a&S POLSKA
www.aspolska.pl

CZASOPISMO RYNKU SECURITY
nr 5/2017
wrzesień/październik
15 zł (w tym 8% VAT)

TEMAT NUMERU

Jesteśmy świadkami rewolucji przemysłowej. Co przyniesie? Roboty, widzenie maszynowe i inteligentne czujniki to tylko początek...

str. 18

ISSN 2451-5175
09
9 772451 517703

KAMERY 4K

Magia wysokich rozdzielczości

Pojawienie się kamer o wysokich rozdzielczościach to dopiero początek fascynujących zmian w telewizji dozorowej.

str. 52

TRENDY

Nowoczesna kontrola dostępu

Nadszedł czas dynamicznego rozwoju! Do 2020 r. rynek KD będzie większy od rynków telewizji dozorowej i sygnalizacji włamania i napadu.

str. 86

SMART HOME

Technologie inteligentnego domu

Specjaliści z rynku zabezpieczeń technicznych coraz częściej i śmielej spoglądają w kierunku inteligentnych domów.

str. 80

EASY IP 3.0

Hikvision oferuje kompletny, innowacyjny i opłacalny profesjonalny system monitoringu wizyjnego Easy IP 3.0 HD, który cechuje się prostotą instalacji i podłączenia do sieci, a także łatwością przechowywania i odtwarzania nagrań. System ten pozwala mieć pewność, że cała nieruchomość jest dobrze chroniona. Poznaj korzyści, jakie daje monitoring IP i wkrocz z nami w nową erę monitoringu wizyjnego.

Kluczowe cechy:

- Lepsza kompresja wideo H.265+
- Jeszcze lepsze oświetlenie dzięki EXIR 2.0
- Pełna gama rozdzielczości, aż do 4K UHD
- Technologia Darkfighter
- VCA (analiza zawartości obrazu)
- Obiektywy z autofokusem sterowane silnikami
- IP67
- IK10

HIKVISION

TURBO HD 4.0
NOWE REWOLUCYJNE ROZWIĄZANIE

8 MP W ANALOGU

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

www.hikvision.com

Drodzy Czytelnicy

Bezpieczeństwo obiektów przemysłowych to niezwykle istotna sfera, zwłaszcza w czasach wielkich przemian, jakie zachodzą obecnie w przemyśle. Mówi się, że jesteśmy świadkami kolejnej rewolucji przemysłowej, która zaowocuje inteligentnymi fabrykami naszpikowanymi elektroniką i nowoczesnymi technologiami (s. 18). Te przemiany, a także nieznane dotychczas rodzaje zagrożeń wymuszają zmiany w stosowanej koncepcji zabezpieczeń – o tym pisze **Jacek Grzechowiak, nowy członek naszego kolegium redakcyjnego** (s. 22). Nie można przy tym zapominać o nowych sposobach zabezpieczeń technicznych – zarówno w ochronie obwodowej (s. 26), jak i w zakresie bezpieczeństwa pożarowego, niezwykle ważnego dla tego sektora rynku (s. 38).

Duży akcent położyliśmy w tym wydaniu na coraz bardziej popularne **kamery 4K; zalety, ale i pułapki związane ze stosowaniem wysokich rozdzielczości** opisuje Jan T. Grusznic (s. 52). Prezentujemy także obszerny przegląd oferty rynkowej kamer 4K wiodących producentów (s. 64). Praktycy z zakresu telewizji dozorowej nie mogą też przeoczyć **artykułu Macieja Grządkowskiego nt. oświetlenia sceny** (s. 72).

Rynek zabezpieczeń technicznych rozwija się dynamicznie w zakresie zastosowań *stricte* security, ale swoją szansę dostrzega również w innych sektorach. Naturalnym rynkiem dla firm tej branży jest zdobywający coraz większą popularność *smart home*. **Technologie inteligentnego domu** mogą zatem stać się motorem rozwoju firm security (s. 80). Ciekawe są też trendy obserwowane w kontroli dostępu, która do 2020 r. pod względem wielkości ma prześcignąć rynki telewizji dozorowej oraz sygnalizacji włamania i napadu. **O kierunkach rozwoju KD** piszemy na s. 86.

Tradycyjnie polecamy także dział Bezpieczeństwo biznesu – tym razem Michał Czuma pisze **o (cyber)nieostrożności w cyberbezpieczeństwie** (s. 96), a Marek Blim porusza niezwykle dziś ważną kwestię zmian wynikających z **konieczności wdrażania RODO** (s. 102). Wielu Czytelników zainteresuje poradnik, krok po kroku opisujący, jak zlikwidować stanowisko **pełnomocnika ds. ochrony informacji niejawnych** (s. 108).

Nowe technologie wkraczają także do mediów. Można nas czytać nie tylko w wersji drukowanej – wszystkie wydania „a&s Polska" są dostępne bezpłatnie na naszej **aplikacji mobilnej w AppStore i Google Play.** Ponadto aktualne informacje z rynku security zamieszczamy na portalu **www.aspolska.pl**

Nie tylko publikujemy ciekawe artykuły merytoryczne i najważniejsze informacje z życia branży, ale także łączymy uczestników rynku security i osoby zainteresowane tematem podczas organizowanych przez nas spotkań. Osoby związane z poszczególnymi rynkami wertykalnymi zapraszamy na **śniadania ekspertów**. Ostatnie spotkanie – tak jak wydanie czasopisma – było poświęcone bezpieczeństwu w handlu (relacja na s. 16), na kolejnym (zaproszenie na s. 51) będziemy rozmawiali o bezpieczeństwie w przemyśle, które jest tematem tego numeru „a&s Polska".

Marta Dynakowska
redaktor naczelna

Mariusz Kucharski
dyrektor zarządzający

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
Jacek Grzechowiak
Roman Maksymowicz
Dariusz Mostowski
Przemysław Pierzchała
Janusz Sawicki
Stefan Jerzy Siudalski
Jerzy Sobstel
Paweł Wittich
Waldemar Wnęk
Aleksander M. Woronow

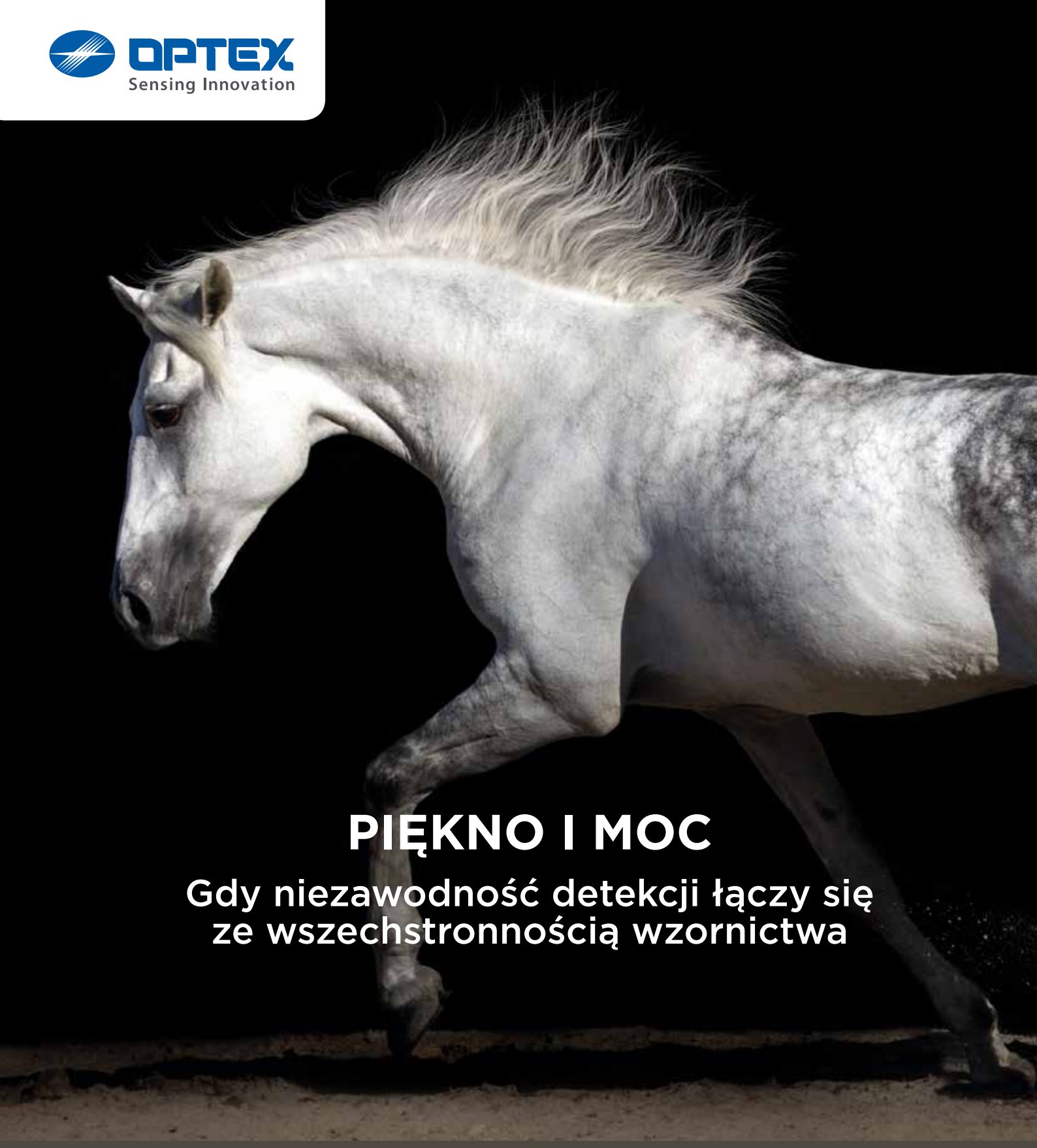
Korekta
Jolanta Kucharska

Projekt graficzny
Sylwester Dmowski

Skład
Dorota Cybulska
Sylwester Dmowski

Prenumerata
www.aspolska.pl/prenumerata

OPTEX
Sensing Innovation



PIĘKNO I MOC

Gdy niezawodność detekcji łączy się ze wszechstronnością wzornictwa

Seria VX Shield

12m, 90° zewnętrzna

PIR/PIR+MW

Seria VXI Shield łączy w sobie niezawodne technologie, z których słynie OPTEX, oraz ciekawy design. Jest to linia produktów łatwych w instalacji i konfiguracji. Obudowy w kilku wersjach kolorystycznych ułatwiają dopasowanie czujek do wymagań użytkownika. Seria VXI Shield oferuje modele zasilane zarówno przewodowo jak i bateryjnie, przez co z łatwością znajdują one zastosowanie w ochronie budynków mieszkalnych i komercyjnych.

OPTEX od prawie 40 lat projektuje i produkuje urządzenia detekcyjne stosowane w branży urządzeń alarmowych, systemach automatyki budynkowej, automatyce przemysłowej oraz ochronie środowiska.

Więcej informacji na www.optex.com.pl

OCHRONA WEWNĘTRZNA | OCHRONA ZEWNĘTRZNA | LICZENIE PRZEPŁYWU LUDZI | KONTROLA DOSTĘPU

W numerze...

TEMAT NUMERU

RAPORT
STR. 18

BEZPIECZEŃSTWO BIZNESU

OCHRONA INFORMACJI NIEJAWNYCH

SERWIS INFORMACYJNY

Kontrola dostępu
STR.94

Włamania do systemów kontroli dostępu

Rynek security
STR.72

Więcej światła... a może mniej czyli o oświetleniu planu

Bezpieczeństwo biznesu

STR. 102

RODO

Jak nadzorować prowadzenie i ochronę zbiorów danych osobowych

Aktywny konwerter xCOAX do transmisji Ethernet oraz PoE po przewodzie koncentrycznym

Atte
www.atte.pl

ASET-xCOAX to zestaw aktywnych konwerterów umożliwiający montaż kamer IP PoE w miejscach, gdzie wymiana istniejącego okablowania koncentrycznego jest niemożliwa bądź nieopłacalna. Moduł xCOAX-1-10-HS SWITCH po podłączeniu do dowolnego switcha PoE (port RJ45) zasila się automatycznie i za pośrednictwem kabla koncentrycznego umożliwia dwukierunkową komunikację sieciową oraz zasilanie modułu xCOAX-1-11-HS CAMERA. Kamerę bądź inny odbiornik PoE dołączamy do portu RJ45 modułu xCOAX na końcu linii.

