewakuować. Rekomendacja ta nie jest wiążąca i opiera się na aktualnie posiadanych przez policję informacjach operacyjnych, a te nie zawsze są wyczerpujące. Mimo rekomendacji odpowiedzialność za bezpieczeństwo obiektu i znajdujących się w nim osób spoczywa bezpośrednio na administratorze. W ub.r. w Polsce odnotowano 391 fałszywych powiadomień, a fałszywym alarmem zostało objętych 1949 obiektów (CBŚP). Wskazane jest więc szkolenie personelu, by posiadał umiejętność odbierania informacji (telefon, e-mail, przesyłka listowa) oraz przekazania jej przełożonym i służbom. Zniszczenie lub zniekształcenie informacji może skutkować brakiem możliwości ustalenia sprawcy i udowodnienia mu winy, a brak kary za wybryk – spowodować eskalację zachowań, nie wspominając o innych sprawach, jak zwrot kosztów ewakuacji, zatrzymanie procesów technologicznych czy też rekompensata strat w zaatakowanym obiekcie. Najczęstsze błędy w trakcie odbierania takiej informacji wynikają z braku elementarnej wiedzy.

Mimo obowiązku rejestracji numerów *pre-paid* większość informacji o podłożeniu „bomby” nadal jest przekazywana przez telefon. W przeciwieństwie do listu czy e-maila treść rozmowy jest ulotna, łatwo ją zniekształcić lub pominąć bardzo istotne elementy, dlatego warto wrócić do nieco już zapomnianego „formularza dla osoby odbierającej rozmowę o podłożeniu bomby”. Pomaga on uporządkować przebieg rozmowy oraz zapisać najważniejsze informacje – cechy głosu osoby informującej, głosy w tle, płęć. Może stać się samodzielnym dowodem procesowym, odciążając w dużym stopniu osobę odbierającą rozmowę. Przykładem jest fałszywe powiadomienie o podłożeniu „bomby” na lotnisku w Modlinie w marcu 2016 r. Osoba, która odebrała informację telefoniczną, nie dysponowała formularzem. Po ustaleniu sprawy i postawieniu zarzutów główny świadek miał trudności z opisaniem „z pamięci” najważniejszych cech głosu podejrzanego, co w dużym stopniu utrudniło ustalenie istotnych dla sprawy faktów. Zagrożeń związanych z materiałami wybuchowymi i wybuchami w przestrzeni miejskiej jest więcej. Do częstych należą włamania do bankomatów, niewybuchy i niewypały znajdowane w trakcie prac budowlanych czy remontowych lub ujawniane przez policję w związku z nielegalnym posiadaniem. Zagrożenie stanowi obrót i używanie wyrobów pirotechniki widowiskowej, a także wybuchy mieszanin gazów palnych z powietrzem. ■

Tomasz Goleniowski od 20 lat zajmuje się zagrożeniami związanymi z materiałami i urządzeniami wybuchowymi. Był m.in. technikiem bombowym w policji oraz członkiem Zespołu ds. Zwalczania Aktów Terroru Kryminalnego KWP w Katowicach. Obecnie prowadzi firmę EOD TECH.

Spóźniona nowelizacja

Od wejścia w życie rozporządzenia Rady Ministrów z 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz.U. z 2012 r., poz. 683) **środowisko technicznej ochrony osób i mienia polskiej branży security ten akt prawa powszechnego traktowało – łagodnie mówiąc – ambiwalentnie. Litera i duch tego rozporządzenia są skomplikowane i mało komunikatywne, zatem trudne w praktycznym stosowaniu. Nie dziwi więc, że zwłaszcza w środowisku pracowników zabezpieczenia technicznego było ono krytykowane.**



Marek Ryszkowski

Oniedostatkach rozporządzenia pisa-
sano obszernie na łamach prasy
branżowej, m.in. w „Systemach
Alarmowych”, poprzedniku obecnego
dwumiesięcznika „a&s Polska”. Po-
wszechnie też postulowano jego dogłęb-
ną nowelizację lub zastąpienie go nowym,
które w przystępnej, komunikatywnej for-
mie i treści regulowałoby zasady doboru
środków bezpieczeństwa fizycznego sto-
sowanych do zabezpieczenia informacji

niejawnych przed nieuprawnionym dostę-
pem do nich osób nieupoważnionych.
Spodziewano się, że pod presją krytyki
i postulatów zostanie opracowana nowe-
ła rozporządzenia, które w dość zawiły
sposób regulowało problemy ochrony fi-
zycznej szczególnego rodzaju informacji
– ściśle tajnych, tajnych, poufnych i za-
strzeżonych – o których mowa w ustawie
z 5 sierpnia 2010 r. o ochronie informa-
cji niejawnych (Dz.U. z 2016 r., poz. 1167
– tekst jednolity z późn. zm.). Rozporzą-
dzenie nowelizacyjne istotnie przygo-
towano i wprowadzono jako rozporzą-
dzenie Rady Ministrów z 22 lutego 2017 r.

(Dz.U. z 13 marca 2017 r., poz. 522). We-
szło ono w życie, zgodnie z brzmieniem
jego § 2, z dniem 28 marca 2017 r. Jednak
nowelizacja ta nie spełnia oczekiwań za-
interesowanych nią środowisk polskiej
branży security. Twórcy zmienionego rozporządzenia
przedstawili jego projekt do rozpatrze-
nia na forum Rady Ministrów RP z uza-
sadnieniem, które w artykule przy-
taczam w oryginalnym brzmieniu dla
odróżnienia od tekstu autorskiego ze
względu na ubogą polszczyznę jego tek-
stu (składnia i interpunkcja) oraz żargon
urzędniczy.

Uzasadnienie

Polski Komitet Normalizacyjny w dniu 29 października 2014 r. wycofał ze zbioru norm normę PN-EN 50133-1:2007 – Systemy alarmowe – Systemy kontroli dostępu w zastosowaniach dotyczących zabezpieczenia – Część I. Wymagania systemowe. Norma była przywołana w załączniku 2 do rozporządzenia Rady Ministrów z dnia 29 maja 2012 roku w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz.U. poz. 683). Wycofana wyżej wspomniana norma PN-EN 50133-1:2007 została zastąpiona nową normą PN-EN 60839-II-1:2014-1 – Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część II-1: Elektroniczne systemy kontroli dostępu – Wymagania dotyczące systemów i części składowych. W związku z tym należało dokonać nowelizacji przedmiotowego rozporządzenia. Z uwagi na fakt, iż nowa norma PN-EN 60839-II-1:2014-1 ma inną konstrukcję niż wycofana norma PN-EN 50133-1:2007, zaproponowano nowelizację przedmiotowego rozporządzenia poprzez opisowe określenie wymogów technicznych stawianych systemowi kontroli dostępu stosowanemu do zabezpieczenia informacji niejawnych (§ 4 ust. 5a i 6) oraz nowelizację załącznika 2 do projektowanego rozporządzenia. W toku prac nad projektem rozporządzenia nie wpłynęły zgłoszenia zainteresowanych pracami nad projektem, o których mowa w art. 7 ustawy z dnia 7 lipca 2005 r. o działalności lobbingsowej w procesie stanowienia prawa (Dz.U. z 2005 r., nr 169, poz. 1414 ze zm.). Przedmiot projektowanej regulacji pozostaje poza zakresem prawa Unii Europejskiej. Projekt rozporządzenia nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych, ponieważ nie zawiera przepisów technicznych. Przedmiotowy projekt rozporządzenia nie był przedstawiany instytucjom i organom Unii Europejskiej lub Europejskiemu Bankowi Centralnemu celem uzyskania opinii, dokonania konsultacji albo uzgodnienia, ponieważ przepisy przedmiotowego projektu rozporządzenia pozostają poza zakresem prawa UE. Zgodnie z § 52 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów (M.P. z 2015 r., poz. 1063 oraz z 2016 r., poz. 494) projekt jest udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Pierwsze opinie o przeprowadzonej nowelizacji rozporządzenia z 2012 r. nie są oczywiście związane z jej skutkami dla funkcjonowania polskiej branży security, ponieważ normalizacja zbyt krótko funkcjonuje w obiegu prawnym, lecz z tym, że nie spełnia oczekiwań tych, którzy prowadząc swój biznes, muszą kierować się dyspozycjami znowelizowanego rozporządzenia. Rekapitulu-
jąc pierwsze opinie, można obrazowo stwierdzić „z dużej chmury mały deszcz”, rozporządzenie nowelizacyjne nie usuwa bowiem mankamentów rozporządzenia nowelizowanego, które nadal pozostaje skomplikowane i mało komunikatywne, zatem trudne w praktycznym stosowaniu.

Przedstawiam istotne fragmenty rozporządzenia nowelizacyjnego opatrzone laconicznymi komentarzami pozyskanymi od przedstawicieli sektora technicznej ochrony osób i mienia polskiej branży security. Szczegółowy komentarz do treści całego rozporządzenia będzie mógł być opublikowany na łamach „a&s” nie wcześniej niż co najmniej kilka miesięcy od jego wejścia w życie 28.03.2017 r. Wymaga to bowiem dogłębnej analizy rozporządzenia oraz oceny znaczenia i skutków nowych regulacji dla ich praktycznego stosowania w działalności pracowników zabezpieczenia technicznego, a także po zebraniu przez nich doświadczeń i ocenie kosztów wynikających ze stosowania praktycznego nowych regulacji.

Treść preambuły i § 1. rozporządzenia nowelizacyjnego.

„Na podstawie art. 47 ust. 1 i 3-6 ustawy z 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. z 2016 r., poz. 1167) zarządza się, co następuje:

§ 1. W rozporządzeniu Rady Ministrów z 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz.U. poz. 683) wprowadza się następujące zmiany:

- 1) w § 4:
 - a) po ust. 5 dodaje się ust. 5a w brzmieniu:
5a. Elektroniczne systemy pomocnicze wspomagające ochronę informacji niejawnych należy wykonywać zgodnie z zasadami sztuki inżynierskiej i aktualnym poziomem wiedzy technicznej, opisanym w szczególności w odpowiednich (których? – podkr. autora) Polskich Normach.
 - b) ust. 6. otrzymuje brzmienie:
6. Elektroniczne systemy pomocnicze wspomagające ochronę informacji niejawnych powinny posiadać wydane przez dostawcę, z uwzględnieniem przepisów o systemie oceny zgodności, poświadczenia zgodności z wymogami określonymi w rozporządzeniu.
- 2) w załączniku nr 2 do rozporządzenia:
 - w Części I pkt 10 uchyla się tiret piąte,
 - w Części III tabela „KATEGORIA K4: Kontrola dostępu. Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu” otrzymuje brzmienie określone w załączniku.

PREZES RADY MINISTRÓW”

Zmiany w załączniku nr 2 do nowelizowanego rozporządzenia wynikają z wycofania Polskiej Normy, o której mowa w cytowanym wyżej uzasadnieniu. Uchylenie tiretu piątego, o którym mowa w § 1 pkt 2a) rozporządzenia nowelizacyjnego to nic innego jak wykreślenie uchylonej Polskiej Normy z katalogu siedmiu norm wskazanych do stosowania w rozporządzeniu nowelizowanym. Nowej normy w miejsce usuniętej nie wpisano, zatem w tym katalogu pozostało nadal sześć Polskich Norm wymienionych pierwotnie w jego treści.

Treść zmian w załączniku nr 2, o których mowa w § 1 pkt 2b, przedstawiono w dolnej części tabeli. Poprzednie brzmienie tego fragmentu rozporządzenia nowelizowanego umieszczono w części górnej. Pozwoli to lepiej zobrazować skalę i głębię dokonanych zmian.