Dane techniczne:

- porty LAN 10/100 Mb/s, auto MDI-MDIX, autonegocjacja
- obsługiwane nadajniki PoE 802.3af - do 15,4 W, 802.3at – do 30 W (domyślny), PoE PASSIVE – do 40 W
- długość kabla koncentrycznego 100 m dla RG59, 200 m dla RG-6
- wyjście PoE PoE PASSIVE/mode B (4,5+) (7,8-)

Najważniejsze cechy i funkcje:

- niewielkie rozmiary modułów,
- zasięg transmisji po koncentryku do 200 m,
- możliwość zasilania ze switcha/adaptera PoE 802.3at/af lub PASSIVE (xCOAX-1-10-HS),
- możliwość zasilania odbiorników PoE 802.3at/af lub PASSIVE,
- do 40 W sumarycznej mocy w całym torze zasilania,
- wyraźna, optyczna sygnalizacja stanu zasilania i transmisji danych,
- łatwe i szybkie uruchomienie bez konieczności konfiguracji parametrów.

Obudowa HS (*Heat Shrink*) zapewnia izolację oraz możliwie jak najmniejsze gabaryty urządzenia. Niewielki rozmiar daje szerokie możliwości doboru miejsca montażu.

AXIS P13 – nowe modele kamer w rozdzielczości 5 Mpix i 4K

AXIS
www.axis.com/pl

Przeznaczona do użytku wewnętrznego kompaktowa kamera sieciowa AXIS P1367 (5 Mpix), a także opracowane pod kątem pracy na zewnątrz modele AXIS P1367--E (5 Mpix) i AXIS P1368-E (4K) to najnowsze produkty z cenionej serii urządzeń AXIS P13. Dzięki zwiększonej czułości, lepszej jakości obrazu oraz większej liczbie kl./s w rejestrowanym materiale zapewniają monitorowanie dużych przestrzeni z dużą rozdzielczością nawet przy niekorzystnych warunkach oświetleniowych. Kamery powstały z myślą o monitoringu miejskim, a także rozwiązaniach przeznaczonych do transportu i handlu, np. zatłoczonych parkingów, dworców kolejowych czy uczęszczanych rejonów miast.

Kamery AXIS P1367/-E mogą wykorzystywać obiektywy CS oraz i-CS, zaś AXIS P1368-E zapewnia rozdzielczość do 4K dzięki wbudowanej optyce i-CS. Mają także innowacyjne rozwiązania ułatwiające dostęp, które równocześnie zapewniają więcej miejsca na obiektyw. Wbudowane szyny zwiększają możliwości pracy kamer i umożliwiają instalację obiektywów zmiennoogniskowych.

Lekkie modele AXIS P1367-E i AXIS P1386-E to doskonały przykład kamer opracowanych do pracy na zewnątrz – wyjaśnia Andres Vigren, Global Product Manager odpowiedzialny za kamery kompaktowe w Axis Communications. – *To kompleksowy system z obiektywem CS Mount opracowany od podstaw. Dzięki temu udało nam się zbudować urządzenia, które mogą używać obiektywów zmiennoogniskowych czy pracować z wykorzystaniem formatu Axis Corridor Format pozwalającego na ograniczenie wielkości przesyłanego materiału oraz obserwacji zbędnych obszarów.*

Dozór wizyjny z lotu ptaka

Dahua Technology Poland
www.dahuasecurity.com/pl

Dahua Technology, wprowadzając kategorię UAV do swojej oferty, rozpoczęła nowy rozdział w dziedzinie bezpieczeństwa. Bezzałogowe statki powietrzne od wielu lat są wykorzystywane do celów militarnych, teraz zastosowanie tej techniki jest możliwe w cywilnych systemach bezpieczeństwa. Dron stanowi mobilny punkt monitoringu o nowych, nieosiągalnych wcześniej możliwościach dozoru. Wielowirnikowiec Dahua X820 został wyposażony w 4 wirniki generujące moc 768 W, co pozwala na zabranie w powietrze zaawansowanej technologicznie kamery, spełniającej najwyższe standardy systemów dozoru wizyjnego.

Dron X820 osiąga prędkość 90 km/h, a jego maks. wysokość lotu wynosi 1500 m. Może być wyposażony w 2 warianty kamer:
6 Mpix kamerę z przetwornikiem Starlight 1/1,9"i zoomem optycznym 30x zamontowaną na gimbalu stabilizacyjnym o dokładności do 0,01° oraz kamerę termowizyjną z przetwornikiem 640 x 512.

Sterowanie dronem umożliwia aparatura wyposażona w ekran dotykowy. Maksymalny dystans, na jaki dron może się oddalić od operatora, wynosi aż 5 km. Użytkownik ma też do dyspozycji mobilną stację PC do obserwacji obrazu z kamery oraz nadzorowania parametrów lotu. Pojemny akumulator litowo-polimerowy (LiPo 22 tys. mAh) zapewnia około 38 min lotu.

Zgodnie z obowiązującymi standardami dla tego typu statków powietrznych dron został wyposażony w moduł lokalizacji satelitarnej współpracujący z systemami GPS, Beidou i GLONASS. Współpraca z oprogramowaniem DSS pozwala na włączenie drona do zintegrowanego systemu dozoru wizyjnego.

@saltosystems

Nowy XS4 One:

INSPIRUJĄCA INNOWACJA

Witamy w nowym wymiarze kontroli dostępu!

Technologia – Zamek elektroniczny z wbudowaną najnowszą technologią bezprzewodowej kontroli dostępu.

Dostęp mobliny – Wbudowana technologia Wireless oraz klucz mobilny JustIN Mobile.

Wszechstronność – Nieskończone możliwości w dopasowaniu do wszelkiego typu drzwi.

Funkcjonalność – Bezpieczny i łatwy w użytkowaniu system bez klucza mechanicznego.

Design – Nowoczesny styl, który podkreśla estetykę całego obiektu.

Niezawodność – Gwarancja jakości SALTO Systems.

SALTO SYSTEMS
Tel.: +48 609 01 7777
Email: info.pl@saltosystems.com
www.saltosystems.pl

SALTO
inspired**access**

CALLISTO – komfortowe w instalacji rozwiązanie do domu i biura

EBS
www.callistoalarm.pl

Centrala alarmowa Callisto jest rozwiązaniem hybrydowym, które można dopasować do niemal każdego typu obiektu. 16 wejść bezprzewodowych (zamiennie 7 przewodowych i 9 bezprzewodowych), czujki dostępne w ofercie, przyjazne aplikacje mobilne zarówno dla użytkownika, jak i dla instalatora.
Rozwiązanie umożliwia programowanie online za pomocą telefonu komórkowego i bezpłatnej aplikacji AVA Install, co oszczędza czas i wpływa na jakość instalacji. Automatyczne dodawanie czujek poprzez odczyt kodów QR, możliwość wgrania gotowych szablonów instalacyjnych to tylko niektóre z niestandardowych funkcji aplikacji AVA INSTALL. Centrala spełnia wymagania normy PN-EN 50131, Grade 2.

Funkcje i zalety

- kod pod przymusem,
- funkcja STAY/AWAY umożliwiająca częściowe uzbrojenie alarmu,
- alarmowe klawisze funkcyjne: NAPAD / POMOC MEDYCZNA / POŻAR,
- możliwość zaprogramowania wiadomości SMS do 10 różnych użytkowników – ani typ telefonu, ani aplikacja nie ograniczają użytkownika,
- zintegrowana radiolinia i GPRS,
- elastyczny wybór między czujkami bezprzewodowymi a przewodowymi,
- zdalny dostęp do konfiguratora i podgląd statusu centrali – szybka zmiana parametrów, szybki i efektywny serwis,
- darmowe aplikacje dla użytkownika końcowego i instalatora – możliwość monitoringu przez agencję ochrony oraz jednoczesne korzystanie z aplikacji mobilnej AVA do sterowania systemem.

Kamera C3S Ezviz 1080p z obrazem na smartfonie

EZVIZ
www.ezviz.eu/pl

Małe punkty handlowe czy biura na ogół nie są szczególnie zagrożone, jednak ich właściciele chcą mieć wgląd w to, co się dzieje podczas godzin pracy, bądź wiedzieć, o której godzinie personel otwiera i zamyka sklep. Dysponując skromnym budżetem, oczekują prostego, a jednocześnie niezawodnego rozwiązania.
Kamera C3S firmy Ezviz doskonale spełnia te oczekiwania. Jej instalacja odbywa się w kilku prostych krokach: trzeba pobrać aplikację na smartfon, założyć konto, dodać kamerę skanując kod QR, i natychmiast uzyskuje się połączenie z obrazem live z kamery na smartfonie. Transmisja wideo odbywa się przez Wi-Fi, więc wystarczy kamerę zasilić i wybrać miejsce instalacji bez konieczności prowadzenia dodatkowych przewodów.

Dzięki aplikacji Ezviz mobile można na smartfonie na bieżąco sprawdzać, co dzieje się w sklepie czy biurze. Wideodetekcja ruchu powiadomi o wykrytym ruchu po godzinach otwarcia sklepu wraz z materiałem wideo w celu weryfikacji zdarzenia. Aplikacja Ezviz mobile wyświetla obraz z czterech kamer jednocześnie (każda może znajdować się w innej lokalizacji). Obraz może być rejestrowany na karcie microSD w kamerze lub w rejestratorze.

Główne parametry C3S: rozdzielczość 1080p, prędkość transmisji 25 kl./s adaptacyjna, WDR 120 dB, obiektyw stały 4 mm, kąt widzenia 90o, kompresja H.264, klasa szczelności IP66. C3S występuje w wersjach Wi-Fi oraz PoE.

System wideodomofonowy C5-IP

Genway
www.genway.pl

O systemie

C5-IP marki VidiLine to nowoczesny system wideodomofonowy w technologii IP z wbudowanymi systemami: kontroli dostępu, alarmowym oraz powiadomień SOS. Cechy, które wyróżniają system, to: brak ograniczeń odległości, wszechstronność zastosowań, szybkość wdrożenia oraz możliwość integracji z systemem CCTV IP. Podstawowy system wideodomofonowy składa się z niewielu elementów: panel zewnętrzny IP, dotykowy monitor IP oraz switch i zasilacz.

Brak ograniczeń

Skrętka czy światłowód? Wykorzystanie standardów sieci TCP/IP pozwala na nieograniczoną odległość pomiędzy urządzeniami, można wykorzystać istniejącą sieć lub wykonać dedykowaną do systemu wideodomofonowego. Wszystkie budynki można grupować w większe struktury w celu zamknięcia terenu i obsługi przez portiera lub ochronę.

Szybkie wdrożenie

Uruchomienie systemu sprowadza się do podłączenia sprzętu i nadania monitorom numerów lokali. Znajomość protokołu IP nie jest konieczna, gdyż adresy IP w sieci wideodomofonowej są nadawane automatycznie. Nasz system jest oparty tylko na jednym kablu sieciowym. Obraz, dźwięk, sterowanie i zasilanie PoE (*Power over Ethernet*) są przesyłane jednym kablem UTP kat. 5.

Integracja z kamerami IP

Lubimy czuć się komfortowo i bezpiecznie. Wszechobecne kamery stają się standardem. Nasz wideodomofon pozwala na integrację z systemem monitoringu IP, który pracuje zgodnie z protokołem ONVIF. Wystarczy podłączyć do systemu monitoringu bramkę CCTV systemu C5-IP, aby móc oglądać obraz z kamer na monitorze.

XDL12TT-AM

Dobrze dopasowana, zawsze chroni

Zaprojektowana, dopracowana, gotowa do działania

Nowa, o niskim montażu czujka XD łączy technologie Tri-Signal Detection Logic oraz Dual-Vision, co zwiększa zdolność detekcji, zapewniając przy tym niezawodną odporność na zwierzęta domowe. Spełniając wymagania stopnia bezpieczeństwa (Grade) 3. i 4. zapewnia niezawodną pracę i sprawne działanie w zastosowaniach zewnętrznych. Przy 90-stopniowym kącie pokrycia i montażu na wysokości 1,2 m nowa czujka XD zapewnia maksymalny zasięg detekcji 12 m.