ZAŁĄCZNIK NR 2 DO ROZPORZĄDZENIA NOWELIZOWANEGO
Kategoria K4: Kontrola dostępu. Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu (brzmienie przed nowelizacją).
Typ 4. Punktacja – 4 pkt Elektroniczny automatyczny system kontroli dostępu o następujących cechach: 1) spełnia co najmniej wymagania systemu w klasie rozpoznania 3, a w klasie dostępu B – określone w normie PN-EN 50133-1; 2) jest to automatyczny system zapewniający właściwy stopień ochrony, wymagający jedynie minimalnego nadzoru przez personel bezpieczeństwa; 3) jest stosowany w połączeniu z barierą dostępu uniemożliwiającą powrót, działającą na zasadzie uniemożliwiającej otwarcie danego przejścia kontrolowanego, jeżeli wcześniej nie nastąpiło wyjście ze strefy, do której zamierza się wejść, bądź bez uprzedniego wejścia do poprzedzającej go strefy; 4) sygnały ostrzeżeń i alarmów z systemu są przekazywane do stacji monitoringu obsługiwanej przez personel bezpieczeństwa; 5) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru.
Typ 3. Punktacja – 3 pkt Elektroniczny automatyczny system kontroli dostępu o następujących cechach: 1) spełnia co najmniej wymagania systemu w klasie rozpoznania 3, a w klasie dostępu B – określone w normie PN-EN 50133-1; 2) wstęp jest kontrolowany przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru przez personel bezpieczeństwa; 3) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru.
Typ 2. Punktacja – 2 pkt Dopuszcza się zastosowanie jednego z poniższych rozwiązań: 1. elektroniczny automatyczny system kontroli dostępu o następujących cechach: a) spełnia co najmniej wymagania systemu w klasie rozpoznania 2, a w klasie dostępu B – określone w normie PN-EN 50133-1; b) wstęp jest kontrolowany przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru strażnika; c) obejmuje wszystkie wejścia i wyjścia kontrolowanego obszaru lub 2. system kontroli dostępu obejmujący wszystkie wejścia i wyjścia z kontrolowanego obszaru, wymagający: a) obecności personelu bezpieczeństwa; b) zastosowania fotografii lub systemu wstępu na podstawie unikalnych przepustek; w zależności od ustaleń związanych z przyznawaniem wstępu mogą być akceptowane również inne dokumenty identyfikacyjne, np. legitymacja służbowa.
Typ 1. Punktacja – 1 pkt System tego typu może być stosowany do zabezpieczania obszarów, w których są przetwarzane informacje niejawne najwyższej o klauzuli „poufne”. System kontroli dostępu oparty na zamkniętych drzwiach pomieszczenia lub obszaru, do którego można uzyskać dostęp za pomocą: 1. kodów – spełnia co najmniej wymagania systemu w klasie rozpoznania 1, a w klasie dostępu B – określone w normie PN-EN 50133-1 lub 2. kluczy wydawanych uprawnionym osobom.

Lektura treści uzasadnienia rozporządzenia nowelizacyjnego dostarcza bulwersujących informacji. Oto bowiem napisano w nim, że jedynym powodem dokonanej nowelizacji jest działanie Polskiego Komitetu Normalizacyjnego, który 29 października 2014 r. wycofał jedną z Polskich Norm wskazaną do stosowania w treści rozporządzenia nowelizowanego, wprowadzając – zamiast normy wycofanej – inną, podobno bardziej nowoczesną Polską Normę. Zatem dano zainteresowanemu środowiskom jasno do zrozumienia, że zgłaszane przez nie wszelkie postulaty i uwagi dotyczące mankamentów nowelizowanego rozporządzenia, a także wieloaspektowa krytyka dyspozycji tego rozporządzenia na łamach specjalistycznych wydawnictw branżowych nie zostały uznane za wystarczający powód wcześniejszej jego nowelizacji.

Trzeba zwrócić uwagę jeszcze na dwa spostrzeżenia, które rzucają się w trakcie lektury tego uzasadnienia. Pierwsze to inercja organu władzy publicznej, który już dawno powinien zareagować na krytykę. Inercja ta spowodowała, że zainteresowane środowiska nadal będą się borykać w praktycznym działaniu z tym „okazem sztuki legislacyjnej”, jak nazywały wcześniej i nazywają to rozporządzenie po nowelizacji. Ponadto w obowiązującym akcie prawa powszechnego już od prawie 30 miesięcy (dokładnie od co najmniej 28) nakazywało się stosować pracownikom zabezpieczenia technicznego wycofaną Polską Normę. Pojawiają się więc pytania, ile przedsiębiorców i właścicieli nieruchomości zainwestowało w tym czasie w budowę stref ochronnych w swoich nieruchomościach, stosując przepisy nieistniejącej Polskiej

Normy, a także czy po wejściu w życie rozporządzenia nowelizacyjnego zjawia się w podmiotach prawa handlowego i innych podmiotach kontrolerzy z ramienia organu władzy publicznej, by „wykryć” i nakazać usunięcie niezgodności funkcjonujących systemów kontroli dostępu do zorganizowanych stref ochronnych z wymogami „nowej” od kilkudziesięciu miesięcy Polskiej Normy. Nowelizacja weszła przecież w życie z dniem 28 marca br. Należy zadać kolejne dwa pytania: ile to może kosztować i czy autorzy przygotowanej nowelizacji zadali sobie powyższe pytania. Drugie spostrzeżenie dotyczy czynnika czasu. Dlaczego tak długo trwało, by w urzędzie administracji publicznej zaważono, że Polski Komitet Normalizacyjny zrobił to, co zrobił? Przecież w tym urzędzie funkcjonuje departament ma-

ZAŁĄCZNIK DO ROZPORZĄDZENIA NOWELIZACYJNEGO
Kategoria K4: Kontrola dostępu. Środek bezpieczeństwa K4S1 – Systemy kontroli dostępu
Typ 4. Punktacja – 4 pkt Elektroniczny automatyczny system kontroli dostępu: 1) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru; 2) spełnia co najmniej wymagania systemu, w którym rozpoznanie następuje w wyniku powiązania odczytu identyfikatora (karty, klucza itp.) z wprowadzeniem informacji zapamiętanej (hasło, osobisty numer identyfikacyjny PIN) lub powiązania odczytu cech biometrycznych (odciski palców, kształt dłoni, tęczówka oka, układ naczyń krwionośnych itp.) z wprowadzeniem informacji zapamiętanej, lub powiązania odczytu identyfikatora z odczytem cech biometrycznych, a na przejściach stosuje się uzależnienie uprawnień dostępu od czasu oraz rejestruje zdarzenia; 3) zapewnia właściwy stopień ochrony wymagający jedynie minimalnego nadzoru przez personel bezpieczeństwa; 4) jest stosowany w połączeniu z barierą dostępu uniemożliwiającą powrót, działającą na zasadzie uniemożliwiającej otwarcie danego przejścia kontrolowanego, jeżeli wcześniej nie nastąpiło wyjście ze strefy, do której zamierza się wejść, albo bez uprzedniego wejścia do poprzedzającej go strefy; 5) przekazuje sygnały ostrzeżeń i alarmów do stacji monitoringu obsługiwanej przez personel bezpieczeństwa.
Typ 3. Punktacja – 3 pkt Elektroniczny automatyczny system kontroli dostępu: 1) obejmuje wszystkie wejścia i wyjścia kontrolowanego pomieszczenia lub obszaru; 2) spełnia co najmniej wymagania systemu, w którym rozpoznanie następuje w wyniku powiązania odczytu identyfikatora (karty, klucza itp.) z wprowadzeniem informacji zapamiętanej (hasło, osobisty numer identyfikacyjny PIN) lub powiązania odczytu cech biometrycznych (odciski palców, kształt dłoni, tęczówka oka, układ naczyń krwionośnych itp.) z wprowadzeniem informacji zapamiętanej, lub powiązania odczytu identyfikatora z odczytem cech biometrycznych, a na przejściach stosuje się uzależnienie uprawnień dostępu od czasu oraz rejestruje zdarzenia; 3) wstęp jest kontrolowany przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru przez personel bezpieczeństwa.
Typ 2. Punktacja – 2 pkt Dopuszcza się zastosowanie jednego z poniższych rozwiązań: 1. elektroniczny automatyczny system kontroli dostępu: a) obejmuje wszystkie wejścia i wyjścia kontrolowanego obszaru; b) spełnia co najmniej wymagania systemu, w którym rozpoznanie następuje w wyniku odczytu identyfikatora (karty, klucza itp.) lub odczytu cech biometrycznych (odciski palców, kształt dłoni, tęczówka oka, układ naczyń krwionośnych itp.), a na przejściach stosuje się uzależnienie uprawnień dostępu od czasu oraz rejestruje zdarzenia; c) wstęp jest kontrolowany przez odpowiednią barierę, która może wymagać bezpośredniego nadzoru strażnika; lub 2. system kontroli dostępu obejmujący wszystkie wejścia i wyjścia z kontrolowanego obszaru, wymagający: a) obecności personelu bezpieczeństwa; b) zastosowania fotografii lub systemu wstępu na podstawie unikalnych przepustek; w zależności od ustaleń związanych z przyznawaniem wstępu mogą być akceptowane również inne dokumenty identyfikacyjne, np. legitymacja służbowa.
Typ 1. Punktacja – 1 pkt System tego typu może być stosowany do zabezpieczania obszarów, w których są przetwarzane informacje niejawne najwyższej o klauzuli „poufne”. System kontroli dostępu oparty na zamkniętych drzwiach pomieszczenia lub obszaru, do którego można uzyskać dostęp za pomocą: 1. kodów – weryfikowanych przez elektroniczny automatyczny system kontroli dostępu, w którym rozpoznanie następuje w wyniku wprowadzenia informacji zapamiętanej (hasło, osobisty numer identyfikacyjny PIN), a na przejściach stosuje się uzależnienie uprawnień dostępu od czasu oraz rejestruje zdarzenia, lub 2. kluczy wydawanych uprawnionym osobom.

jący w nazwie określenie „ochrony informacji niejawnych”. Działa też komórka prawna. Być może w porę dostrzeżono zamianę wspomnianych Polskich Norm i niezwłocznie podjęto stosowne prace legislacyjne na tyle skomplikowane, że musiały one trwać tak długo? Chyba nie, bo znajomy prawnik, specjalista w zakresie legislacji, któremu pokazano ogłoszone właśnie rozporządzenie

nowelizacyjne, powiedział z trudem zachowując powagę, że student pierwszego lub drugiego roku Wydziału Prawa jakiegokolwiek polskiej uczelni wyższej napisał-

by projekt takiego aktu prawnego w ciągu kilku godzin. I to zapewne lepiej, niż napisano to rozporządzenie nowelizacyjne, które właśnie przeczytał. ■

W wyrazami współczucia dla przedsiębiorców i pracowników zabezpieczenia technicznego polskiej branży security, zmuszonych do posługiwania się w swojej działalności biznesowej i pracowniczej takimi „okazami sztuki legislacyjnej” jak rozporządzenia – nowelizowane i nowelizacyjne – o których była mowa wyżej.
Autor

Polskie Normy po polsku

Jerzy W. Sobstel

Stowarzyszenie NOWACERT

Wszystkie aktualne Polskie Normy dotyczące systemów zabezpieczeń, bezpieczeństwa publicznego, a także jakości zarządzania itd. powstały w europejskich komitetach normalizacyjnych CEN, CENELEC i ETSI lub w międzynarodowych organizacjach normalizacyjnych ISO i IEC. Tylko nieliczne z nich zostały przetłumaczone i opublikowane w języku polskim. Pozostałe zostały wprowadzone do zbioru Polskich Norm bez tłumaczenia. Do angielskich oryginałów Polski Komitet Normalizacyjny dodał tylko stronę tytułową w języku polskim i polski tytuł.

Dlaczego tak się dzieje?

Polski Komitet Normalizacyjny jako krajowa jednostka normalizacyjna ma zagwarantowaną ustawowo [1] wyłączność publikowania Polskich Norm oraz wszystkich norm europejskich i międzynarodowych, a także majątkowe prawa autorskie do wydawanych norm, tak jak do utworów literackich. PKN jest państwową jednostką organizacyjną, co oznacza, że działa w ramach przyznanego mu budżetu. Budżet ten jest wykorzystywany głównie na utrzymanie całej struktury administracyjnej PKN i jego funkcjonowanie. Na tłumaczenie norm, i to zwykle na tłumaczenie wybranych norm zharmonizowanych, są przeznaczane niewielkie kwoty. Pozostałe mogą być tłumaczone i publikowane na koszt zainteresowanych podmiotów we-

dług zasady, że normy są opracowywane przez tych, którzy są zainteresowani ich stosowaniem i na ich koszt.

Skutki takiego sposobu finansowania

Przyjrzyjmy się, dla przykładu, normom serii EN 54 dotyczącym urządzeń wchodzących w skład systemów sygnalizacji pożarowej. Są to normy zharmonizowane, a więc de facto ich stosowanie jest obligatoryjne. Niestety, znaczna ich część nie ma wersji polskich. Normy te zostały wymienione w tabeli 1. Nie ma też polskich wersji następujących dokumentów: EN 54-13:2017 *Ocena kompatybilności podzespołów systemu* CEN/TS 54-32:2015 *Planning, design, installation, commissioning, use and maintenance of voice alarm systems*. W tym roku można się spodziewać publikacji CEN/TS 54-14, a także EN 54-4 i EN 54-2, której ostatnia, zmieniona wersja pochodzi z 2006 r. Publikacja nowych wersji piętnastu podstawowych norm serii EN54 została wstrzymana z powodu nieporozumień pomiędzy CEN/TC 72 a KE. Gdy te prze-

szkody zostaną usunięte, możemy zostać wręcz zasypani nowymi normami. Tymczasem PKN w 2018 r. zamierza sfinansować tłumaczenie tylko jednej z wymienionych wyżej norm. Nie ma też chętnych do sfinansowania tłumaczenia i publikacji pozostałych norm.

Czy są potrzebne polskie wersje językowe Polskich Norm?

Taka wątpliwość pojawiła się podczas dyskusji prowadzonej w jednej z grup na LinkedIn. Wprawdzie znajomość języka angielskiego jest coraz szersza, ale jeszcze daleka od powszechności, która gwarantowałaby pełne i jednoznaczne rozumienie wymagań zapisanych w tym języku. Istnieje jednak ważniejszy, i to zasadniczy, powód prawny. Można dyskutować o tym,

czy normy mogą być przywoływane tylko w ustawach, przy czym obstaje PKN na podstawie ustawy o normalizacji [1], czy także w ministerialnych rozporządzeniach, co jest często praktykowane. *Sko-ro jednak rozporządzenie stanowi jedno ze źródeł prawa powszechnie obowiązującego, obok konstytucji...* [2], to zmuszanie obywateli do korzystania z tekstów w języku angielskim i rozstrzyganie sporów na tej podstawie stanowiłoby naruszenie praw obywatelskich wywodzących się z konstytucji. Bo jeżeli w języku angielskim, to dlaczego nie w chińskim czy arabskim?

Normy dotyczące zabezpieczeń technicznych

Zaległości w tłumaczeniu norm występują w każdej dziedzinie zabezpieczeń tech-

nicznych i tym szybciej narastają, im szybciej dana dziedzina się rozwija. W zakresie systemów dozoru wizyjnego lista nieprzetłumaczonych norm została zamieszczona w tabeli 2.

Nowej serii norm dotyczących kontroli dostępu, opracowanych w IEC i przyjętych następnie przez CENELEC (tabela 3), poświęcono wiele artykułów, prezentacji i szkoleń. Niestety, żadna z nich nie doczekała się jeszcze publikacji w języku polskim. Wprawdzie pierwsza z wymienionych norm została już przetłumaczona, ale PKN jeszcze jej nie opublikował. Podobne zaległości są także w innych grupach norm dotyczących systemów transmisji alarmu, stacji monitorowania, systemów socjalnych, sygnalizacji włamania i napadu itd.

Kto i dlaczego finansuje tłumaczenie norm

Zaległości w tłumaczeniu norm dotyczą nie tylko sektora bezpieczeństwa publicznego, ale także innych dziedzin. Niektóre jednak normy, a nawet ich grupy, są tłumaczone niezwykle skwapliwie jeszcze przed ich opublikowaniem, a nawet przed formalnym zatwierdzeniem. Są to normy wykorzystywane jako dokumenty odniesienia przy certyfikacji. Ich aktualność warunkuje prowadzenie działalności komercyjnej przez firmy certyfikujące, otwiera im nowe pola certyfikacji lub możliwość recertyfikacji. Firmy szkolące, a także stowarzyszenia i organizacje biznesowe prowadzące szkolenia nie spieszą się tak z tłumaczeniami, bo ich trenerzy wolą występować w roli „jedynych wtajemniczonych” objawiających nową wiedzę swoim słu-

Numer oryginału	Tytuł polski
EN 54-12:2015	Czujki dymu – Czujki liniowe działające z wykorzystaniem wiązki światła przechodzącego
EN 54-22:2015	Liniowe kasowalne czujki ciepła
EN 54-26:2015	Czujki tlenu węgla – Czujki punktowe
EN 54-27:2015	Kanałowe czujki dymu
EN 54-28:2016	Czujki ciepła liniowe niekasowalne
EN 54-29:2015	Czujki pożarowe wielodetektorowe – Czujki punktowe wykorzystujące kombinacje detektorów dymu i ciepła
EN 54-30:2015	Czujki pożarowe wielodetektorowe – Czujki punktowe wykorzystujące kombinację detektorów tlenu węgla i ciepła
EN 54-3:2014	Pożarowe urządzenia alarmowe – Sygnalizatory akustyczne
EN 54-5:2017	Punktowe czujki ciepła
EN 54-31/A1:2016	Czujki pożarowe wielodetektorowe – Czujki punktowe wykorzystujące kombinację detektorów dymu, tlenu węgla i opcjonalnie ciepła

TABELA 2

Numer oryginału	Tytuł polski
EN 62676-1-1:2014	Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 1-1: Wymagania systemowe – Postanowienia ogólne
EN 62676-1-2:2014	Część 1-2: Wymagania systemowe – Wymagania eksploatacyjne dotyczące transmisji wizji
EN 62676-2-1:2014	Część 2-1: Protokoły transmisji wizji – Wymagania ogólne
EN 62676-2-2:2014	Część 2-2: Protokoły transmisji wizji – Zastosowanie międzyoperacyjności IP oparte na usługach HTTP i REST
EN 62676-2-3:2014	Część 2-3: Protokoły transmisji wizji – Zastosowanie międzyoperacyjności IP oparte na usługach Web
EN 62676-3:2015	Część 3: Analogowe i cyfrowe interfejsy wizyjne
EN 62676-4:2015	Część 4: Wytyczne stosowania
prEN 62676-5E	Part 5: Data specifications and image quality performance for camera devices

chaczom. Poszczególne ministerstwa i podległe im jednostki zazwyczaj nie wspierają prac normalizacyjnych, nie tworzą budżetów na to przeznaczonych, a niektóre wolałyby nawet nie otrzymywać powiadomień o nowych normach. Taki stan ma źródło w ustawie o normalizacji [1], która w art. 1 stwierdza: „Ustawa określa podstawowe cele i zasady normalizacji oraz jej organizację i finansowanie”. Jeżeli chodzi o finansowanie prac normalizacyjnych, to jedyny zapis, jaki znalazł się w tej ustawie, dotyczy przyznania PKN wyłącznego, majątkowego prawa autorskiego do utworów, jakimi są Polskie Normy. Nie ma tam natomiast informacji o prawach i zobowiązaniach finansowych poszczególnych resortów, firm i organizacji. Nie można też liczyć na środki unijne, bo takich, przynajmniej zgodnie z wiedzą autora, na tłumaczenie norm po prostu nie ma.

Kto może i powinien finansować tłumaczenie i publikację norm

Trzeba wrócić do zasady, że normy opracowują ci, którzy są zainteresowani ich sto-

sowaniem, i to na własny koszt. Dotyczy to także tłumaczenia. Stosowaniem norm nie są zainteresowani ministerialni urzędnicy ani dysponenti publicznych pieniędzy. Zainteresowani są bezpośredni użytkownicy – firmy, organizacje, instytucje, a także eksperci, doradcy i biegli sądowi. Koszt przetłumaczenia i publikacji normy przez PKN wynosi od kilku do kilkunastu tysięcy złotych. Nie jest to dużo dla zasobnej firmy, ale nawet wtedy pojawia się pytanie: *Dlaczego to właśnie ja mam płacić za tłumaczenie normy, skoro będą z niej korzystali także inni, w tym moi konkurenci, a na końcu będę jeszcze musiał tę normę w PKN kupić?*

Skoro norma jest wykorzystywana przez grupę użytkowników, to ta grupa powinna też sfinansować jej wydanie. Stowarzyszenie Ekspertów Normalizacji, Walidacji i Certyfikacji NOWACERT proponuje sposób wdrożenia takiego pomysłu poprzez

system darowizn celowych na tłumaczenie i publikację norm – szczegóły na www.nowacert.org. NOWACERT jest organizacją non profit, a proponowane rozwiązanie jest przykładem projektu społecznościowego. Jego zasięg nie ogranicza się do systemów zabezpieczeń, ale dotyczy wszystkich środowisk i komitetów normalizacyjnych, w których występują problemy z finansowaniem prac normalizacyjnych. Każdy może wskazać normę, która jest szczególnie potrzebna, i zainicjować jej tłumaczenie. Każdy może dołożyć swoją cegiełkę. NOWACERT stwarza jedynie platformę do realizacji całego projektu obejmującego wycenę prac, umowy z PKN i tłumaczami itd. Udostępnia też swoje konto bankowe, na które można przekazywać darowizny.

Rola NOWACERT kończy się z chwilą przekazania projektu przetłumaczonej normy do PKN. Dalsze prace będą prowadzone przez właściwe komitety techniczne PKN. Kwotę przekazaną do stowarzyszenia jako darowiznę celową można odliczyć od przychodu. Dotyczy to zarówno osób fizycznych, jak i prawnych. Pierwszą normą zgłoszoną do tłumaczenia na powyższych zasadach jest PN-EN 16763:2017-04 – wersja angielska *Usługi w zakresie systemów ochrony przeciwpożarowej oraz systemów zabezpieczeń technicznych*. Powszechne jej stosowanie przyczyniłoby się do podniesienia jakości świadczonych usług. Powinna zainteresować zarówno usługodawców, jak i inwestorów, zarządców nieruchomości itd. ■

Literatura

- [1] Ustawa z 12 września 2002 r. o normalizacji (Dz.U. nr 169, poz. 1386).
[2] <https://pl.wikipedia.org/wiki/Rozporzadzenie>

TABELA 3

Numer oryginału	Tytuł polski (jeżeli istnieje)
EN 60839-11-1:2013	Systemy alarmowe i elektroniczne systemy zabezpieczeń – Część 11-1: Elektroniczne systemy kontroli dostępu – Wymagania dotyczące systemów i części składowych
EN 60839-11-2:2015	Część 11-2: Elektroniczne systemy kontroli dostępu – Wytyczne stosowania
EN 60839-11-31:2017	<i>Alarm and electronic security systems – Part 11-31: Electronic access control systems – Core interoperability protocol based on Web services</i>
EN 60839-11-32:2017	<i>Alarm and electronic security systems – Part 11-32: Electronic access control systems – Access control monitoring based on Web services</i>



Monitoring wizyjny w szkołach: potrzebne są lepsze regulacje

Paweł Wittich
Akademia Monitoringu Wizyjnego

Jakość szkolnych systemów monitoringu wizyjnego skontrolowanych przez NIK jest dobra mimo niestaranego rozporządzenia, które zapoczątkowało ich instalowanie. Mogą być skutecznie wykorzystywane przez szkoły, ale wymaga to wdrożenia dodatkowych działań organizacyjnych i technicznych. Jednocześnie z raportu NIK wynika, że dobra komunikacja oraz zaufanie między uczniami a nauczycielami stanowią podstawę ich poczucia bezpieczeństwa w szkole. Wskazane przez NIK mankamenty szkolnych systemów CCTV są echem postulatów pokontrolnych w miastach – potrzebna jest ustawa dotycząca systemów monitoringu wizyjnego w Polsce.