Rejestrator iDS-9632NXI-I8/16S

Hikvision
www.hikvisionpoland.pl

Firma Hikvision wprowadziła na rynek pierwszy na świecie rejestrator NVR korzystający z funkcji *Deep Learning*. Ten inteligentny NVR został „nauczony", by wychwytywać osoby znajdujące się w polu widzenia kamer i dzięki temu odfiltrować fałszywe alarmy wywoływane przez ruchome obiekty tła, takie jak zwierzęta czy gałęzie. Ten nowy, 32-kanałowy rejestrator iDS-9632NXI-I8/16S jest pierwszym modelem z linii *Deep in Mind*. Fałszywe alarmy wywoływane przez poruszające się zwierzęta, liście, cienie, zmiany oświetlenia i inne nieistotne obiekty zakłócają pracę personelu ochrony, są czasochłonne i drogie. Dzięki zdolności wykrywania osób VNR iDS-9632NXI-I8/16S skutecznie je eliminuje.
Deep in Mind NVR identyfikuje zagrożenie i wyzwala alarm tylko w przypadku pojawienia się człowieka w obserwowanej scenie, z prawdopodobieństwem przekraczającym 90%. Jego wydajny procesor GPU wykonuje obliczenia, a zaawansowane algorytmy *Deep Learning* poprawiają dokładność identyfikowania intruza. Funkcje bazujące na technologii *Deep Learning* umożliwiają upoważnionym użytkownikom przeszukiwanie nagranych materiałów i znajdowanie celów znacznie szybciej niż tradycyjne NVR-y.
Deep in Mind jest wyposażony w 32 kanały wizyjne dla kamer IP (do 12 Mpix), 2 pary wyjść wideo, w tym HDMI o rozdzielczości 4K, funkcję RAID (0, 1, 5, 6 i 10) dla maks. 8 TB dysków twardych oraz 2 karty sieciowe zapewniające redundancję połączeń i podział systemu na dwie podsieci.
Wymiana standardowego rejestratora na nowy z serii *Deep in Mind* znacząco zwiększy wydajność standardowego systemu dozoru wizyjnego.

UPS-y z serii VFI RMG PF1

Impakt
www.impakt.com.pl

Tym razem popularny producent zasilaczy awaryjnych przygotował nowe rozwiązania dla biznesu czy instytucji publicznych – zasilacze awaryjne PowerWalker serii VFI RMG. Są one przeznaczone do montażu w szafach 19". Ich zastosowanie pozwala zyskać cenne minuty na wykonanie *backupu* danych czy bezpiecznego wyłączenia sprzętów, gdy w firmie dochodzi do poważnej awarii i przerwy w dostawie prądu.
Dzięki współczynnikowi mocy wynoszącemu 1.0, szerokiemu zakresowi mocy wejściowej i wsparciu dla generatora prądu zmiennego zasilacze cechują się wysoką jakością pracy nawet w niestabilnej sieci energetycznej. Ponadto UPS-y zawierają ładowarkę z opcją regulowania przepływu prądu, co pozwala użytkownikowi na szybsze naładowanie baterii.
Opisywane modele UPS-ów PowerWalker zostały wyposażone w nowy panel LCD. To na nim można odczytać szacowany czas działania urządzenia w trybie pracy na baterii *(battery mode)*. Część informacji jest ukazana w postaci diagramów, by ułatwić poznanie stanu urządzenia.
UPS-y z serii VFI RMG PF1 są dostępne w wersjach o mocy rzeczywistej: 1000 W, 1500 W, 2000 W i 3000 W.

Dane techniczne:

- Typ zasilacza: online
- Moc: 1000, 1500, 2000 i 3000 VA
- Współczynnik mocy: 1.0
- Napięcie: 160–300 VAC lub 110–300 VAC przy niskim stanie baterii
- Zakres częstotliwości: 40–70 Hz
- Częstotliwość: 46–55 Hz lub 54–66 Hz
- Wsparcie dla generatora prądotwórczego
- Wyświetlacz LCD
- Regulacja napięcia: ±1%

Zasilacze awaryjne serii VFI CG PF1

Impakt
www.impakt.com.pl

Popularny producent UPS-ów poszerzył swoją ofertę o nowe produkty, m.in. o przeznaczone do użytku komercyjnego.
Prezentowane UPS-y to desktopowe zasilacze typu online o współczynniku mocy 1.0. Parametry o takiej wartości mają znaczny wpływ na jakość działania urządzenia, zwłaszcza jeśli chodzi o rzeczywistą ilość energii zużytej do pracy.
Nowe urządzenia PowerWalker dysponują szerokim zakresem mocy wejściowej i wsparciem dla generatora prądu zmiennego. Mogą zatem pracować w warunkach, gdy sieć energetyczna jest niestabilna. UPS-y serii VFI CG PF zostały wyposażone w silniejszą ładowarkę z opcją regulowania przepływu prądu, użytkownik sam decyduje o wykorzystanej przez urządzenie energii.
Zasilacze VFI CG PF mają nowy panel LCD pokazujący m.in. szacowany czas działania urządzenia w trybie pracy na baterii (*battery mode*). Użytkownik będzie więc dokładnie wiedział, ile pozostało czasu do wyłączenia UPS-a. Oprócz tego niektóre informacje są przedstawiane w postaci czytelnych diagramów.
UPS-y z serii VF CG PF są dostępne w wersjach o mocy rzeczywistej 1000 W, 1500 W, 2000 W i 3000 W.

Dane techniczne:

- Typ zasilacza: online
- Moc: 1000, 1500, 2000 i 3000 VA
- Współczynnik mocy: 1.0
- Napięcie: 160–300 VAC lub 110–300 VAC przy niskim stanie baterii
- Zakres częstotliwości: 40–70 Hz
- Częstotliwość: 46–55 Hz lub 54-66 Hz
- Wsparcie dla generatora prądotwórczego
- Wyświetlacz LCD
- Regulacja napięcia: ±1%

Satel®
MADE TO PROTECT

INTEGRUM

ZINTEGROWANE ZARZĄDZANIE BEZPIECZEŃSTWEM

- **INTEGRUM to efektywny nadzór** nad rozproszonymi instalacjami bezpieczeństwa (systemami alarmowymi) dzięki możliwości połączenia wielu obiektów w jeden zintegrowany, skalowalny system.
- **INTEGRUM to wygodna, globalna administracja** zasobami ludzkimi dzięki jednej wspólnej bazie użytkowników wszystkich obiektów.
- **INTEGRUM to obsługa** systemu **z dowolnego miejsca na świecie**, także z urządzeń mobilnych.
- **INTEGRUM to podgląd** stanu systemu **w czasie rzeczywistym** oraz czytelna **wizualizacja** sytuacji **na mapach**.
- **INTEGRUM to realne oszczędności** dzięki obniżeniu kosztów obsługi zarządzania rozproszoną strukturą obiektów.

Zarządzanie systemami bezpieczeństwa łatwe jak nigdy dotąd!

SATEL sp. z o.o.
ul. Budowlanych 66, 80-298 Gdańsk, tel.: (58) 320-94-35, e-mail: integrum@satel.pl, integrum.satel.pl

Ekonomiczna seria kamer termowizyjnych FLIR FB-O

Linc Polska
www.linc.pl

Ze względu na stale rosnące możliwości zastosowań rozwiązań termowizyjnych w branży zabezpieczeń technicznych oferta FLIR Systems została poszerzona o nową ekonomiczną linię kamer FLIR FB-O. Są one produkowane na terenie Unii Europejskiej, co bezpośrednio przekłada się na uproszczenie procedury zakupowej i skrócenie terminów dostaw. Są oferowane w korzystnej cenie, a przy tym zapewniają wysoką jakość, płynny obraz i solidność wykonania (IP66).
Zgodność z ONVIF, obsługa protokołów sieciowych, wyjście analogowe i IP (2 niezależne kanały) to kolejne atuty serii FB-O. Kamery są kompatybilne z różnymi systemami i rozwiązaniami firm trzecich, m.in. z zewnętrzną analityką wideo.
Ponadto ich współpraca z oprogramowaniem FLIR United VMS oferuje dodatkowe funkcjonalności, takie jak możliwość zdalnej konfiguracji i zarządzania alarmami, z naciskiem na prostotę, niezawodność i bezbłędne działanie. W oparciu o sygnał z kamer FLIR FB-O możliwa jest również współpraca np. z kamerami obrotowymi w celu automatycznego śledzenia danego obiektu.
Obrazowanie termowizyjne jest wykorzystywane zarówno w ochronie obwodowej, jak i zabezpieczeniu rozległych przestrzeni. Zaawansowany system umożliwiający automatyczne dopasowanie parametrów obrazu do warunków atmosferycznych, a także technologia zapewniająca ostre krawędzie i wysoki kontrast detali gwarantują wysoką jakość obrazu.

LISTEC® – system liniowej detekcji ciepła w ofercie Schrack Seconet Polska

Schrack Seconet Polska
www.schrack-seconet.pl

Firma Schrack Seconet Polska ma w ofercie system liniowej detekcji ciepła w dwóch wariantach: δ-LIST® oparty na kontrolerze SCU 800 współpracującym z kablem sensorycznym SEC 15 i wyspecjalizowanymi czujnikami zewnętrznymi ESD oraz LIST® oparty na jednostce oceniającej Listcontroller współpracującej z kablem sensorycznym SEC 20. Stosuje się je do zabezpieczenia przestrzeni trudno dostępnych bądź o niekorzystnych warunkach środowiskowych, np. ujemne temperatury, wysoka wilgotność, zapylenie. To kompleksowa oferta do obiektów przemysłowo-magazynowych.
System δ-LIST® umożliwia podłączenie dwóch kabli sensorycznych SEC15 o dł. do 250 m każdy. Jest przeznaczony do lokalnej ochrony urządzeń i zabezpieczenia mniejszych obiektów: · krótkie tunele, trasy kablowe · parkingi podziemne, magazyny itp.
System LIST® pozwala na podłączenie kabla sensorycznego o dł. do 3500 m w układzie linii lub pętli. Jest przeznaczony do zabezpieczenia rozległych obiektów: · długie tunele drogowe, kolejowe, metro · duże systemy przenośników taśmowych itp. Systemy mogą chronić obszary EX (strefy 2 i 22). Czujniki pomiarowe zintegrowane w kablu sensorycznym umożliwiają identyfikację źródła zagrożenia pożarowego nawet z 0,5 m. Wbudowane interfejsy komunikacyjne pozwalają połączyć w sieć większą liczbę kontrolerów oraz zintegrować z systemami nadrzędnymi, np. SIS-FIRE.
Zachęcamy do kontaktu z firmą i udziału w szkoleniach dla projektantów. Szczegóły na www.schrack-seconet.pl.

Przełącznik Smart PoE TP-Link T1600G-28PS

TP-Link Polska
www.tp-link.com.pl

Przełącznik T1600G-28PS to wydajne i oszczędne rozwiązanie, dzięki któremu można zasilić punkty dostępowe, kamery monitoringu, telefony IP lub inne urządzenia korzystające z technologii PoE. Został wyposażony w 24 porty PoE 10/100/1000 Mb/s (802.3at/af) mogące łącznie dostarczyć 192 W mocy oraz w 4-gigabitowe sloty SFP umożliwiające podłączenie urządzenia do sieci światłowodowej lub łączenie przełączników ze sobą.
Kompaktowy i wszechstronny T1600G-28PS jest idealnym rozwiązaniem dostarczającym zasilanie PoE w małych i średnich sieciach firmowych. Doskonale sprawdzi się np. do zintegrowania systemu CCTV z istniejącą siecią.
Najważniejsze cechy i funkcje:
- 24 porty PoE+, 802.3at/af – o maks. przesyłanej mocy do 30 W na każdy z nich,
- moc całkowita podłączonych urządzeń maks.192 W,
- funkcja routingu statycznego warstwy 2+,
- rozbudowane funkcje zabezpieczające ruch sieciowy, w tym obsługa VLAN 802.1Q,
- porty *Security* oraz *Storm control* skutecznie zabezpieczają sieć lokalną,
- możliwość zoptymalizowania transmisji głosowej i wideo dzięki funkcjom QoS (L2/L3/L4) oraz IGMP *snooping*,
- obsługa IPv6, z możliwością podwójnego stosu IPv4/IPv6,
- MLD *snooping* oraz IPv6 *neighbor discovery*.

T1600G-28PS jest urządzeniem łatwym w użytkowaniu i zarządzaniu. Udostępnia wiele przyjaznych dla użytkownika możliwości zarządzania, np. intuicyjny graficzny interfejs użytkownika (GUI) obsługiwany przez przeglądarkę internetową.

My nie idziemy drogą, my ją wytyczamy

Linc
Polska Sp. z o.o.

www.linc.pl

Pracuj z najlepszymi!

Nowoczesność i bezpieczeństwo

ŚNIADANIE EKSPERTÓW

Bezpieczeństwo w handlu

O bezpieczeństwie w **obiektach handlowych, funkcjach inteligentnych,** *loss prevention* **i zastosowaniu security w marketingu** rozmawiali uczestnicy kolejnego śniadania ekspertów a&s Polska.

Film ze spotkania na:
www.aspolska.pl/sniadanie-handel

Rozwiązania z rynku zabezpieczeń technicznych – oprócz zastosowań stricte security – stały się narzędziem marketingowym dostarczającym handlowcom dane statystyczne o klientach. Ten temat stał się przyczynkiem do ciekawej dyskusji przedstawicieli producentów zabezpieczeń technicznych z użytkownikami końcowymi z sektora *retail*. Gościliśmy osoby odpowiedzialne za bezpieczeństwo i *loss prevention* w galeriach handlowych i sieciach sklepów detalicznych.

Kolejne spotkanie odbędzie się 10 listopada. Będzie poświęcone bezpieczeństwu w obiekrach przemysłowych – więcej na s. 51.

Adam Suliga
Polska Izba Handlu

Idea spotkania jest fantastyczna. Powinniśmy jak najczęściej spotykać się w gronie osób decyzyjnych, które potrafią nie tylko podjąć wyzwania wynikające z tego, co się dzieje na obecnie na rynku i wykorzystać nowe trendy, ale też wpływać na zmiany. Chciałbym, aby każde z takich spotkań kończyło się podjęciem pewnych decyzji, które faktycznie wpłyną na poprawę bezpieczeństwa sieci retail, które reprezentuję.

Maciej Pietrzak
Dahua Technology Poland

Bardzo ciekawe spotkanie i szerokie spektrum poruszanej tematyki. Byli tu i producenci, i odbiorcy końcowi, i osoby, które zajmują się warstwą teoretyczną, czyli kwestią prawa.

Spotkanie jak najbardziej na plus! Oprócz tego, co przedstawiali pozostali eksperci reprezentujący producentów security, mogliśmy również zapoznać się z tym, czego oczekują klienci końcowi. Dzięki temu będziemy mogli lepiej pracować nad planem rozwoju produktów w przyszłości.

Radosław Suchodoła
Hikvision Poland

Michał Sidor
Schrack Seconet Polska

Świetne spotkanie. Można było usłyszeć o wielu aspektach, o których na co dzień nie rozmawiamy. Wiele ekspertów w jednym miejscu, punkt widzenia z różnych stron – to wartość tego spotkania. Omawiana tematyka systemów zabezpieczeń w galeriach handlowych i obiektach handlowych naprawdę ciekawa. Jak zwykle udane spotkanie!

Forma tego spotkania mnie zaskoczyła. Jestem bardzo zadowolona z wymiany zdań i poglądów wielu ekspertów z rynku security, począwszy od firm, które świadczą usługi ochrony, po firmy, które dostarczają rozwiązania techniczne dla galerii handlowych. Istotne jest dzielenie się wiedzą i doświadczeniem pomiędzy uczestnikami.

Jakub Sobek
Linc Polska

Taka formuła spotkań, kiedy mamy czas, żeby na spokojnie porozmawiać, nie spotykamy się przy jakiejś okazji i nie rozmawiamy o konkretnych produktach, jest bardzo dobrą okazją, żeby wymienić swoje doświadczenia. Spotykamy się tu z klientami końcowymi, którzy znają problemy „dnia codziennego" i wiedzą, czego oczekują. Podczas innych spotkań rozmawiamy o produktach, które mamy, ale nikt się nigdy nie zastanawia, jak w praktyce je wykorzystać. Tu jest to miejsce, gdzie teorię możemy zderzyć z praktyką i to jest największa wartość.

Barbara Berta
BNP Paribas Real Estate

Bardzo interesujące spotkanie, podczas którego można wymienić się wieloma ważnymi informacjami. To dla mnie bardzo potrzebne. Oczekuję, że będziemy się spotykali częściej.

Jacek Bechta
RTV Euro AGD


PRZEMYSŁ
4.0

Machine Vision + RFID
Inteligentne fabryki

Przemysł 4.0 – to w tę stronę przesuwa się produkcja przemysłowa. Tradycyjną pracę ludzi w coraz większym stopniu zastępuje automatyzacja. Fabryki wprowadzają systemy *machine vision* oraz techniki identyfikacji radiowej (RFID). Pierwsze zapewniają kontrolę wytwarzanych towarów, drugie pozwalają śledzić jednocześnie dużą liczbę produktów.

William Pao
a&s International

Machine vision można opisać jako „oczy" produkcji, przydatne w wielu procesach, np. podczas kontroli produktów lub kierowania pojazdami autonomicznymi. Eliminuje podstawowy problem związany ograniczeniami oka ludzkiego. *Załóżmy, że mam linię produkcyjną, którą kontroluje wielu operatorów* – mówi Roger Wang, menedżer w dziale wizji w firmie Solomon. *– Problem polega na tym, że każdy z nich widzi inaczej. Poza tym oczy się męczą, co stwarza ryzyko pomyłek. W tym przypadku z pomocą przychodzi algorytm* machine vision*, zaimplementowany w systemie, który zapewni jednolity standard kontroli, jest też mniej podatny na błędy i nigdy się nie męczy.*

Dla producentów, którzy chcą poprawić jakość produkcji lub ją zautomatyzować,, systemy te będą pierwszym potencjalnym wyborem – twierdzi Bruno Menard, menedżer ds. systemów wizyjnych w Teledyne DALSA. *– Opracowano je do kontroli wizualnej i inspekcji w zastosowaniach przemysłowych wymagających dużej szybkości, dużej precyzji, nieprzerwanej pracy lub powtarzalności pomiarów* – dodaje. *– Kontrola maszynowa umożliwia wykonywanie powtarzalnych czynności szybciej, dokładniej i dłużej, niż potrafią to robić ludzie. Ponadto pozwala zmniejszyć koszty pracy, poprawić wydajność produkcji i wyeliminować kosztowne błędy związane z niekompletnym lub źle wytworzonym produktem.*

Podstawowe komponenty

Typowy system *machine vision* składa się z kamer (wraz z obiektywami i przetwornikami obrazu), oświetlenia, urządzeń do przetwarzania analogowego obrazu na format cyfrowy (*frame grabber*) oraz oprogramowania. *Stosuje się dwa typy kamer przemysłowych: ze skanowaniem liniowym (line-scan) i matrycowe (area-scan). Częściej stosowane są kamery line-scan, ponieważ generują obrazy o wyższej rozdzielczości* – wyjaśnia Hingsuk Lee, menedżer ds. rozwoju biznesu w SuaLab. *– Frame grabbery przechwytują pojedyncze nieruchome klatki w postaci cyfrowej z analogowego lub cyfrowego strumienia wideo. Klatki są zwykle przechwytywane w postaci cyfrowej, aby można je było łatwo i szybko przesyłać dalej.*

W obiektach przemysłowych coraz częściej instaluje się też kamery głębi lub kamery 3D. *W przeciwieństwie do tradycyjnych kamer rejestrujących obrazy dwuwymiarowe kamera głębi dodaje do obrazu 2D dane na temat*

WYKORZYSTANIE *DEEP LEARNING*

Coraz więcej systemów obserwacji maszynowej wykorzystuje potencjał *deep learning*, zwłaszcza w obszarze kontroli. *W systemie umieszcza się obrazy dobrych i złych próbek, na ich podstawie system zaczyna wnioskować samodzielnie, rozpoznając wady i skazy bez dodatkowej pomocy* – wyjaśnia Roger Wang, menedżer działy wizyjnego w firmie Solomon.

Hongsuk Lee, menedżer ds. rozwoju biznesu w SuaLab, jako przykład podaje technologię zastosowaną w branży tekstylnej. *Jesteśmy pierwszą firmą na świecie, która skomercjalizowała bezobsługowy system kontroli jakości produktów tekstylnych z wykorzystaniem deep learning. Zastosowanie widzenia maszynowego w branży tekstylnej było trudne z dwóch powodów. Po pierwsze tło na produkcie tekstylnym jest złożone, więc trudno wykryć defekt, opierając się na prostym algorytmie. Po drugie cykl życia produktu jest krótki, więc nie ma dość czasu na optymalizację algorytmu. Aby rozwiązać problem, w systemie machine vision zastosowaliśmy dedykowany algorytm, który umożliwia odnalezienie niewykrytych defektów i potrafi szybko reagować na zmianę produktu.*

głębi, zapewniając lepszą czytelność i dokładność – mówi Calvin Lee, dyrektor operacyjny w LIPS Corporation.

Oprócz sprzętu, ważną rolę odgrywa oprogramowanie. *Dobry system wizyjny to taki, który zapewnia wysoką wykrywalność defektów. Do tego niezbędne są zaawansowane urządzenia gwarantujące dobrej jakości obrazy, które z kolei powinny być analizowane przez wysoko wydajne oprogramowanie* – podkreśla H. Lee z SuaLab. – *Bez względu na to, jak wysokiej jakości byłby sprzęt, system wizyjny nie będzie dobry, jeśli wydajność analizy obrazu jest niska.*

Zastosowania

Widzenie maszynowe może znaleźć zastosowanie w różnych operacjach produkcyjnych, włączając w to kontrolę, lokalizację i sterowanie robotami czy pojazdami autonomicznymi. Najważniejszym zastosowaniem jest wykrycie trudno widocznych gołym okiem defektów, np. w fabrykach odzieży wskazanie pękniętych szwów, przebarwień czy innych wad. *Machine vision ma największy wpływ na „inteligentne fabryki" w obszarze kontroli produkowanych artykułów* – wyjaśnia H. Lee. – *W zależności od branży i produktów dzięki machine vision niektóre firmy już stosują pełną automatyzację procesu kontroli. Inne wykorzystały tę technologię do redukcji liczby pracowników zaangażowanych w ten proces.*

Kolejną operacją, która może być oparta na *machine vision*, jest lokalizacja produktów. *Stosując metodę dopasowania do wzorca, możemy określić położenie, orientację, czyli ułożenie, a także rozmiar elementu lub obiektu. Po „nauczeniu" tzw. złotych wzorców algorytmy są w stanie przesuwać, obracać i skalować, czyli zwiększać lub zmniejszać obraz produktów* – mówi B. Menard. – *Po ustawieniu granicznych parametrów akceptowalności aplikacja może odszukać obiekt i dokonać porównania, aby podjąć decyzję o akceptacji bądź odrzuceniu produktu. Machine vision* zapewnia niezbędne dane wizyjne coraz większej liczbie automatycznych wysięgników. *Gdy np. ramię robota przenosi coś z punktu A do B, kamera głębi dostarcza potrzebny obraz, wskazując robotowi, jak ma obiekt chwycić i gdzie odłożyć* – wyjaśnia C. Lee z LIPS. – *Operator nie musi też ustalać toru jazdy pojazdów autonomicznych. Kamera głębi pomoże określić najlepszą drogę do celu i ominąć ewentualne przeszkody.*

Branże, które zyskają

Stosując technikę *machine vision* korzyści może odnieść wiele branż – od tradycyjnych po elektroniczne. *Machine vision to pierwszy potencjalny wybór dla każdej fabryki, chcącej poprawić jakość produktów lub zautomatyzować produkcję* – podkreśla B. Menard. – *Liczne branże, od półprzewodnikowej, elektronicznej, poprzez motoryzacyjną, spożywczą i opakowań, aż po ogólnoprodukcyjną, mogą skorzystać na wdrożeniu systemu widzenia przemysłowego* – kontynuuje. – *Mogą one zwiększyć wydajność produkcji, wpływając jednocześnie na podniesienie jakości.*

Od części składowych po gotowe produkty – ostatnim etapem każdego procesu produkcyjnego jest kontrola. W zasadzie każda branża może skorzystać z machine vision – uważa H. Lee. – *Ponieważ trudno byłoby ustanowić proces zapisywania obrazu dla każdego rodzaju produktu, technologia machine vision znajduje zastosowanie w specyficznych obszarach, które łatwo zobrazować, takich jak przemysł elektroniczny (m.in. półprzewodniki i wyświetlacze). Jeśli tego typu trudności uda się pokonać za pomocą deep learning, będzie można zastosować widzenie maszynowe w dowolnej branży produkcyjnej* – prognozuje Lee.