Słabości „rozporządzenia Giertycha”

Rozporządzenie Rady Ministrów z 6 września 2007 r. w ograniczonym stopniu stało się przed szkołami i projektantami wymóg budowania skutecznych rozwiązań. Tylko w przypadku tzw. zestawu do monitoringu wizyjnego w wersji standardowej, czyli dwóch kamer montowanych w wejściu do

szkoły, w rozporządzeniu wskazano cel obserwacji i wymagania techniczne: kolorowy obraz o rozdzielczości wystarczającej do identyfikacji wchodzących i wychodzących osób. W dokumencie nie sprecyzowano, co oznacza pojęcie „identyfikacja”, i nie odwołano się do Polskiej Normy (w kolejnych normach te parametry się zmieniały). W rozporządzeniu nie pojawił się też wymóg, który został opisany w Rządowym Programie „Monitoring wizyjny w szkołach i placówkach” – urządzenia utrwalające powinny rejestrować obraz z częstotliwością 25 kl./s dla każdej kamery, z rozdzielczością nie mniejszą niż 400 linii TV [1], co mogło wpłynąć na obniżenie wymagań dotyczących jakości szkolnych systemów dozorowych. W hierarchii aktów prawnych w polskim prawodawstwie rozporządzenie obowiązuje przed uchwałą – rządowym programem dotyczącym monitoringu w szkołach, dlatego zapisy rozporządzenia były wiążące dla dyrektorów i projektantów. Rozporządzenie posługuje się nic nieznaczącym pojęciem „urządzeń zgodnych z Polską Normą”. Każdą kamerę i rejestrator dostępne na rynku, tanie czy drogie, dobrej czy kiepskiej jakości, można w tym rozumieniu uznać za zgodne z normą. Dla każdego, kto zetknął się z normami, jest oczywiste, że nie opisują one parametrów urządzeń, ale

są zbiorem zaleceń, jak zaprojektować skuteczny system monitoringu. W rozporządzeniu brakuje wymogu opracowania wymagań użytkowych dla szkolnego systemu monitoringu wizyjnego. W normach składają się na nie m.in.:

- wskazanie celu prowadzenia obserwacji i rejestracji obrazu – czy będzie to statyczna fasada budynku, czy dynamicznie poruszające się osoby lub grupy,
- ustalenie, jak często dochodzi do zagrożeń, i wysokości faktycznych lub potencjalnych szkód,
- uwzględnienie warunków środowiskowych, czyli natężenia światła, przeszkód w obserwacji, np. drzewa i układ pomieszczeń,
- zalecenie oceny skuteczności rozwiązań alternatywnych dla systemu CCTV.

Nie określono w nim również wskaźników efektywności szkolnego systemu monitoringu wizyjnego ani sposobów ich weryfikacji. Iloraz liczby uczniów i kosztów zakupu systemu, którym posłużono się w rozporządzeniu, jest wskaźnikiem efektywności finansowej, a nie skuteczności systemu. Można więc stwierdzić, że „rozporządzenie Giertycha” o systemie monitoringu wizyjnego w szkołach zostało przygotowane niestannie, bez uwzględnienia opinii specjalistów zajmujących się techniką wizyjną.

Przyzwoity monitoring w szkołach

Mimo słabości rozporządzenia z 2007 r. należy uznać, że szkoły dobrze poradziły sobie z wprowadzeniem monitoringu. W ponad 80% kontrolowanych przez NIK placówek jakość nagrań była dobra. Niewystarczającą wykazano w pięciu spośród 28 szkolnych systemów (17,8%). W kontrolowanych szkołach przed budową lub rozbudową systemu dyrektorzy przeprowadzali diagnozę problemów związanych z bezpieczeństwem, omawiając je wspólnie z pracownikami szkoły i rodzicami uczniów oraz we współpracy z kuratoriami i policją. Kontrola NIK wykazała jeden przypadek instalacji kamery nadmiernej ingerującej w prywatność (skierowaną na pisuary), co należy uznać za osobliwe działanie projektanta lub dyrekcji szkoły, ponieważ rozporządzenie z 2007 r. w § 6.1 pkt 5 wyraźnie wskazuje możliwe miejsca instalacji kamer, i nie ma wśród nich toalet. Uznając tę praktykę za naganną, warto odnotować, że była to tylko jedna kamera na 482 zainstalowane w szkołach objętych kontrolą. W relacji dyrektorów 28 szkół publicznych objętych kontrolą NIK system monitoringu wizyjnego „w latach 2010–2015 pozwolił zapobiec lub pomógł ustalić sprawców i przebieg 916 zdarzeń, takich jak kradzieże (91), dewastacja mienia szkoły (284), agresja fizyczna wśród uczniów (322), wejście na teren szkoły osób niepowołanych z zewnątrz (44), zagrożenia związane z używkami (111), zastraszanie i wymuszenie (64)” [2]. Warto zauważyć, że Najwyższa Izba Kontroli swobodnie używa słowa identyfikacja w kontekście systemów CCTV, zamiennie z rozpoznaniem, co nie jest zgodnie z zaleceniami wcześniejszych i aktualnej normy.

Szkolne systemy CCTV mają dobrą opinię wśród nauczycieli

W badaniu ankietowym przeprowadzonym w ponad 2 tys. gimnazjów w ramach kontroli NIK 81,4% ich pracowników wskazało, że monitoring wizyjny w znacznym stopniu zapobiega występowaniu zdarzeń niepożądanych w szkole [2]. Takie samo zdanie miało 70% pracowników blisko 6 tys. szkół podstawowych, 95% ankietowanych nauczycieli odpowiedziało, że szkolny monitoring był pomocny przy ustaleniu sprawców i przebiegu zdarzenia. Dla 84% jest skutecznym narzędziem pozwalającym zwalczyć problemy wychowawcze. W opinii 51% nauczycieli uczniowie w monitorowanych obszarach byli spokojniejsi, a 61% uwa-

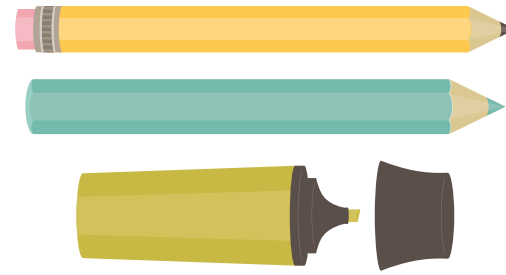
ża, że wymusza on pożądane zachowania uczniów. Część nauczycieli uznała, że system monitoringu wizyjnego ma pozytywny wpływ na jakość ich pracy: 41% z nich czuje się bezpieczniej na dyżurach, a dla 55% jest pomocny w ustaleniu odpowiedzialności w przypadku jakiegokolwiek zdarzenia podczas dyżuru. Czytając raport NIK, można odnieść wrażenie, że opinie uczniów potraktowano po macoszemu. W ankiecie dla uczniów brakuje pytania, czy chcą oni, żeby kamery były instalowane w szkołach. Uczniowie nie wskazują kamer jako czynnika budującego ich poczucie bezpieczeństwa – tu kluczową rolę odgrywają przyjaźnie między uczniami (56% odpowiedzi), nauczyciele pełniący dyżury (54%) i dobry kontakt z wychowawcą (32%). W tym kontekście warto się zastanowić nad postulatem NIK, by obraz z kamer był obserwowany w czasie przerw. Jeżeli miałoby się to odbywać kosztem dyżurów nauczycielskich, przełoży się to na zmniejszenie poczucia bezpieczeństwa uczniów. Według kontrolerów NIK uczniowie czują się bezpieczniej dzięki kamerom. Spora ich część uważa, że obecność kamer „wpłynęła na zmniejszenie liczby bójek w szkole (58%), kradzieży (59%), wyłudzeń (46%), zastraszonych (43%), graffiti na ścianach (56%)”. Te opinie należy potraktować jako wyobrażenie uczniów o prewencyjnej sile oddziaływania kamer, jako że uczniów, którzy faktycznie spotkali się z zastosowaniem systemu CCTV do ustalenia sprawcy zdarzenia, było mniej: bójka (42%), kradzież (32%), wyłudzenie (18%), zastraszanie (21%), graffiti na ścianach (29%). Uczniowie deklarują, że szkolne systemy CCTV mają ograniczony wpływ na ich zachowanie – w przypadku

15% uczniów obecność kamer zawsze wpływa na ich zachowanie, dla 35% czasami, a 48% uczniów nie zwraca na nie uwagi.

Mankamenty monitoringu i potrzeba regulacji

NIK wskazuje wiele mankamentów szkolnych systemów dozoru wizyjnego. Najważniejsze z nich to brak nadzoru po stronie organów prowadzących szkoły (czyli samorządów), nieprzeprowadzenie weryfikacji skuteczności działania systemów, brak procedur dotyczących dostępu do obrazów z kamer i nagrań, zbyt krótki czas przechowywania nagrań, nieumieszczenie w statucie szkoły wymaganych wpisów dotyczących wykorzystania systemu i niewystarczające uświadomienie uczniom tych zasad. Według NIK negatywnie na skuteczność szkolnych systemów monitoringu wizyjnego wpływa nieobecność obserwatorów przed monitorami w czasie przerw, kiedy to występuje największe ryzyko zagrożeń, a także niepowiadomianie o wykrytych zagrożeniach. Szkoły nie rejestrowały systemów monitoringu wizyjnego – zbiorów danych osobowych w rejestrze prowadzonym przez GIOD. Dyrektorzy tłumaczyli niedociągnięcia brakiem przepisów, które by ich obligowały do określonych działań. Trudno nie przyznać im racji. Jako specjaliści Akademii Monitoringu Wizyjnego spotykamy się z podobnymi problemami w systemach monitoringu wizyjnego miast. One także wynikają z braku jasno określonych wymagań w przepisach prawa. Jeżeli publiczne pieniądze na rozwój systemów monitoringu wizyjnego w Polsce mają być dobrze wydawane, należy wprowadzić standardy ich działania w formie

NIK wskazuje m.in. brak procedur dotyczących dostępu do obrazów z kamer i nagrań, zbyt krótki czas przechowywania nagrań, nieumieszczenie w statucie szkoły wymaganych wpisów dotyczących wykorzystania systemu i niewystarczające uświadomienie uczniom tych zasad.



Systemy monitoringu wizyjnego mogą być skutecznym narzędziem wspomagającym działania poprawiające bezpieczeństwo.

ustawy; także w kontekście ochrony praw osób w obszarach objętych dozorem CCTV. W czasie konsultacji organizowanych przez MSWiA w latach 2013–2015 wiele publicznych i prywatnych podmiotów zgłosiło własne propozycje dotyczące systemów monitoringu wizyjnego. Wystarczy, żeby rząd skierował je do prac w sejmie.