Wybór właściwego systemu

Użytkownicy końcowi muszą przestrzegać określonych zasad i wymagań. Również system kontroli maszynowej powinien te wymagania spełniać. Bruno Menard wskazał, że szczególną uwagę należy zwrócić na kilka aspektów:

- Należy określić zadania, jakie ma wykonywać system wizyjny, ponieważ różne cele wymagają różnych parametrów wizji. *Machine vision* przeznaczony do kontrolowania jednego zadania może nie być odpowiedni do innego.
- Muszą zostać zdefiniowane kluczowe kryteria wizualne, które zagwarantują odpowiednią wydajność kamery i obiektywu, biorąc pod uwagę takie czynniki, jak najmniejszy rozmiar obiektu lub defektu do wykrycia, wymagana dokładność pomiaru, rozmiar obrazu, liczba klatek na sekundę i szybkość przetwarzania, a także potrzeba widzenia kolorów. Wszystkie te elementy mają wpływ na wybór kamery i obiektywu.
- Należy rozważyć czynniki środowiskowe – np. niektóre kamery są przystosowane do oglądu scen statycznych, inne sprawdzą się w obserwacji liniowego ruchu obiektów. Z kolei czynniki temperatury, wilgotności i wibracje mogą determinować zastosowanie specjalnej technologii lub specjalnych technik montażu.

Należy też uwzględnić kwestie ekonomiczne i budżet, jakim dysponują użytkownicy, system widzenia maszynowego jest bowiem rozwiązaniem złożonym,

Ogromną liczbę towarów (np. odzież w fabryce tekstyliów) można zeskanować i jednocześnie wygenerować dane, które pozwolą na lepszą kontrolę procesu produkcji.

ściśle dostosowanym do konkretnych wymagań. *Trzeba dokonać dokładnej analizy, czy inwestycja się zwróci* – zaleca R. Wang. – *W niektórych krajach koszty pracy nie są wysokie, więc trzeba się zastanowić, czy warto inwestować w system machine vision. Może się zdarzyć, że lepszym rozwiązaniem będzie po prostu zatrudnienie kolejnych pracowników.*

Inteligentne fabryki dzięki RFID

Systemy radiowej identyfikacji sprawiają, że fabryki stają się *smart* – ale na nieco innej zasadzie. W przeciwieństwie do *machine vision*, które stanowi „oko produkcji", technologia RFID pozwala na natychmiastową identyfikację znacznej liczby produktów, ich części lub komponentów bez potrzeby zachowania ich w polu widzenia. To metoda bardziej wydajna od tradycyjnych technologii, np. skanowania kodów kreskowych.

Skanowanie kodów kreskowych jeden po drugim stwarza kilka problemów. Po pierwsze jest zbyt wolne – wyjaśnia Brian Ma, główny menedżer w GIGA-TMS. – *Po drugie łatwo o błędy, ponieważ operatorzy się mylą lub nie wykonują pracy zgodnie z instrukcją. Z kolei technika identyfikacji radiowej (RFID) przekonuje do siebie możliwością jednoczesnej i natychmiastowej identyfikacji dużej liczby otagowanych artykułów, ich części lub komponentów, co jest rozwiązaniem szybszym i bardziej wydajnym. Przemysłowe rozwiązania RFID wprowadziły już tzw. „tunel RFID", przez który przesuwają się otagowane przedmioty. Wszystkie artykuły są skanowane jednocześnie.*

Angeline Fraud, szefowa marketingu w INVENGO, zgadza się z uwagami Briana Ma. *Skojarzone z artykułami aktualne dane można odczytywać i modyfikować automatycznie w punktach przetwarzania, czyli stacjach RFID, co zmniejsza czynnik błędu ludzkiego, a także zwiększa tempo produkcji i kontroli jakości. Problemy są identyfikowane na poziomie jednostkowym* – tłumaczy. – *Wpływa to też pozytywnie na dokładność dostaw. Wszystko to przyczynia się do poprawy wydajności operacyjnej.*

Rodzaje RFID

RFID można podzielić na trzy kategorie skategoryzować w zależności od zakresu częstotliwości radiowych: LF pracuje w zakresie 120–150 kHz, HF – 13,56 MHz, UHF – 433 MHz.

Dominującą technologią śledzenia i identyfikacji komponentów w fabrykach nadal pozostaje kod kreskowy, ale coraz więcej użytkowników skłania się w stronę techniki UHF RFID głównie z powodu jej zalet. *UHF RFID może wykonywać odczyty partii produkcyjnych. Mogę zeskanować ponad sto elementów w trzy sekundy, to naprawdę bardzo szybko* – wyjaśnia B. Ma. – *Mogę też dokonać odczytu ze znacznie większej odległości. UHF RFID stosuje tę samą technologię co eTag, tyle że ja używam jej w przemyśle tekstylnym, a nie w bramkach na autostradzie.*

Angelina Fraud uważa, że wybór odpowiedniej częstotliwości RFID zależy od rodzaju produkcji i celów użytkownika końcowego. *Jako dostawca systemów identyfikacji radiowej zapewniamy ekspercką analizę w fabryce oraz badanie procesów przebiegających wokół otagowanego radiowo produktu* – wyjaśnia. – *Dzięki temu mamy bazę, by doradzić użytkownikom, jakiej częstotliwości użyć w zależności od różnych czynników. Najpierw musimy ustalić, jaki produkt ma zostać otagowany RFID, czy zawiera elementy metalowe albo płyny. Następnie środowisko produktu: wilgotność, montaż w powietrzu, wewnątrz, na zewnątrz, pod ziemią. Czy stosowane oprzyrządowanie jest wykonane z metalu, a także jaka jest wymagana odległość odczytu oraz liczba elementów odczytywanych jednocześnie.*

Na co uważać

Urządzenia RFID – czy to czytniki, czy znaczniki (tagi) – muszą w środowisku przemysłowym spełniać pewne wymagania. *Konieczne, by były wytrzymałe i odporne na trudne warunki otoczenia, takie jak wilgoć, zapylenie czy niewłaściwe użytkowanie. Urządzenie RFID wymaga ponadto odpowiedniego dostrojenia i nastawienia, aby mogło pracować w środowisku metalowych maszyn czy neonowego oświetlenia, bo te czynniki w istotny sposób wpływają na sprawność odczytu RFID* – wyjaśnia A. Fraud. – *Na przykład znaczniki RFID umieszczone na odzieży z Inu muszą być odporne na proces jego konserwacji, który obejmuje mycie, suszenie na gorąco oraz operacje namaczania i wyciskania przy ciśnieniu 60 barów.*

Chociaż identyfikację radiową można wykorzystać w wielu różnych branżach, nadal należy uwzględniać potencjalne problemy. *Istnieją przeszkody i ograniczenia mające wpływ na decyzję o wprowadzeniu RFID. Wynikają one z natury technicznej, np. nieprzyjazne środowisko skutkujące niską jakością odczytu, a także z kwestii finansowej, w tym z kosztów wdrożenia, od znaczników znacznie tańsze są bowiem kody kreskowe. Ważne są również kwestie prywatności i bezpieczeństwa* – mówi A. Fraud.

Mimo to eksperci są zgodni, że perspektywy stosowania RFID w fabrykach są obiecujące, zwłaszcza ze względu na oferowaną możliwość śledzenia zasobów i szybkiego generowania danych. *Przykładowo 150 artykułów tekstylnych ma zostać przesłanych do dalszego etapu produkcji, okazuje się jednak, że jest ich tylko 140. Mogę więc sprawdzić w systemie lokalizację tych 10 brakujących sztuk i dowiedzieć się, jaki jest ich los*– opowiada B. Ma. – *Zarządzający produkcją powinni mieć możliwość szczegółowej analizy, by móc na bieżąco kontrolować proces produkcji i raportować do centrali. Dzięki RFID są w stanie dokonywać analizy i podejmować decyzje na podstawie aktualnych i rzeczywistych danych.*

Obserwujemy coraz większe zainteresowanie rozwiązaniami do identyfikacji radiowej, nie tylko w fabrykach, ale także na całej drodze produktu aż do klientów. Głównie za sprawą istotnych korzyści, jakie technologia RFID przyniosła fabrykom w ostatnich latach, a także dzięki dojrzałości i optymalizacji rozwiązań all-in-one – ocenia A. Fraud. *Na korzyściach płynących z RFID zyskuje nie tylko użytkownik końcowy, ale także całe otoczenie biznesowe. Identyfikacja radiowa zmienia reguły gry, a gracze na tym rynku liczą na innowacyjność i możliwość wyróżnienia się na tle konkurencji.*

Obie techniki: *machine vision* oraz RFID sprawiają, że fabryki stają się „inteligentne" i zmniejszają zależność od pracy ludzi. W kontekście trendu Przemysłu 4.0 mają dużą szansę na rozpowszechnienie i coraz częstsze stosowanie w fabrykach na całym świecie. Na rynku jest już wiele możliwych rozwiązań, więc użytkownicy mogą wybrać te, które najlepiej odpowiadają ich branży i celom biznesowym. Pozwoli to czerpać korzyści, jakie zapewniają *machine vision* i RFID.

Bezpieczeństwo przemysłowe wobec współczesnych zagrożeń

Żyjemy i prowadzimy działalność gospodarczą w kraju mającym specyficzne doświadczenia usprawiedliwiające niestety wciąż obecne przyzwolenie dla czynów nieetycznych, a nawet karalnych. Przez wiele lat w Polsce nie kradło się, ale „załatwiało", „organizowało" albo po prostu „przynosiło".

Jacek Grzechowiak

Załatwiało się" wszystko, materiał na ogrodzenie, papier do napisania pisma czy wreszcie herbatę i cukier, które były w firmie. Ta zaś była państwowa, a więc – w przekonaniu wielu – niczyja. To z kolei usprawiedliwiało „załatwianie", bo przecież mienie „załatwione" było niczyje. Minęło wiele lat od tzw. transformacji ustrojowej i wydawałoby się, że żyjemy w innej rzeczywistości, ale teza ta nie wszędzie jest zgodna z prawdą. Przyzwolenie dla „załatwiania" wciąż funkcjonuje, nie w takim roz-

miarze, jak niegdyś, ale jednak jest wciąż obecne w naszej rzeczywistości. Mało tego, jest istotnym czynnikiem wpływającym na stan bezpieczeństwa chronionych zasobów. Jeśli do tego dodamy niekorzystne doświadczenia historyczne z zaborcami i okupantem, okaże się, że mamy do czynienia z wyjątkowo trudnym do przezwyciężenia psychologicznym mechanizmem usprawiedliwiania czynów zabronionych.

Zmiana modelu funkcjonowania przedsiębiorstw

Współczesne przedsiębiorstwa w obliczu dużej i niekiedy agresywnej konkurencji są zmuszone do poszukiwania rozwiązań zapewniających im przewagę konkurencyjną. Głównym polem tej walki jest cena, jako ten wskaźnik, który klienci identyfikują w pierwszej kolejności. Jednym z narzędzi optymalizacji kosztowej jest efektywna gospodarka komponentami produkcyjnymi. Strategia *just in time* jest dziś standardem powszechnie stosowanym. Jej wdrożenie wymusiło także zmianę podejścia do zarządzania bezpieczeństwem, zapewnienie nienaruszalności wartości chronionego mienia nie jest bowiem już jedynym zadaniem ochrony. Dziś, oprócz wartości mienia, niezbędne jest zarządzanie bezpieczeństwem kompletności ładunku, gdyż w pewnych sytuacjach brakująca sztuka komponentu produkcyjnego może spowodować problem z ciągłością procesu produkcyjnego. Ten sam problem dotyczy sieci handlowych, zaopatrujących je firm logistycznych oraz rzeszy małych i średnich firm będących dostawcami dużych producentów.

Rozpowszechnienie strategii *just in time* spowodowało konieczność wprowadzenia rozwiązań zapewniających kompletność dostawy oraz bezpieczeństwo całego transportu. Stosowane rozwiązania bazują na aktywnym monitoringu zarówno transportów, jak i wybranych komponentów, zapewniającym nie tylko wzbudzenie alarmu w przypadku wystąpienia incydentu, a także – a nawet przede wszystkim – alarmowanie w razie pojawienia się symptomów zagrożeń, takich jak opuszczenie trasy przejazdu czy nieplanowany postój, i podejmowanie odpowiednich działań, by upewnić się, że sytuacja nie zmierza w kierunku incydentu lub potwierdzenia, że wystąpiły symptomy zdarzeń (pojedyncze lub określone sekwencje), które występują zawsze lub bardzo często przed incydentem, więc sytuacja wymaga uruchomienia procedur i zasobów przeznaczonych na reagowanie bezpośrednio przed wystąpieniem incydentów i w ich trakcie.