Stanowisko AMW w sprawie instalowania monitoringu wizyjnego w szkołach

Systemy monitoringu wizyjnego mogą być skutecznym narzędziem wspomagającym działania poprawiające bezpieczeństwo. Mogą przeciwdziałać dewastacjom, wchodzeniu na teren szkoły po jej zamknięciu, śmieceniu i spożywaniu tam alkoholu oraz podobnym zagrożeniom. Szkoły inwestują w budynki, place zabaw, boiska, dlatego dyrektorzy powinni mieć możliwość instalowania tych systemów na zewnątrz budynków i wokół szkoły – w interesie swoim, nauczycieli, uczniów i rodziców. Skuteczny system monitoringu wizyjnego wymaga wdrożenia rozwiązań organizacyjnych i technicznych, które będą gwarantowały wykrywanie zagrożeń, ich rejestrację na obrazach o wysokiej jakości i skuteczne reagowanie pracowników szkoły, policjantów lub strażników miejskich. Może się to wiązać z koniecznością dodatkowego oświetlenia, zmiany aranżacji przestrzeni, np. przeswietlenia koron drzew, wycięcia krzewów w celu poprawy pola widzenia kamer.

Instalując kamery w budynku szkoły warto rozważyć następujące propozycje:

1) Podejmowanie działań, których celem jest przeciwdziałanie agresji i zachowaniom niepożądanym przez poprawę komunikacji, budowanie wzajemnego szacunku i zaufania pomiędzy uczniami i w relacji uczeń – nauczyciel. Z raportu NIK wynika, że dla uczniów zagrożeniem są koledzy lub koleżanki (opinia 42% ankietowanych). Drugim w kolejności zagrożeniem (36%) są grupy

uczniów ze swojej lub równoległej klasy, ale także nauczyciele (40%). Tylko 30% uczniów, którzy byli świadkami zagrożenia, zgłaszało ten fakt dyrekcji szkoły. Uczniowie czują się bezpiecznie w szkole dzięki przyjaźniom, dyżurom nauczycielskim na przerwach i dobremu kontaktowi z wychowawcą, dlatego należy wzmacniać te elementy. Wiedza o procesach grupowych i komunikacji interpersonalnej wskazuje, że klasa moderowana przez nauczyciela może skutecznie budować poczucie bezpieczeństwa, uczyć rozpoznawania i radzenia sobie z agresją, rywalizacją i innymi zachowaniami, które mogą powodować zmniejszenie poczucia bezpieczeństwa wśród uczniów. Nauczyciele powinni odbywać kursy i treningi doskonalące ich umiejętności w pracy z „trudnymi sytuacjami” w klasie, w szerszej perspektywie – całej szkoły.

2) Szkoły mają do dyspozycji wiele środków, za których pomocą można budować system bezpieczeństwa. Poczucie bezpieczeństwa tworzą jasno określone zasady oraz ich rzetelne przestrzeganie przez nauczycieli i pracowników szkoły, a także środki techniczne. Przykładowo, wejście do szkoły jest otwierane elektrozamkiem. Recepcjonistki dyżurujące przy wejściu dbają, żeby dorośli, którzy chcą wejść na teren szkoły, wpisali się do rejestru gości. Rodzice, dziadkowie odbierający dzieci po lekcjach czekają w strefie wyznaczonej przy recepcji, nie chodzą po szkole. Recepcjonistki znają dzieci i odbierających je opiekunów, co tworzy przyjazną atmosferę i buduje zaufanie do szkoły. Wymagane jest wcześniejsze złożenie upoważnienia, jeżeli inna osoba niż zazwyczaj odbiera dziecko. Szatnie są otwarte rano i podczas przerw, a szatniarki dbają, żeby rodzice czekali, kiedy dzieci się przebierają w wyznaczonej dla nich strefie. Nauczyciele na bieżąco, korzystając z „zeszytów kontaktów” i regularnych zebrań, in-

formują o sukcesach i problemach dzieci oraz klasy. Zdecydowanie reagują na nieporozumienia, przejawy agresji, omawiając takie sytuacje na forum klasy i z rodzicami dzieci sprawiających problemy. Jednocześnie szkoła organizuje konkursy, jarmarki, akcje dobroczynne, które integrują uczniów i rodziców ze szkołą.

3) Instalacja kamer systemu CCTV we wnętrzu budynku szkoły (na korytarzach, w szatniach, ale nie w klasach) jest uzasadniona, jeżeli strategię zapewnienia bezpieczeństwa są niewystarczające. Natężenie negatywnych zjawisk może być tak duże, że wymaga od szkoły podjęcia działań, których celem jest zwiększenie poczucia społecznej kontroli. Współczesne badania na temat moralności potwierdzają mit o pierścieniu Gygesa: ludzie chętniej przestrzegają reguł, jeżeli mają świadomość, że ich zachowanie jest zauważane i oceniane przez innych [3]. Warto przywołać z raportu NIK pozytywne opinie nauczycieli na temat systemów monitoringu: zwiększają ich poczucie bezpieczeństwa w czasie dyżurów i w relacjach z uczniami. Należy jednocześnie przeciwdziałać nadmiernej chęci dyscyplinowania i kontrolowania uczniów. Instalowanie kamer powinno być uzasadnione. Szkoły we współpracy z Ministerstwem Edukacji Narodowej, pedagogami i psychologami powinny wypracować standardy, dobre praktyki, które określą warunki instalowania kamer we wnętrzu budynku szkoły i korzystania z otrzymanego z nich obrazu.

4) Jako zalecenia należy traktować opracowanie wymagań użytkowych, ponieważ pozwalają one całościowo analizować problemy wewnątrz i w otoczeniu szkoły oraz wskazać adekwatne rozwiązania organizacyjne i techniczne, w tym systemu monitoringu wizyjnego.

5) Należy przeprowadzać systematyczną ocenę skuteczności i poprawności wykorzystania szkolnego systemu wizyjnego. ■

Źródła:

- [1] Załącznik do uchwały nr 156/2007 Rady Ministrów z 5 września 2007 r., s. 4.
[2] Raport NIK *Wykorzystanie monitoringu wizyjnego w szkołach i jego wpływ na uczniów*.
[3] Heidt J., *Prawny umysł. Dlaczego dobrych ludzi dzieli religia i polityka*, Wyd. Smak Słowa, 2014.

Serwis informacyjny

Otwarcie targów uświetnił koncert tradycyjnych tajwańskich bębniarzy.



Dużym zainteresowaniem cieszyły się nowe technologie.



W otwarciu targów uczestniczyli przedstawiciele instytucji rządowych z Tajwanu, Tajlandii i Malezji.

20. EDYCJA TARGÓW: Secutech Taipei 2017



Wystawcy zaprezentowali ciekawe rozwiązania z wykorzystaniem dronów i robotów.



Ponad 22 tys. gości z 75 krajów odwiedziło jubileuszową edycję targów Secutech na Tajwanie. Podczas trzech dni wystawy (12–14 kwietnia) na 30 tys. m² można było zapoznać się z produktami security ponad 370 wystawców z 13 krajów.

Mariusz Kucharski
korespondencja z Tajpej

Secutech Taipei to jedno z najważniejszych azjatyckich targów branży security. Od dwóch dekad są organizowane w stolicy Tajwanu, jednego z azjatyckich tygrysów, który od lat wyznacza kierunki rozwoju m.in. w produkcji elektroniki użytkowej. W tym roku organizatorzy położyli szczególny nacisk na modny obecnie IoT (Internet Rzeczy). Ciekawe inteligentne i innowacyjne rozwiązania były prezentowane w specjalnych strefach: *Intelligent Special Pavilions* oraz *Intelligent Video Analytics Showroom*. Targi wyróżniają się prężnie działającym programem *Business Matching*, budującym relacje pomiędzy wystawcami i kluczowymi odwiedzającymi. Obecność na eventach branżowych i wymiana wizytówek stały się nieskuteczne, *Business Matching* jest więc rozwiązaniem wychodzącym naprzeciw oczekiwaniom zarówno producentów i dystrybutorów produktów security, jak i potencjalnym klientom poszukującym odpowiednich rozwiązań. Organizatorzy targów, na podstawie dokładnych wytycznych i rozpoznania rynku, oferują gościom „szyte na miarę” indywidualne sesje biznesowe. W tym roku 438 sesji zakończyło się nawiązaniem współpracy pomiędzy 73 wystawcami i 151 gośćmi. Podczas targów odbyło się także wiele inte-

resujących wykładów i prezentacji. Podczas 150 seminariów poruszono najważniejsze dla globalnego rynku security tematy, m.in. integracja systemów, bezpieczeństwo rozwiązań IoT oraz smart home.

Oficjalnym patronem medialnym targów Secutech jest grupa a&s International.

Targi Secutech są organizowane przez Messe Frankfurt, największego na świecie organizatora targów, kongresów i konferencji. Firma działa w 175 krajach, posiadając globalną sieć 29 filii, 5 oddziałów i 48 międzynarodowych przedstawicielstw handlowych. Jest też właścicielem a&s International, największej na świecie grupy wydawniczej branży security. Poza Tajwanem targi Secutech są organizowane także w Indiach, Tajlandii i Wietnamie. Pod nazwą Intersec odbywają się ponadto w Dubaju, Arabii Saudyjskiej, Argentynie i Kenii.





Targi przemysłowo-technologiczne Hannover Messe 2017

Jedne z największych targów przemysłowo-technologicznych na świecie – Hannover Messe – są okazją do corocznego prezentowania efektów działań *research & development* firm z całego globu. Pięciodniową imprezę odwiedziło w tym roku ponad 225 tys. gości, a swoje osiągnięcia zaprezentowało 6,5 tys. wystawców. Tegoroczna edycja była wyjątkowa również dla polskich firm, ponieważ nasz kraj był głównym partnerem targów.

Hannover Messe 2017 to już 70. spotkanie inżynierów i twórców, dostawców najnowocześniejszych technologii. Partnerem jubileuszowej edycji, odbywającej się pod hasłem *Smart means Poland*, była Polska. Swoją obecnością imprezę zaszczyliły takie osobistości, jak kanclerz Angela Merkel, premier Beata Szydło czy reprezentanci przemysłu i niemieckiej administracji publicznej.

Po raz pierwszy na hanowerkich targach wystąpiło ponad 200 wystawców z Polski. Pierwsze dni obfitowały w wiele spotkań prasowych, minikonferencji i paneli dyskusyjnych. Podczas gali poprzedzającej targi wręczono Nagrodę Hermesa przyznaną za wyjątkowo innowacyjne osiągnięcia w branży technologicznej. W tym roku laur ten przypadł firmie SCHUNK GmbH za stworzenie i wdrożenie *cobot*a, zwanego również robotem współpracującym. To zdecydowanie przyszłość automatyki przemysłowej, szczególnie dzięki możliwościom integracyjnym *cobot*ów, skutkującym m.in. zmniejszeniem kosztów pracy. Innymi wyróżniającymi się na targach rozwiązaniami były roboty wielkogabarytowe, roboty samojezdne stosowane na liniach produkcyjnych, a także platformy automatyzacyjne działające w chmurze. Polska firma APA Group zaprezentowała w Hanowe-



rze swoją autorską platformę NAZCA, która wykorzystując szerokie możliwości automatyzacji, nadzorowała działanie całego stoiska firmy (więcej na s. 115). Targi technologiczne w Hanowerze są doskonałą okazją dla firm do wymiany doświadczeń i idei oraz wyjątkową szansą dla młodych inżynierów i przedsiębiorstw do wyróżnienia się na rynku.

Przemawiają za tym statystyki tegorocznej imprezy – organizator podaje, że w ciągu pięciu dni nawiązano tu ponad 5,6 mln kontaktów biznesowych.

Na podstawie oferty targowej w Hanowerze można wysnuć podstawowy wniosek: Industry 4.0 to już nie tylko koncepcja i wizja przyszłości, ale rzeczywistość. ■

Premiera systemu NAZCA na największych targach przemysłowych na świecie



Targi Hannover Messe co roku przyciągają wystawców przemysłowych z całego świata, którzy prezentują tu najnowsze technologie. Tegoroczna, 70. edycja (24–28.04) miała szczególny wymiar – Polska była krajem partnerskim wydarzenia. Ponadto APA Group zaprezentowała tu nowy uniwersalny system NAZCA pozwalający automatyzować i analizować dane w ramach różnych kategorii zastosowań.