Drugim wyróżnikiem współczesnego profilu organizacji biznesowych jest duże nasycenie infrastrukturą informatyczną, sterującą procesem produkcji, procesem obsługi produkcji i procesami logistycznymi (szczególnie zamówienia wyrobów i komponentów, organizacja transportu). Jednocześnie współcześni producenci realizują swój proces produkcyjny w wielu obiektach, z reguły zlokalizowanych w różnych miejscach. Dodatkowo infrastruktura teleinformatyczna zawsze przebiega przez miejsca chronione, ale także – i to w dużej mierze – przez miejsca niechronione, w wyniku czego jest w sposób ponadprzeciętny podatna na zagrożenia. To powoduje, że duża część zasobów jest zlokalizowana poza obiektami i w tych miejscach także występuje zagrożenie dla biznesu.

Współczesne zagrożenia dla biznesu

Rozważając stan bezpieczeństwa obiektu, należy postrzegać go przez pryzmat wielopłaszczyznowego oddziaływania na organizacje biznesowe. Podstawową (i jednocześnie najbardziej rozpowszechnioną) formą oddziaływania przestępczego pozostaje kradzież, jej formy jednak uległy dużym przeobrażeniom, związanym zarówno z edukacją osób dokonujących przestępstw, jak i ewolucją środków bezpieczeństwa. Przykładem takiego rozwoju jest nagłośniony medialnie przypadek wywiezienia w styczniu 2008 r. z fabryk Sharp i Orion w Łysomicach znacznej liczby telewizorów o szacunkowej wartości 1,5 mln zł[1] przez zorganizowaną grupę przestępczą. Mając powyższe na względzie, należy pamiętać, że bezpieczeństwo biznesowe to bezpieczeństwo obiektu, bezpieczeństwo produktów, polegające na ochronie przed kradzieżami (wewnętrznymi i zewnętrznymi), piractwem lub działaniami mającymi na celu narażenie wizerunku na szwank, a także bezpieczeństwo własności intelektualnej.

> Podstawową formą działania przestępczego pozostaje kradzież, jej formy jednak uległy dużym przeobrażeniom, związanym zarówno z edukacją osób dokonujących przestępstw, jak i ewolucją środków bezpieczeństwa.

Niezmiernie ważny jest fakt, iż współczesne organizacje biznesowe są także narażone na zagrożenia, wydawałoby się „z minionej epoki", takie jak sabotaż. Przykładem może być incydent w firmie EADS: *W jednym z montowanych w Tuluzie samolotów Airbus 380 znaleziono trzy przecięte kable. Dyrekcja fabryki podejrzewa sabotaż. Śledztwo wszczęła żandarmeria. Nie poinformowano, w jakiej części samolotu znajdowały się przecięte kable ani jaka była ich funkcja*[2]. Przypadki sabotażu zdarzają się najczęściej w podmiotach, w których występują równolegle lub występowały wcześniej napięcia w relacjach pracownicy–pracodawcy.

Również szpiegostwo gospodarcze jest wciąż obecne. Przykładem tego zagrożenia jest ujawniona w lutym 2014 r. kradzież informacji poufnych z jednego ze znanych zakładów przetwórstwa mięsnego w województwie wielkopolskim. Przeprowadzone postępowanie wyjaśniające ujawniło, iż osoba zatrudniona na stanowisku analityka przez ponad pół roku przekazywała konkurencyjnemu przedsiębiorstwu informacje dotyczące produkcji, sprzedaży oraz kontrahentów swojego pracodawcy[3].

Trendy w bezpieczeństwie obiektów

Obserwowane w ostatnim czasie nasilenie kradzieży pracowniczych skłania przedsiębiorców do ponoszenia większych nakładów na różne systemy zabezpieczeń. W przypadku firm pracujących w systemie dwuzmianowym lub funkcjonujących z niewielkimi przerwami, a takimi przedsiębiorstwami z reguły są zakłady produkcyjne, wykorzystuje się przede wszystkim systemy kontroli dostępu, systemy dozoru telewizyjnego oraz odpowiednie uregulowanie proceduralne dotyczące przede wszystkim zasad wnoszenia i wynoszenia mienia. Osiągnięcie satysfakcjonującego poziomu bezpieczeństwa jest jednak możliwe tylko w przypadku stworzenia spójnego systemu, łączącego:

- opracowaną i ogłoszoną politykę bezpieczeństwa,

- ogłoszoną i konsekwentnie realizowaną politykę „zero tolerancji”,
- procedury wewnętrzne zakładu uwzględniające aspekty bezpieczeństwa,
- współpracę pomiędzy kierownictwem zakładu a służbami ochrony,
- nieustanne analizowanie stanu bezpieczeństwa i korygowanie przyjętych rozwiązań,
- wykorzystanie skuteczności systemów zabezpieczeń technicznych.

Dlatego konieczne jest aktywne zarządzanie bezpieczeństwem poprzez tworzenie systemów wykorzystujących synergię ściśle związanych z celami firmy elementów mechanicznych, technicznych i organizacyjnych. Stosowanie systemów zabezpieczeń technicznych jest już standardem. Bardzo rzadko można spotkać obiekty chronione przez zespoły ochrony fizycznej bez wsparcia systemów zabezpieczeń technicznych. Trend ten z pewnością będzie miał charakter wznoszący jeszcze przez wiele lat, zarówno ze względu na zwiększającą się dostępność technologiczną i cenową systemów zabezpieczeń technicznych, jak i zwiększone koszty pracy pracowników ochrony. Widoczna zmniejszająca się liczba pracowników ochrony sprzyja temu trendowi. W obliczu tych zmian krytyczne wydają się trzy kwestie:

- właściwe rozpoznanie chronionych zasobów, ich podatności (przede wszystkim na kradzież) i znaczenia dla organizacji (szczególnie w zakresie ciągłości biznesu),
- właściwa ocena możliwości systemów zabezpieczeń technicznych, w tym typowo w zakresie działań ochronnych i wsparcia działów non-security,
- właściwy dobór personelu, jego szkolenie, zadaniowanie oraz rozliczanie pracy.

Rozpoznanie chronionych zasobów jest jednym z trudniejszych przedsięwzięć, wymaga bowiem pełnego i efektywnego zaangażowania kadry *non-security*, gdyż to ona posiada najlepszą wiedzę w zakresie swojego mienia. Bywają sytuacje, w których mienie może mieć dwie lub nawet więcej odmian, co może mieć wpływ na jego podatność na kradzież. Przykładem mogą być włókniny – mając bardzo podobny skład, znajdują zastosowanie zarówno w krawiectwie, rolnictwie, ogrodnictwie czy budownictwie (zarówno infrastrukturalnym, jak i wykańczaniu wnętrz), zależnie od grubości czy jakości. Tym samym produkt ma zmienną podatność w zależności od rodzaju produkcji, ale i komponent produkcyjny, z pozoru nieatrakcyjny dla potencjalnych złodziei, będzie podatny na kradzież (faktyczną i sfingowaną). Innym przykładem mienia z pozoru nieatrakcyjnego są żeliwne czy stalowe kule stosowane w różnego rodzaju młynach. Zużywają się w sposób naturalny, poprzez ścieranie, a tym samym ich rozliczalność jest problematyczna. Ponieważ nie są drogie, firmy często nie przywiązują wagi do sprawdzania stanów magazynowych oraz ochrony miejsc ich przechowywania, do czasu, aż kule znikną, a ich brak wstrzyma produkcję.

Stosowanie systemów zabezpieczeń technicznych jest już standardem. Bardzo rzadko można spotkać obiekty chronione przez zespoły ochrony fizycznej bez wsparcia systemów zabezpieczeń technicznych.

Właściwy dobór systemów zabezpieczeń technicznych jest więc sprawą mającą szczególne znaczenie. Obecnie na rynku jest bardzo duży wybór systemów, a ich sprzedawcy zapewniają, że mają one niemal nieograniczone możliwości. Ale czy ich parametry są adekwatne do naszych potrzeb? Odpowiedź na takie pytanie wymaga wykonania zawsze szczegółowej analizy mienia, jego rodzaju, elementów identyfikujących je (kształt, kolor, numer itp.), miejsca jego zlokalizowania (zewnętrzne, wewnętrzne, chronione przez inne systemy), rodzajów ryzyka zewnętrznego (włamanie, kradzież) i wewnętrznego (włamanie, kradzież, sprzeniewierzenie), a także własnych zasobów (np. liczba osób, ich profil, wykształcenie, rotacja personelu i wynikające z niej doświadczenie w obiekcie) oraz ich potencjału (zdolności przyswajania nowej wiedzy, zaangażowanie w pracę, umiejętności kojarzenia faktów). Zanim kupimy urządzenia, musimy się upewnić, że są nam potrzebne, samo porównanie ich parametrów czy zasięgu działania jest niewystarczające. Trzeba przeanalizować zmianę pór doby, pór roku, „życie” obiektu.

Kolejnym elementem, zwłaszcza w zakładach przemysłowych o dużym zapyleniu, jest konserwacja urządzeń, szczególnie kamer, których rozdzielczość nigdy nie zwycięży z zalegającym na obiektywach czy obudowach kurzem. Kurz to jeden z największych wrogów, a walka z nim jest równie ważna jak walka ze złodziejami. Dużym wyzwaniem jest współdziałanie systemów zabezpieczeń z pozostałą infrastrukturą obiektu, szczególnie oświetleniem. Oświetlenie może być w różnym stopniu sprzymierzeńcem i wrogiem CCTV, i to nie tylko w przypadku niewystarczającego oświetlenia. Również zbyt silne może powodować problemy z obserwacją terenu za pomocą kamer CCTV. Jednym słowem, inwestycje w infrastrukturę *non-security* wymagają od security managera pełnego zaangażowania już na etapie ich przygotowania, inwestycje w systemy security zaś wymagają od security managera skutecznego zaangażowania kadry non-security.

Jednym z najpoważniejszych obecnie problemów w zarządzaniu bezpieczeństwem jest odpowiednie skonfigurowanie struktury ochrony, szczególnie wobec zmian w zakresie wynagrodzeń pracowników ochrony. Sprawy personalne mają przede wszystkim wymiar socjalny, dlatego są one z reguły skomplikowane, wymagają rzetelnego przygotowania i rozłożenia wprowadzania ich zmian w dłuższym okresie, a także odpowiedniej komunikacji z pracownikami, aby nie byli oni zaskakiwani zmianami, a także w celu wyeliminowania niepewności co do ich przyszłości. Właściwy dobór osób na poszczególne stanowiska to jeden z elementów kluczowych. W obiektach przemysłowych wyróżnia się trzy zasadnicze grupy stanowisk ochronnych:

- zarządzanie zespołem – są to szefowie ochrony/obiektu i dowódcy zmian, czyli osoby, które delegują zadania, rozliczają z ich wykonania oraz kierują całokształtem prac zespołu ochronnego; oprócz spełnienia wymagań prawnych, wynikających z regulacji ustawy o ochronie osób i mienia, powinny mieć także pozytywne cechy przywódcze, zapewniające precyzję stawianych zadań, mobilizację pracowników do właściwego wykonywania obowiązków oraz rozwiązywania sytuacji trudnych wewnątrz zespołu ochronnego i w relacjach z pracownikami, podwykonawcami oraz – co naturalne – intruzami;
- operatorzy systemów zabezpieczeń (głównie CCTV) – ci pracownicy powinni

mieć wysokie umiejętności posługiwania się urządzeniami technicznymi; operatorzy CCTV powinni mieć także bardzo dobrą znajomość topografii obiektu, co pozwoli im nie tylko właściwie obsługiwać systemy, ale także odpowiednio precyzyjnie instruować pracowników liniowych, zwłaszcza w przypadku incydentu;
- pracownicy liniowi – to najbardziej niedoceniana grupa pracowników ochrony. Niesłusznie. To oni realizują zadania wymagające największej odwagi, zdolności przewidywania zdarzeń i umiejętności współdziałania z osobami z security oraz spośród kardy non-security. Współczesne firmy ochrony od pewnego czasu wdrażają rozwiązania polegające na tworzeniu profili stanowiskowych i wykorzystaniu tego narzędzia do optymalnego obsadzania rekrutowanych osób na stanowiskach pracy. Dziś to element jeszcze dość nowy, ale z pewnością będzie się rozwijał, tkwią w nim bowiem olbrzymie możliwości dla wszystkich: pracowników, firm ochrony, odbiorców usług.

Dostawca faktyczny czy wirtualny?

Jednym z ważniejszych elementów bezpieczeństwa przemysłowego jest właściwy dobór dostawcy usług oraz właściwe skonstruowanie umowy. Ze względu na regulacje prawne każda firma ochrony jest zobowiązana do posiadania koncesji wydawanej przez Ministerstwo Spraw Wewnętrznych i Administracji. Obligatoryjne jest również posiadanie polisy ubezpieczenia OC. Mimo to poprzeczka wejścia na rynek jest zawieszona bardzo nisko, co powoduje, że działa tak dużo firm ochrony. Samo sprawdzenie koncesji i polisy jest zdecydowanie niewystarczające. Równie istotne jest upewnienie się, że wobec potencjalnego dostawcy nie toczy się postępowanie o cofnięcie koncesji.

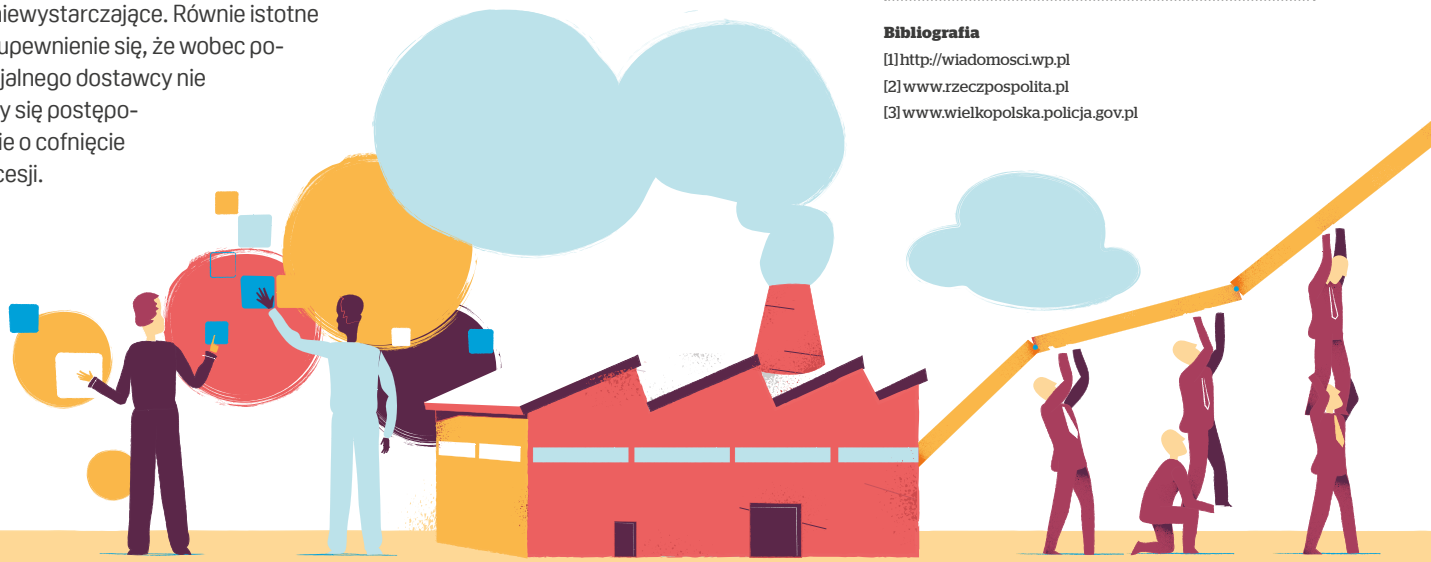
Drugim ważnym elementem, powszechnie niedocenianym, jest status firmy ochrony. Zgodnie z polskim prawem firmy ochrony dzielą się na posiadające status Specjalistycznej Uzbrojonej Formacji Ochronnej (SUFO) oraz nieposiadające takiego statusu. Jest to ważne niezależnie od tego, czy obiekt podlega obowiązkowej ochronie, czy też nie, firmy mające status SUFO podlegają bowiem regularnym kontrolom prowadzonym przez Wydziały Postępowań Administracyjnych komend wojewódzkich policji. Nawet jeśli kontrole te nie są prowadzone w obiektach niepodlegających obowiązkowej ochronie, to sam fakt regularnego sprawowania nadzoru takiej firmy powoduje, że przestrzeganie procedur jest tam na wyższym poziomie niż w firmach niemających statusu SUFO, które podlegają kontrolom praktycznie tylko w przypadku wystąpienia incydentu. Ta sprawa ma bezpośredni wpływ na jakość świadczonych usług, celowe jest więc świadome zarządzanie tym aspektem bezpieczeństwa.
Obserwowane przeze mnie w ciągu ostatnich kilkunastu lat procesy przetargowe wskazują, iż coraz więcej firm przykłada dużą wagę do odpowiednich regulacji umownych, mając na względzie także zdolność dostawcy usługi do poniesienia ryzyka. Zapisanie w umowie nielimitowanej lub pełnej odpowiedzialności nie rozwiązuje problemu. Niezbędne jest podejście systemowe, polegające na zdefiniowaniu zasobów przekazywanych pod ochronę, określeniu ich wartości oraz zweryfikowaniu zdolności finansowej dostawcy usługi do poniesienia tego ryzyka i utrzymania tej zdolności przez cały czas trwania umowy.

Drugim ważnym ryzykiem jest zdolność dostawcy usługi do wykonania tejże. Obecna sytuacja na polskim rynku ochrony, wynikająca z niespotykanej gdzie indziej bardzo dużej liczby firm ochrony, powoduje, że dostajemy oferty od firm, które nie mają jeszcze żadnego kontraktu, ale już określają się mianem lidera rynku. Takie są realia i wymagają one zarówno od security managerów, jak i działów zakupów wnikliwego przeanalizowania potencjału dostawcy. Potencjału nie deklaratywnego, ale faktycznego. Listy referencyjne i wizyty referencyjne są już standardem w rozwiniętych organizacjach, ale głębsze przeanalizowanie statystyk rotacji personelu, programów szkoleń, struktury R&D jest także pożądane.
Ochrona obiektów przemysłowych stanowi więc kompleks działań zarówno formalnoprawnych, organizacyjnych, technicznych, jak i socjologicznych. Ten aspekt do niedawna nie występował w branży ochrony, a dziś jest już obecny. Obiekty przemysłowe zmieniają profil działania, nawet gdy nie zachodzi zmiana profilu produkcyjnego. Jest to stan już utrwalony, który powinniśmy uznać za standard, również w przyszłości. To nam, osobom zarządzającym bezpieczeństwem, przynosi nowe wyzwania, ale i nowe możliwości.

BIO

Jacek Grzechowiak
Menedżer ryzyka i bezpieczeństwa. Przez ostatnich 13 lat związany z grupą Securitas, obecnie w grupie Celsa.
Absolwent Wojskowej Akademii Technicznej oraz studiów podyplomowych w SGH i Akademii Leona Koźmińskiego. Wykładowca gościnny na uczelniach wyższych.

Bibliografia
[1] http://wiadomosci.wp.pl
[2] www.rzeczpospolita.pl
[3] www.wielkopolska.policja.gov.pl



Telewizja dozorowa w ochronie obwodowej

Ochrona obwodowa stanowi zwykle pierwszą linię zabezpieczenia zwłaszcza takich obiektów, jak lotniska, rafinerie czy bazy wojskowe. Wykrywanie prób włamania i odpowiednie reagowanie to dla operatorów zadanie priorytetowe. **Systemy telewizji dozorowej, które stają się dziś narzędziem coraz bardziej zaawansowanym, są stosowane zarówno do detekcji intruza, jak i w celach weryfikacji.**

William Pao
a&s International

Obraz wyświetlany na ekranie monitora pokazuje operatorowi przyczynę alarmu. *Zaawansowane technologie dozorowe ograniczają liczbę fałszywych alarmów w porównaniu do konwencjonalnych czujek ochrony zewnętrznej, które mogą zostać wzbudzone przez różne czynniki, m.in. zjawiska atmosferyczne lub zwierzęta* – wyjaśnia Mike Prysock, odpowiedzialny za sektor lotnisk i portów morskich w Pelco by Schneider Electric.

Wzrok jest podstawowym zmysłem człowieka wykorzystywanym w krytycznych sytuacjach. Nawet gdy inna czujka sygnalizuje zdarzenie, człowiek i tak będzie chciał zweryfikować sytuację wizualnie, by upewnić się, że informacja jest prawdziwa – dodaje Eric Olson, wiceprezes ds. marketingu w PureTech Systems.

Najważniejszym elementem wizyjnej detekcji w ochronie obwodowej jest kamera. Najczęściej stosuje się kamery termowizyjne, które są odporne na problemy kamer światła widzialnego. *Kamery termowizyjne są bardzo dokładne. Korzystanie w funkcji analitycznych obrazów światła widzialnego może prowadzić do licznych zwodniczych alarmów wynikających z rozproszenia światła i innych zjawisk, np. blasku reflektorów nocą czy ich odbić w deszczu lub kałużach. Termowizja jest na te problemy niewrażliwa. Jest niemal doskonałym detektorem osób* – podkreśla John Romanowich, prezes SightLogix.

W wielu zastosowaniach kamery światła widzialnego współpracują z termowizyjnymi. *Kamera termowizyjna służy do detekcji intruza, a obraz z tradycyjnej kamery stanowi uzupełnienie, dzięki czemu użytkownik*

może uzyskać więcej danych na temat obserwowanego obiektu – tłumaczy Romanowich. Zazwyczaj wykrycie obiektu przez kamerę termowizyjną uruchamia kamerę PTZ, która koncentruje się na obiekcie. *Połączenie detekcji termowizyjnej z obrotową kamerą PTZ ma na celu precyzyjne śledzenie zdarzenia i zebranie danych wizyjnych* – dodaje Andrea Sorri, dyrektor ds. rozwoju biznesu w sektorze Infrastruktury Krytycznej w Axis Communications.

Bardziej inteligentne niż kiedykolwiek

Obrazy przekazywane z kamer są następnie poddawane analizie treści wizyjnej, której efektem może być wszczęcie alarmu po spełnieniu określonych uprzednio warunków. Dzisiejsze systemy analityczne są coraz bardziej inteligentne. Potrafią znacznie więcej niż tylko zainicjować alarm, gdy intruz wejdzie w określony obszar. Są w stanie uzależnić alarm od rodzaju wykrytego obiektu (człowiek, zwierzę, samochód) lub działania podejmowanego przez obiekt, np. podejrzane zachowanie, nieautoryzowane wejście z osobą uprawnioną czy upuszczenie przedmiotu.

Inne kierunki rozwoju obejmują możliwość wykonywania analizy obrazu na platformach będących w ruchu: na pojazdach, dronach czy łodziach, a także połączenia jej z detekcją z innych urządzeń ochrony obwodowej w celu poprawy niezawodności detekcji: radarami, systemem GPS, czujkami napłotowymi, detektorami wystrzału z broni palnej, urządzeniami kontroli dostępu lub działającymi w środowisku Internetu Rzeczy (IoT) – wylicza E. Olson. – *Dostępność oprogramowania* open source *sieci neuronowych ma wpływ na rynek analizy obrazu. Głębokie uczenie się (*deep learning*) ma określone zastosowania w niektórych rodzajach detekcji wideo. Dowiedziono, że ma korzystny wpływ na zmniejszenie ryzyka fałszywych alarmów w tego typu systemach.*

Dokładność detekcji zwiększa się, gdy kamera ma wbudowane mapowanie współrzędnych w przestrzeni, dzięki czemu potrafi określić odległość różnych obiektów w swoim polu widzenia. – *Pies z odległości 10 m od kamery jest w przybliżeniu 250 razy większy niż człowiek oddalony o 300 m. Kamery bez wspomnianej funkcji „odbiorą" psa jako większy obiekt i uruchomią alarm, ignorując postać w oddali* – wyjaśnia J. Romanowich. – *Kamera z mapowaniem przestrzeni, przeliczając rozmiar obiektu na podstawie odległości, potrafi określić, że człowiek jest w rzeczywistości większy od psa i – ze względu na jego wielkość – uzna go za właściwy cel.*

System inteligentnej analizy obrazu (VCA) może być zainstalowany w kamerach, na serwerach czy nawet w *edge boxach*, zależnie od zastosowania.