Od lat wydarzenia w Hanowerze przyciągają największych graczy przemysłowych z dziedziny automatyki i nowych technologii, są miejscem prezentacji pomysłów, wymiany opinii, doświadczeń i kontaktów biznesowych. Pierwszy dzień targów obfitował w wiele spotkań prasowych, minikonferencji i paneli dyskusyjnych. APA Group pojawiła się na jednym z nich na zaproszenie Polish German Business Summit. Jego głównym gościem był wicepremier, minister rozwoju i finansów Mateusz Morawiecki. Wicepremier z dumą pochwalił współpracę firm z Polski i Niemiec oraz zaprezentował prognozę, według której Polska ma w najbliższych latach znaleźć się w pierwszej piątce partnerów strategicznych Niemiec.

Wśród tematów, które zdominowały tegoroczne targi, znalazły się zagadnienia związane z zarządzaniem wielkimi zbiorami danych – *Big Data*. I tu szczególne miejsce zajął własny system automatyki NAZCA opracowany przez inżynierów z APA Group. Drogą do wykorzystania *Big Data* w celu poprawy jakości życia, optymalizacji kosztów utrzymania czy

ochrony środowiska są m.in. systemy, które pozwalają na integrowanie, monitorowanie oraz kontrolowanie pracy urządzeń i instalacji technicznych w budynkach. Takie systemy, korzystając z zaawansowanych technologii *Big Data*, integrują i przetwarzają ogromne ilości informacji dotyczących zużycia energii, ogrzewania, wentylacji czy z monitoringu wizyjnego. APA, dotrzymując kroku swoim europejskim i światowym konkurentom, opracowała no-

watorskie rozwiązanie, które znajdzie zastosowanie w wielu branżach przemysłu i biznesu. Jego oficjalna premiera odbyła się pierwszego dnia hanowerkich targów. NAZCA, której ideę oddaje hasło *Perfect automation*, jest uniwersalną platformą automatyzacji. Może rozwiązywać problemy i realizować zadania w ramach mniejszych podsystemów funkcjonalnych o charakterze określanym jako BMS, SMS i EMS – czyli kolejno: systemu zarządzania budynkiem, zarzą-

dzania bezpieczeństwem oraz zarządzania jakością i zużyciem energii. NAZCA umożliwia m.in. zaawansowaną wizualizację i monitorowanie dużych zbiorów danych z różnych źródeł, w zależności od wdrożenia. To funkcjonalne oprogramowanie do automatyzacji procesów i analizy danych wyróżnia się łatwością obsługi, skalowalnością i wieloserwerowością. To system zaprojektowany do współpracy m.in. z chmurą Azure firmy Microsoft. Oprócz aspektów technologicznych działająca zgodnie z założeniami normy ISO 5001 NAZCA może przynieść wymierne korzyści finansowe dzięki kontroli zużycia mediów, a w konsekwencji znacząco obniżyć koszty utrzymania obiektu. Jako dowód na szerokie możliwości NAZCA, firma APA Group zintegrowała system ze swoim stoiskiem, na którym odpowiadał za kontrolowanie wszystkich mediów, kamer, oświetlenia oraz nagłośnienia. Ponadto system pobierał i analizował dane z robota KUKA, który był tegoroczną atrakcją stoiska. Dane po ich zebraniu były prezentowane w formie wykresów lub przesyłane do chmury w celu głębszej analizy. ■



Integracja 2017: AxxonSoft i TAP Systemy Alarmowe



W marcu AxxonSoft Polska i TAP Systemy Alarmowe zorganizowały IV edycję seminarium projektowego „Integracja 2017”. W hotelu Turówka w Wieliczce spotkało się ok. 100 projektantów z całej Polski, by mieli okazję poznać szczegóły działania systemów Galaxy Dimension i Axxon Intellect oraz rozwiązania integracyjne z wykorzystaniem systemu kontroli dostępu Honeywell

PRO3200. Gościem specjalnym była tajemnicza firma Promise Technology, która zaprezentowała swoje rozwiązania z zakresu dozoru wizyjnego i przechowywania danych z wykorzystaniem metod RAID. Spotkanie było okazją do podzielenia się wiedzą, wymiany opinii i pomysłów, czemu sprzyjały swobodna atmosfera i gościnne otoczenie zabytkowego murów hotelu. ■



Milestone Community Days

Mariusz Kucharski
korespondencja z Dubaju

Kilkaset osób wzięło udział w pierwszej międzynarodowej konferencji Milestone MIPS dla regionu Europy, Bliskiego Wschodu i Azji (EMEA). Spotkanie odbyło się w dniach 8-11 maja w Dubaju.

Ponad 450 uczestników z całego regionu odwiedziło nowoczesny Dubaj, w którym firma Milestone omawiała nowoczesne zastosowania security. Duńska firma zaprosiła także ponad 30 innych partnerów, którzy prezentowali swoje produkty i usługi. Stoiska mieli m.in. Axis Communications, Bosch, Dahua Technology, DELL EMC, ela-soft, Fujitsu, Hikvision, IBM, Nedap, OPTEX i Seagate. Organizatorzy podkreślali, że chcą budować społeczność partnerską nie tylko ze swoimi klientami, ale także z innymi dostawcami rozwiązań security.



Społeczność była właśnie hasłem przewodnim konferencji. Milestone Community ma być tym, co wyróżni firmę na rynku i da jej przewagę konkurencyjną. Kierownictwo Milestone zrozumiało, że w czasach sieci

społecznościowych i *sharing economy* nie jest możliwe zdobywanie rynku w pojedynkę – do budowania pozycji potrzebne są bliska współpraca oraz współtworzenie produktów i usług w sieci. Podczas

konferencji zostało więc ogłoszone „nowe otwarcie” *Open Platform Community*. Ma to być platforma, do której dosłownie każdy będzie mógł dodać swoje rozwiązanie, aplikację, produkt... Wzorując się na przełomowym projekcie Steve’a Jobsa i jego AppStore, szef Milestone ogłosił uruchomienie podobnej platformy wykorzystującej systemy dozoru wizyjnego. Ma ona wyjść poza zastosowania security – będzie bowiem zawierała rozwiązania dla handlu, marketingu, zarządzania nieruchomościami itp. Zawartość platformy – podobnie jak AppStore – będzie zależała od współtworzącej ją „społeczności”. I podobnie jak w sklepie Apple, pozwoli wszystkim popularyzować własne produkty i na nich wspólnie zarabiać. W tym Milestone widzi przyszłość rynku, stawiając sobie za cel współtworzenie WSZYSTKICH systemów dozoru wizyjnego na świecie!

Podczas konferencji Milestone zaprezentował także najnowszy produkt firmy – drugą generację (R2) sztandarowego XProtect. Najważniejsze cechy nowej wersji platformy to *Highest VMS Performance*, umożliwiający większą prędkość rejestracji na serwerze (do 3,1 Gb/s.) oraz nowe funkcje podnoszące poziom bezpieczeństwa sieciowego.

PRZYSZŁOŚĆ WEDŁUG MILESTONE

O trendach na rynku security i przyszłości polskiego oddziału firmy opowiedział nam **Anders Johansson**, dyrektor na Europę Środkowo-Wschodnią. Rozmowa odbyła się podczas konferencji MIPS w Dubaju.

www.aspolska.pl/wywiad-przyszlosc-rynku-security-wg-milestone



AVIOTEC firmy Bosch z kolejną nagrodą

System wykrywania pożaru AVIOTEC firmy Bosch został uznany za najlepszy produkt w kategorii „Technologiczna ochrona przeciwpożarowa”, zdobywając nagrodę FeuerTRUTZ Fire Protection of the Year 2017.

Przyznając wyróżnienie, „Ochrona przeciwpożarowa 2017”, FeuerTRUTZ Network już po raz siódmy nagrodziła produkty branżowe w kategoriach: technologiczna, architektoniczna i strukturalna ochrona przeciwpożarowa. Zwycięzców ogłoszono podczas branżowych targów

FeuerTRUTZ 2017 w Norymberdze w Niemczech. Zwycięzcy oraz zdobywcy najwyższych notowań miejsc w poszczególnych kategoriach zostali wyłonieni na podstawie ankiet internetowych oraz oceny profesjonalnego jury. Dla systemu AVIOTEC jest to już piąte wyróżnienie. System wykrywania pożaru AVIOTEC oparty na technologii wideo zapewnia optymalne wsparcie w sytuacjach, gdy nie sprawdzają się konwencjonalne systemy wykrywania pożaru. Obraz z kamery, na którym widać

potencjalne zagrożenie, pozwala szybciej wykryć ogień i dym niż konwencjonalna technologia wykrywania pożaru. Dzięki temu można bezzwłocznie podjąć działania zaradcze. System AVIOTEC znajduje zastosowanie przede wszystkim w obiektach o wysokich stropach, takich jak magazyny, hale produkcyjne, hangary czy kompleksy budynków. Można go także instalować tam, gdzie do tej pory nie stosowano rozwiązań przeciwpożarowych, np. w tartakach lub zakładach odzysku surowców.



Fot. Bosch

ALARMTECH

AKUSTYCZNY DETEKTOR ZBICIA SZYBY z funkcją aktywnego antymaskingu

zgodny z EN 50131-2-7-1:2013

GRADE 3

potwierdzone przez VdS

www.alarmtech.pl

POLSKI MISTRZ
TECHNIKI ALARMOWEJ
2016

Główna Nagroda
ZŁOTA ZBROJA



AD 800-AM



Fokus na detale – nowości w serii AXIS P13



Trzy nowe kamery z linii AXIS P13 umożliwiają efektywny doзор otwartych przestrzeni przy zachowaniu najwyższej jakości obrazu (pełnoklatkowość w rozdzielczości 4K). Urządzenia zostały zaprezentowane podczas targów ISC West (Las Vegas) w kwietniu 2017 r.

Przeznaczona do użytku wewnętrznego kompaktowa kamera AXIS P1367 oraz zewnętrzne kamery AXIS P1367-E oraz AXIS P1368-E to najnowsze urządzenia z ceniowej serii

AXIS P13. Dzięki wyższej czułości, lepszej jakości obrazu oraz większej liczbie klatek na sekundę w rejestrowanym materiale dostarczają strumień wideo w rozdzielczości do 4K z rozległych przestrzeni nawet przy niekorzystnych warunkach oświetleniowych. Kamery zaprojektowano do zastosowania w systemach monitoringu miejskiego, a także w rozwiązaniach dla transportu i handlu, (dozór parkingów, dworców kolejowych, uczęszczanych rejonów miast). Modele AXIS P1367-E mogą pracować z obiektywami CS oraz i-CS, model AXIS P1368-E z wbudowaną optyką i-CS zapewnia rozdzielczość do 4K. AXIS P1367-E i AXIS P1368-E

zostały opracowane do pracy na zewnątrz. Mają innowacyjną platformę mechaniczną – rozwiązanie zapewniające łatwiejszy dostęp i jednocześnie więcej miejsca na obiektyw. Wbudowane szyny zwiększają możliwości pracy kamer i umożliwiają instalację obiektywów zmiennoogniskowych. *Lekkie kamery AXIS P1367-E i AXIS P1368-E to doskonały przykład kamer przygotowanych do pracy na zewnątrz. To nie jest zwyczajna kamera w obudowie. Tym razem opracowaliśmy kamerę z obiektywem CS Mount od podstaw. Udało nam się zbudować rozwiązanie wykorzystujące obiektywy zmiennoogniskowe oraz format Axis Corridor umożliwiający obserwację wąskich, pionowych scen. Dzięki temu można wyeliminować*

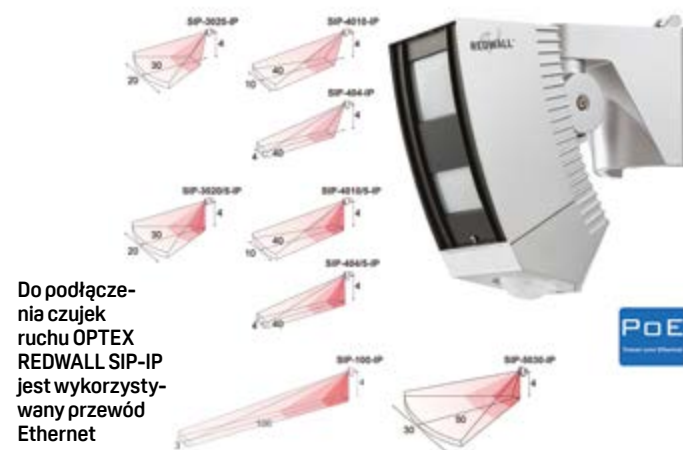
niepotrzebne obszary w obrazie i ograniczyć wielkość przesyłanego materiału – wyjaśnia Andres Vigren, Global Product Manager odpowiedzialny za kamery kompaktowe w Axis Communications. Nowe urządzenia serii AXIS P13 będą dostępne w kanałach dystrybucyjnych Axis w drugim kwartale 2017 r. Podczas ISC West, największych targów branży security w USA, Axis zapowiedział kolejne premiery, m.in. nowego sieciowego detektora radarowego, będącego doskonałym uzupełnieniem istniejących wizyjnych systemów dozoru otwartych przestrzeni, takich jak okolice magazynów czy plac budów, które wymagają całodobowego nadzoru.



SIP-IP wsparcie systemów monitoringu

Czujki SIP-IP mają opinię jednych z najlepszych czujek na świecie. W stosunkowo niskiej cenie otrzymuje się urządzenie wykorzystujące inteligentną logikę detekcji w technologii PIR. Czujki wspierają funkcjonalność detekcji ruchu w kamerach w warunkach ograniczonej widoczności czy zakłóceń powodowanych np. przez insekty, opady itp. Czujki serii SIP mają charakterystyki detekcji powierzchniowej oraz kurtynową i zasięg od 30 do 100 m. Konfigurację systemu ułatwia charakterystyka zasięgu czujek dopasowana do kątów widzenia obiektywów

kamer dozoru. Analiza sygnałów przebiega w dedykowanych mikroprocesorach z zaawansowanym algorytmem detekcji. Rozdzielenie torów obróbki sygnału dla poszczególnych kanałów umożliwia niezależne sterowanie w każdej strefie: czułości detekcji, pracę w trybie AND lub OR albo wyłączenie strefy dalekiej. Niezależne wyjścia alarmowe NC są podłączane do kodera PIE-1. Ochronę przed wandalizmem zapewnia obudowa ze wzmocnionego poliwęglanu, aktywny uchwyt sygnalizujący sabotaż przy zmianie położenia czujki (zerwanie, odwrócenie). Wy-



Do podłączenia czujek ruchu OPTEX REDWALL SIP-IP jest wykorzystywany przewód Ethernet

sokość montażu 4 m utrudnia dostęp do urządzenia. Każda czujka ma układ antymaskingu w technologii podczerwieni. W strojeniu czujek pomagają opcjonalny wizjer i dźwiękowy tester przejścia, ułatwiające zlokalizowanie źródeł fałszywych alarmów spowodowa-

nych np. ustawieniem strefy detekcji poza ogrodzeniem ochraniającego obiektu. Integracja za pomocą oprogramowania do dozoru wizyjnego obejmuje wiodące rozwiązania Milestone, Genetec, Axxon, Exa, Avigilon, Siemens i Mirasys, a teraz również Bosch.



Partnerstwo Hanwha z NVIDIA

Hanwha Techwin Security Business Group (wcześniej Samsung Techwin) zawarła umowę o globalnej partnerskiej współpracy z firmą NVIDIA, liderem technologii sztucznej inteligencji (AI). Wzmocni to konkurencyjność produktów i rozwiązań z dziedziny zabezpieczeń opartych na sztucznej inteligencji. NVIDIA jest pionierem w dziedzinie nowoczesnej grafiki komputerowej. Zajmuje pierwszą pozycję pod względem produkcji kart graficznych. Wytwarza procesory graficzne do komputerów, robotów i samochodów autonomicznych oparte na algorytmach głębokiego uczenia (Deep Learning). Ma siedzibę w Stanach Zjednoczonych. Globalne partnerstwo pozwoli firmom Hanwha Techwin i NVI-

DIA na planowanie współpracy nad platformą inteligentnej analizy wideo, którą NVIDIA obecnie rozwija. Platforma obejmie procesory graficzne zastosowane w urządzeniach zabezpieczających (kamerach i nośnikach pamięci masowej). Szybka, dokładna analiza danych wideo dostarczy klientom istotnych informacji. Hanwha Techwin skoncentruje się na rozwoju kamer AI i urządzeń pamięci masowej, autonomicznie wykrywających nietypowy ruch i sytuacje dzięki wykorzystaniu platformy NVIDIA. Platformę można też zastosować w różnych rozwiązaniach Hanwha Techwin, w tym w systemie monitorowania miast, dozoru wizyjnym punktów sprzedaży detalicznej, ruchu pojazdów itd.



Szkolenie w Linc Polska

Linc Polska zaprasza na szkolenie techniczne Wavestore.

Szkolenie odbędzie się 28 czerwca w Poznaniu. Jego celem jest przybliżenie oprogramowania Wavestore, przeznaczonego do integrowania kamer IP i analogowych różnych producentów (m.in. MOBOTIX i FLIR) w jeden spójny, funkcjonalny system. Podczas szkolenia zostaną omówione najważniejsze cechy platformy Wavestore, niezbędne do zrozumienia istoty jej działania, a także atuty

tego rozwiązania świadczące o jego przewadze rynkowej. To wiedza bardzo pomocna projektantom systemów zabezpieczeń, przydatna również w trakcie rozmów z potencjalnymi klientami. Od strony technologicznej szkolenie będzie wspierane przez firmę Qnap. Zostaną zaprezentowane m.in. możliwości instalacji oprogramowania Wavestore w środowiskach wirtualnych. Linc Polska zachęca też do udziału w webinarach. Rejestracja na: www.linc.pl/szkolenia

GUNNEBO®
For a safer world



SafeCash
Retail Deposit
High Speed

**AUTOMATYZACJA PROCESÓW
GOTÓWKOWYCH
W SIECIACH HANDLOWYCH**

Kalisz, ul. Fryderyka Chopina 20-22
+48 62 768 55 70
polska@gunnebo.com
www.gunnebo.pl



Wideodomofony IP firmy Dahua

Dahua Technology wprowadziła do oferty wideodomofony IP, które pracują z wykorzystaniem zarówno sieci kablowej Ethernet, jak i Wi-Fi. Stacja bramowa VT0211D-WP zawiera dwie karty sieciowe (Ethernet z interfejsem RJ45 oraz łączności bezprzewodowej Wi-Fi). Po prostym skonfigurowaniu i podaniu zasilania może być natynkowo zainstalowana przy bramie lub drzwiach wejściowych. Stację wyposażono w kamerę cyfrową o rozdzielczości 1 Mpx oraz obiektyw o ogniskowej 2,2 mm i szerokim kącie widzenia (125° x 105°). Moduł ma też wbudowany czytnik kart Mifare ułatwiający dostęp stałym użyt-

kownikom. Całość zamknięto w estetycznej obudowie o wysokiej klasie szczelności. Stacja VT0211D-WP może być zastosowana na dwa sposoby: współpraca tylko przez aplikację mobilną, bez potrzeby wewnętrznego monitora oraz z możliwością wykorzystania wewnętrznego monitora. W pierwszym przypadku sygnał dzwonienia poprzez Internet i aplikację mobilną dociera do użytkownika, który może sprawdzić, kto stoi przed drzwiami, może porozmawiać i ewentualnie otworzyć drzwi. W drugim przypadku funkcja dzwonienia grupowego umożliwia wysłanie sygnału zarów-



no na telefon komórkowy abonenta, jak i na skonfigurowany odpowiednio monitor. Do wyboru są dwa monitory dotykowe o przekątnej 7": VTH5221D (czarny) lub VTH5221DW (biały). Oróż funkcji wideodomofonu monitory mogą integrować alarm wewnętrzny (6 wejść i 1 wyjście) oraz podgląd z kamer IP pracujących w sieci wewnętrznej. Po doposażeniu monitora w opcjonalną kartę micro SD osoby dzwoniące będą mogły pozostawić

wiadomość. Oba urządzenia, tzn. stacja bramowa i monitor, mogą być zasilane przez złącze sieciowe w standardzie PoE. System jest prosty w konfiguracji i instalacji, łatwy w obsłudze, a co najważniejsze – spełnia oczekiwania wymagających użytkowników. Więcej informacji na: www.dahuasecurity.com



Dyski WD z optymalizowanymi do systemów niskoprądowych

Seria WD Purple została zaprojektowana i wyprodukowana specjalnie pod kątem wysokich wymagań odnośnie do nośników danych w systemach monitoringu wizyjnego, zwłaszcza z zastosowaniem rejestratorów NVR. Standardowy dysk twardy nie jest przeznaczony do zapisu i odczytu danych w warunkach pracy ciągłej 24/7. Oprócz tego zwykłe dyski co jakiś czas przerywają transmisję,

by skalibrować pracę głowic, np. ze względu na nagrzewanie się. Dyski przeznaczone do macierzy czy systemów wideo powinny być również bardziej odporne na wibracje, które zakłócają stabilność pozycji głowicy. Dyski serii WD Purple umożliwiają obsługę systemów do 8 zatok i z maks. 64 kamerami HD. Nowa specyfikacja dysków WD Purple została zoptymalizowana programowo i sprzętowo pod kątem ciągłej pracy, zapewniając stabilny transfer. Dyski twarde marki Western Digital wykorzystują technologię IntelliSeek odpowiadającą za zmniejszenie wpływu wszelkich negatywnych

czynników, takich jak drgania czy zakłócenia, które mają źródło w otoczeniu urządzeń dozorczych wizyjnego. Dysk twardy WD Purple 3,5" został wyposażony w wysokiej jakości elementy odporne na zużycie. Jego cechą charakterystyczną jest zminimalizowane zużycie energii (3,3 W podczas zapisu/odczytu przy pojemności 1 TB) i przystosowanie do ciągłej pracy w skrajnych temperaturach: od 0°C do 65°C podczas pracy i -40°C do 70°C w spoczynku. Zdolność do obciążenia danymi w przypadku WD Purple kształtuje się na poziomie dysków klasy enterprise i wynosi 180 TB na rok. AllFrame – autorska technologia Western Digital – zapewnia bardzo dużą prędkość zapisu danych na dysk WD Purple.

Rozwiązanie to wykorzystuje komendy transmisji strumieniowej typu ATA, co znacząco wpływa na zmniejszenie straty klatek (klatki na dysku w rejestratorze nie wypadają, czyli wszystkie są poprawnie zapisane). Zastosowanie najnowszych technologii wpływa również pozytywnie na ogólną jakość odtwarzania strumieniowego wykorzystywanego w systemach dozoru wizyjnego. Dyski twarde serii WD Purple są dostępne w pojemnościach: 500 GB, 1 TB, 2 TB, 3 TB, 4 TB, 5 TB, 6 TB, 8 TB, 10 TB. Urządzenia są objęte 3-letnią ograniczoną gwarancją, która zapewnia bezpieczeństwo materiału wideo niezależnie od tego, gdzie znajduje się jego właściciel.



ŚNIADANIE EKSPERTÓW



Bezpieczne miasto

dyskusja o bezpieczeństwie w luźnej atmosferze

ZAPRASZAMY:

- » specjalistów z zakresu smart/safe city
- » przedstawicieli samorządów zainteresowanych kwestiami bezpieczeństwa
- » przedstawicieli straży miejskich
- » operatorów monitoringów wizyjnych
- » security managerów z firm i instytucji zajmujących się bezpieczeństwem w mieście

23 czerwca 2017 r.
godz. 9.00–12.00
Hotel Westin Warszawa

Uczestnictwo w śniadaniu
jest **bezpłatne!**

Rejestracja: www.aspolska.pl/sniadanie

organizator:



partnerzy:



Estetyczny faraon czyli renesans murów

Monumentalizm aż do granic śmiesznego piękna nie umiera nigdy. Na przykład egipskie piramidy zbudowane dla ochrony w zaświatach królewskiej pozycji nieboszczyków i Wielki Mur Chiński dla odstraszenia wrogów za murem, ale i demonów.



Marzenie senno-wyborcze czterdziestego piątego prezydenta USA – przecież przedsiębiorcy budowlanego – trochę można porównać do tego ostatniego. Z ponad 20 tys. km Wielkiego Muru Chińskiego pozostało „tylko” 2,4 tys. To mniej niż rodzący się „mur Trumpa”, bo od oceanu do oceanu południowa granica USA ma ponad 3,3 tys. km. Mury pną się do góry? Ten starożytny budowlano-mechaniczny sposób ochrony granic, osiedli i obiektów budowlanych przeżywa renesans. Oczywiście nie jako prymitywne, ziemne czy murowane bariery, ale wyposażone w urządzenia detekcji optoelektronicznej budowle z betonu i stali, ogrodzeniowe konstrukcje prętów i płaskowników oraz zasieki z ostrej jak brzytwa concertiny. Nie tak dawno odnowicielem murów został Izrael na granicy ze Strefą Gazy. W Europie są i mniejsi faraonowie, np. Orban budujący ogrodzenie na granicy z Serbią. W USA Donald Trump nie jest pionierem. Były już tam pomysły wzniesienia barier nawet na granicy z bogatą Kanadą, bo ochrona tej najdłuższej na świe-

cie lądowej granicy międzypaństwowej (blisko 9 tys. km) jest iluzoryczna. Są odcinki zapór na granicy z Meksykiem mające ograniczyć nielegalną imigrację, przemyt narkotyków i swobodę działania mafii. Ale pod nimi ujawnia się tunele, w tym oświetlone i z klimatyzacją. Zwykli desperaci wspinają się na mury, wielu tę barierę udaje się pokonać sposobami chałupniczymi. I to pomimo tego, że U.S. Border Patrol używa systemów telewizji dozorowej, kamer na podczerwień, czujników ruchu, a granicę patrolują samochody terenowe i helikoptery. Media donosiły, że koniec marca tego roku miał być ostatnim terminem rejestracji firm chętnych do budowy „muru Trumpa”. Do przetargów zgłosiło się ponad 600... Imponująca liczba, ale mur ma mieć ponad 3 tys. km. Inwestycja – tak myślę – wymaga wielu centrów monitorowania i nadzoru. A ile sprzętu! Ciekawe ile kamer będzie potrzebne? Prasa podała „techniczne” wymagania Białego Domu, po lekturze aż się śmiecieć. Mur o wysokości od 5,5 do 9 m powinien uniemożliwiać wspinanie się po nim, kopanie

pod nim i być „miły dla oka od strony... amerykańskiej”. Kto płaci, ten jest większym estetą, choć do wyłożenia 10 czy 20 mld dolarów jakby nie ma chętnych. Na dodatek inwestycja na miarę faraona może zdać się psu na budę. Już widzę taką sytuację: sygnał przemytników np. „1134 km wschód, droga powietrzna”. Przyjeżdża samochód, dwóch ludzi w kilka minut składa nie-dużą „bezelektroniczną” procę lub katapultę. Możliwe że dano wcześniej „w łapę” operatorowi centrum nadzoru, aby zmogła go senność. Może systemy alarmowe i telewizyjne zauważą przemyt, ale zanim ochrona dotrze w odległe miejsce... Atakuje się już wszystko, bo prawie wszystko ma związek ze światem cyfrowo-sieciowym. Rozwija się inteligentne budownictwo. Zastanawiało mnie, dlaczego nie słyszę jeszcze sygnałów o alarmach na tę infrastrukturę, nasyconą przecież rozwiązaniami technicznymi. Zabezpieczenia są tak dobre, czy administratorzy obiektów ukrywają incydenty? A stopień ryzyka cyberataków jeszcze wzrośnie wraz z rozwojem Internetu Rzeczy. W ubiegłorocznych informacjach prasowych pisano o incydencie w Finlandii. W mieście Lappeenranta hakerzy zablokowali system ogrzewania i dostawę ciepłej wody do

dwóch inteligentnych apartamentowców. Atak DDoS spowodował reset systemu informacyjnego i jego zawieszenie.

Teraz o decyzji europarlamentu mogącej oszczędzić rocznie 2,5 tysiąca ludzi w Europie, bo poprawiającej sprawność służb ratunkowych. Od końca marca 2018 r. nowe samochody osobowe i małe dostawcze sprzedawane w krajach UE będą musiały mieć urządzenie alarmowe systemu e-Call. Automatycznie poinformują przez numer 112 centrum ratunkowe o wypadku i podadzą niezbędne dane. Producenci urządzeń muszą zapewnić, że ich konstrukcja umożliwi później usunięcie tych danych (ochrona prywatności).

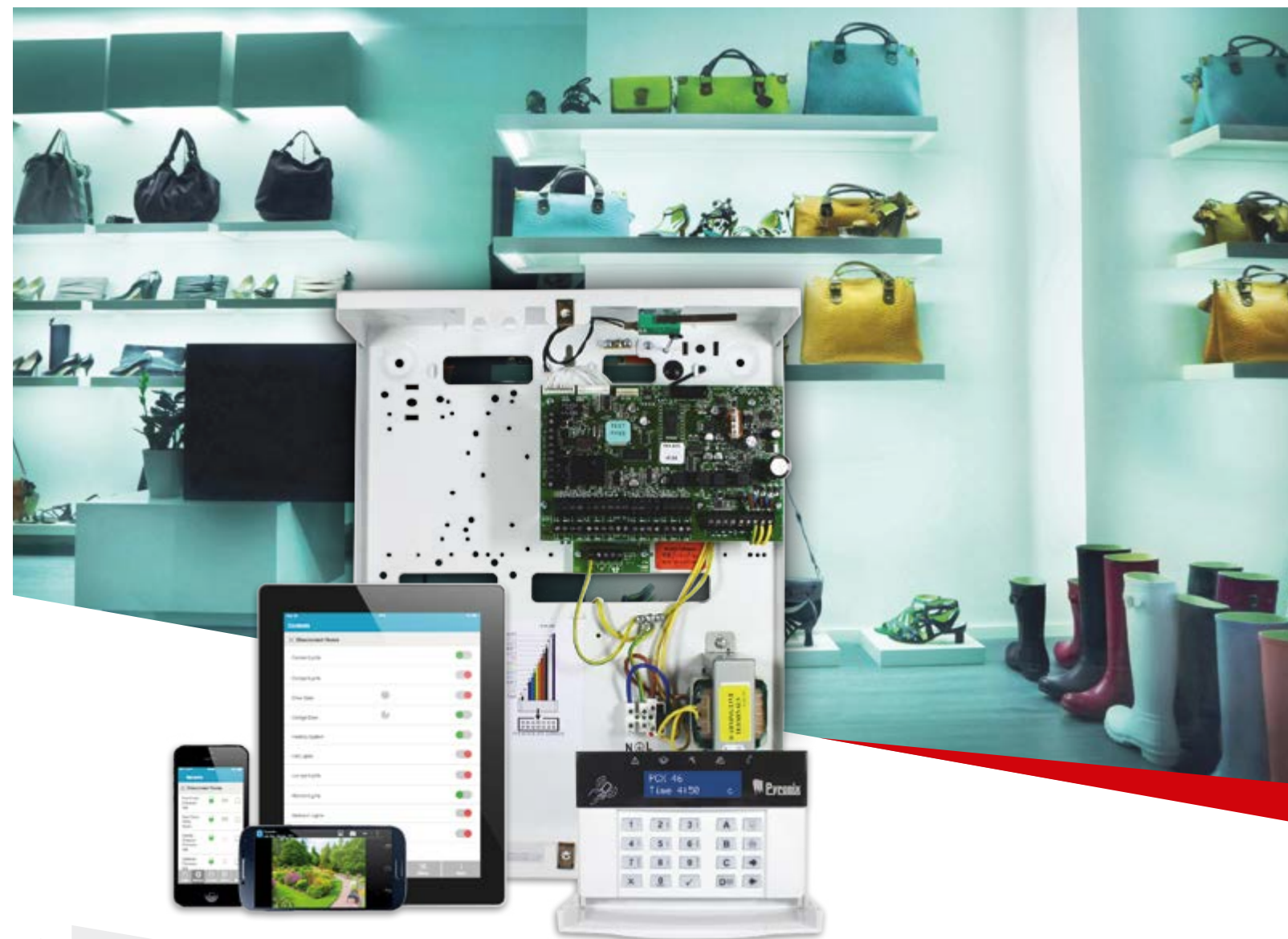
Według CERT Polska (zespołu działającego przy NASK), corocznie przedstawiającego raport o cyberbezpieczeństwie, najczęstszą metodą przestępców komputerowych w Polsce w 2016 r. był *phishing* (722 tys. zgłoszeń). To podszywanie się pod osobę lub instytucję w celu kradzieży tożsamości albo wyłudzenia informacji, np. loginów, haseł, numerów kart kredytowych. Główny motyw działania sprawców był banalny, ale nie dla poszkodowanych. ■

BIO

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

PCX46 APP

Pyronix
HIKVISION



Hybrydowy system alarmowy z aplikacją Adaptowalny, funkcjonalny i pełen cech

PCX 46 APP jest profesjonalnym rozwiązaniem wysokiej klasy bezpieczeństwa z komunikacją IP. Przewodowe i bezprzewodowe, dwukierunkowe akcesoria powodują, że instalacja jest szybka i łatwa, a wszystko z obsługą przez aplikację HomeControl+, dającą użytkownikom pełną kontrolę nad ich systemem z dowolnego miejsca świata!



4K

Now Available over COAX

Leading end-to-end 4K Ultra HD over Coax

HDCVI 4.0 4K

- Kamera kompaktowa 4K: doskonała jakość obrazu dzięki przetwornikowi Starlight+ o rozmiarze 4/3"
- Kamery tulejowe i kopułowe 4K: zasięg podczerwieni 100m / 50m, wysoki stopień ochrony IP67 i IK10
- Wieloprzetwornikowa kamera panoramiczna: widok 180° oraz obraz 3x 2 Mpx jednocześnie
- Kamera Fisheye 4K: panoramiczny widok 360°, 10 trybów prostowania obrazu z HCVR
- HCVR: kompatybilność wsteczna ze wszystkimi kamerami HDCVI
- Transmisja do 500 m przez RG59 oraz do 300 m przez CAT5e, łatwość rozbudowy istniejących systemów



HAC-HF3805G
4/3" 4K HDCVI
Kamera Starlight+



HAC-HFW3802E-Z
4K HDCVI WDR
Kamera tulejowa IR



HAC-PFW3601-A180
4K HDCVI Multi-sensor
Kamera Panoramiczna IR



HAC-EBW3802
4K HDCVI
Kamera Fisheye IR

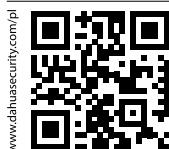


HAC-HDBW3802E-Z
4K HDCVI WDR
Kamera kopułowa IR



HCVR7000-4K
Rejestrator 4K HDCVI

CE FC CCC UL RoHS ISO 9001:2000



www.dahuasecurity.com/pl

Dahua Technology Poland Sp. z o.o.

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