Dla użytkownika różnica sprowadza się zazwyczaj do wymaganego stopnia złożoności algorytmu detekcji albo potrzeby analizowania obrazu w wyższej rozdzielczości. Z powodu ograniczonej przestrzeni wewnątrz obudowy kamery algorytmy VCA instalowane w kamerach mają zwykle ograniczoną szybkość procesora, przepustowość danych i rozmiar dostępnej pamięci. Jeśli zależy nam na lepszej wydajności algorytmu, serwery zawsze będą najkorzystniejszym kosztowo rozwiązaniem – mówi E. Olson. – *Edge boxy to świetna alternatywa, która plasuje się między rozwiązaniami opartymi na kamerze a serwerze. Te niewielkie, odporne na oddziaływania środowiskowe urządzenia, które instaluje się w pobliżu kamer, wykonują funkcje analityczne. Taka wydzielona moc obliczeniowa ma więcej możliwości w zakresie wydajności algorytmów i przepustowości danych.*

W połączeniu z audio

Dla operatorów ujęcie intruza nie jest zwykle tak istotne jak jego odstraszenie, dlatego też obraz często jest łączony z dźwiękiem. *Nasze głośniki sieciowe współpracują z systemem Axis Perimeter Defender. Uumożliwia to operatorom zdalny kontakt z osobami i powstrzymanie ich przed niepożądaną aktywnością. Głośnik może także odtwarzać nagrany uprzednio plik dźwiękowy, który jest uruchamiany ręcznie lub automatycznie w odpowiedzi na sygnał alarmowy* – wyjaśnia A. Sorri. – *Synergię tę można osiągnąć przy niewielkim wysiłku konfiguracyjnym, a każde z urzą-*

RADAR ZDOBYWA POPULARNOŚĆ W OCHRONIE OBWODOWEJ

Radary są coraz częściej wybierane jako alternatywa do ochrony obwodowej, zapewniają bowiem doskonałą skuteczność w konkurencyjnej cenie.

Radar wykrywa i wyznacza odległości za pomocą fal radiowych (*Radio Detection and Ranging*), działa więc jak aktywny detektor. Wysyła do otoczenia sygnały i „nasłuchuje" powracającą do niego energię. Jeśli w jego zasięgu znajdzie się obiekt, którego wcześniej tam nie było, wykrywa ten fakt i przekazuje informację operatorowi.

W porównaniu do innych rodzajów czujek, które wykrywają obecność intruza, radar zapewnia więcej informacji na temat obiektu. *W zależności od sposobu zarządzania radarem pozyskane dane można przekształcić w informacje o ruchu, jego kierunku, prędkości, odległości i orientacji w przestrzeni* – wyjaśnia Martin Maidhof z Działu Bezpieczeństwa Biznesowego w InnoSenT. Radar jest niewrażliwy na działanie różnych czynników środowiskowych. *To bardzo stabilna technologia, zapewniająca działanie bez względu na warunki atmosferyczne* – dodaje M. Maidhof. – *Dla radaru odbicie światła, pył, mgła czy deszcz nie stanowią żadnego problemu.*

Koszty serwisowania radaru są względnie niskie, wymagane jest jedynie ich okresowe czyszczenie. Co ważne, radar może objąć swoim zasięgiem duże obszary – od kilku metrów do nawet kilku kilometrów. Jest zatem rozwiązaniem ekonomicznym w porównaniu do innych technologii. Zdaniem ekspertów koszt kilku radarów monitorujących 15–20 km ogrodzenia może być nawet o połowę mniejszy od kosztu zamontowania wysokiej jakości kamer. Ponadto radar odciąża operatorów, którzy nie muszą przez cały czas wpatrywać się w monitory. Nie oznacza to jednak, że użytkownicy powinni zrezygnować z kamer dozorowych – obraz z nich umożliwia wizualną weryfikację wykrywanych obiektów. System radarowy zintegrowany z kamerami optymalizuje ochronę obwodową, zapewniając użytkownikowi detekcję i weryfikację. *Coraz ważniejsza na rynku staje się współpraca techniki radarowej z innymi, np. z telewizją dozorową. Korzyścią takiego podejścia jest wykorzystanie zalet obu tych rozwiązań – liczba fałszywych alarmów zostanie ograniczona, a przy tym poprawi się wydajność systemów* – podkreśla Maidhof.

dzeń pracuje autonomicznie i niezależnie, zapewniając redundancję.
Podobne rozwiązania automatycznych komunikatów audio oferuje PureTech Systems. Jednak zastosowanie zespołu głośników zewnętrznych to tylko jedna z możliwości.Dla bardziej rozbudowanych lub zaawansowanych układów rozwiązanie rozszerzone zawiera opcję zastosowania odstraszającego systemu audio dalekiego zasięgu (*LRAD: Long-Range Audio Deterrent*). System korzysta z funkcji dźwięku kierowanego, w którym skupia jego strumień bezpośrednio na intruzie. Stosując tę samą technologię *auto trackingu*, sterowaną przez analitykę obrazu, kierunkowy system LRAD skupia emitowany dźwięk na celu nawet wtedy, gdy ten się porusza. Jak sama nazwa wskazuje, urządzenia te mogą wywierać dodatkową presję na intruzie, wydając bardzo głośne, ukierunkowane i odstraszające dźwięki.

Na co zwracać uwagę

Dokonując wyboru rozwiązania ochrony obwodowej opartego na analizie sygnału wizyjnego, integratorzy powinni zwracać uwagę na kilka kluczowych elementów, jak cena, wydajność czy łatwość wdrożenia i użytkowania. *Warto postawić na takie produkty, które są elastyczne i mogą obsługiwać elementy najlepsze w swojej klasie, jednocześnie dając możliwość integrowania z szeroką gamą urządzeń i systemów ochrony perymetrycznej firm trzecich, takich jak systemy zarządzania obrazem VMS, kontrola dostępu, czujniki napłotowe, radar i detekcja mikrofalowa* – podsumowuje M. Prysock. Kluczowe jest jednak spełnienie wymagań i oczekiwań użytkownika. *Należy sobie zadać kilka pytań. Po pierwsze, czy rozwiązanie spełnia wymagania klienta dotyczące detekcji. Po drugie, w jaki sposób możliwości VCA wpisują się w konstrukcję systemu. Czy można go zintegrować z istniejącym oprogramowaniem do zarządzania obrazem i wykorzystać dostępne kamery, czy też wymagana jest rozbudowa? Czy system inteligentnej analizy obrazu jest oparty na urządzeniach brzegowych, serwerze, czy na obu tych rozwiązaniach? Warto też się zastanowić, czy system zapewnia odpowiedni stosunek jakości do ceny i czy oferuje użytkownikowi końcowemu możliwości rozwoju infrastruktury dozorowej w przyszłości* – analizuje E. Olson.

Wybierając narzędzia do analizy obrazu, postaw na takie, które są elastyczne i mogą obsługiwać elementy najlepsze w swojej klasie, jednocześnie dając możliwość integrowania z systemami innych producentów.

Czujki (wciąż) są najważniejsze

W ochronie obwodowej do wykrywania zagrożeń lub intruzów nadal stosuje się czujki i sensory. Mogą być to czujki napłotowe, mikrofalowe lub światłowodowe kable sensoryczne – każdy typ opiera się na innej technologii detekcji. Coraz więcej usprawnień pojawia się w dziedzinie czujników światłowodowych. Poprawia się ich dokładność i zmniejsza liczba fałszywych alarmów.
Skala możliwości naszych światłowodowych czujników detekcji intruza pozwala przeanalizować sygnały z otoczenia, z odróżnieniem losowo rozproszonych zakłóceń wywołanych warunkami atmosferycznymi od zakłóceń skoncentrowanych, wywołanych przez rzeczywiste zagrożenia. W efekcie rośnie prawdopodobieństwo detekcji i zmniejsza się ryzyko alarmów zwodniczych – podkreśla Stewart Dewar, manager produktu w Senstar. – *Czujniki światłowodowe pracują wyjątkowo dobrze na obszarach o wysokim prawdopodobieństwie występowania wyładowań elektrycznych* – dodaje.
Technologie światłowodowe mają tę zaletę, że eliminują wszelkie zwodnicze alarmy wynikające z uderzeń piorunów lub wywołanych przez nie zniszczeń. Są zatem idealne do ochrony takich obiektów, jak elektrownie i stacje elektroenergetyczne, gdzie występują silne pola elektryczne – mówi S. Dewar.
Bernard Lee, wiceprezes ST Electronics, opowiada o czujnikach światłowodowych sprzedawanych pod marką AgilFence. *Skuteczny napłotowy system ochrony obwodowej FIDS* (Fence Instrusion Detection System) *powinien określać, czy zakłócenia są obecne na długim odcinku ogrodzenia, co prawdopodobnie jest wywołane przez czynniki środowiskowe, takie jak deszcz lub silny wiatr. A jeśli zakłócenia występują na jednym przęśle? Wtedy prawdopodobnie mamy do czynienia z włamaniem. Aby takie rozwiązanie zadziałało, czujniki trzeba rozlokować w niewielkich odstępach* – wyjaśnia B. Lee. *System ochrony obwodowej AgilFence wykorzystuje technologię światłowodowej siatki Bragga* (FBG: Fibre Bragg Grating), *w której czujniki są wbudowane bezpośrednio w kabel światłowodowy. Montujemy jeden czujnik FBG co kilka metrów, aby obejmował 2–3 przęsła ogrodzenia, w zależności od jego typu. Zapewnia to dokładność detekcji równoważną odstępom pomiędzy czujnikami FBG, każdy z nich jest bowiem odrębny. Ten czujnik, którego długość falowa najbardziej odbiega od wartości bazowej, wskazuje najbardziej prawdopodobne miejsce włamania. Ponadto rozmieszczone w terenie czujniki FBG generują dane wejściowe dla algorytmów przetwarzania sygnału, umożliwiając lepsze dostrojenie szumów tła w rzeczywistym środowisku pracy. W efekcie nasz system pracuje prawidłowo nawet w trudnych warunkach atmosferycznych.*

Czujniki bywają drogie, więc coraz więcej dostawców oferuje rozwiązania o niższym całkowitym koszcie systemu. *Nasz kabel światłowodowy z wbudowanymi czujnikami FBG w działaniu wykorzystuje wiązkę światła. Nie wymaga źródła zasilania ani urządzeń elektronicznych na kontrolowanym terenie. Nie jest także potrzebny kabel sygnałowy. Przecięcie kabla wywołuje natychmiastowy alarm, a jego naprawa polega na zespawaniu spawarką światłowodową bez potrzeby wymiany całego kabla* – wyjaśnia B. Lee. – *Kabel FBG jest wbudowany w system o solidnej architekturze, wykorzystującej wielokanałowe urządzenie nasłuchujące FBG. Każdy kanał jest odizolowany od pozostałych. Przecięcie kabla w jednym miejscu nie ma wpływu na pozostałe kanały, które nadal działają bez przeszkód. Podobnie naprawa jednego kabla nie wpływa na pracę pozostałych kanałów. Jesteśmy obecnie jedyną firmą w branży, która używa tej technologii w ochronie obwodowej na szeroką skalę.*

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

Kamery termowizyjne – przyszłość systemów dozorowych

Zasada działania kamer termowizyjnych opiera się na wykorzystaniu niewidzialnego promieniowania podczerwonego, którego źródłem jest każdy obiekt o temperaturze wyższej od zera bezwzględnego.

Paweł Augustowski
Hikvision Poland

Głównymi zastosowaniami kamer termowizyjnych, z jakimi spotykamy się w naszych projektach, są przede wszystkim:
- ochrona obwodowa obiektów,
- zabezpieczenie granic państwa,
- pomiary w budownictwie,
- pomiary w przemyśle produkcyjnym.

Kamery termowizyjne „widzą" obiekty, których standardowe kamery światła widzialnego nie są w stanie wychwycić (zauważyć, zarejestrować, dostrzec). Przykładem jest głowica pozycjonująca marki Hikvision, model DS-2TD8166-180ZE2F, która dzięki zastosowaniu przetwornika w rozdzielczości VGA (640 x 512 pix) oraz obiektywu typu motozoom o ogniskowej 45–180 mm pozwala na detekcję pojazdu oddalonego o ponad 15 km. Kamera została również wyposażona w moduł kamerowy światła widzialnego typu Darkfighter o rozdzielczości full HD (2 Mpix) z obiektywem o 62x zoomie optycznym, stanowiącą uzupełnienie systemu dozoru wizyjnego chronionego obiektu. Umożliwia ona operatorowi systemu dokładne przybliżenie interesującego obiektu. Kamera ma zaimplementowane takie funkcje, jak:
- *smart tracking* (śledzenie obiektu),
- przecięcie wirtualnej linii,
- detekcja intruza w zadanej strefie,
- wejście/wyjście z obszaru,
- detekcje pożaru.

W ofercie światowego lidera systemów telewizji dozorowej są również kamery stałopozycyjne. Najpopularniejszym modelem jest kamera termowizyjna w obudowie typu *bullet* DS-2TD2166 o rozdzielczości VGA (640 x 512 pix). Znajduje ona zastosowanie w ochronie perymetrycznej granic państwa i ważnych obiektów wojskowych. W połączeniu z kamerą obrotową światła widzialnego stanowi spójny, zintegrowany system – przekroczenie wirtualnej linii (wirtualnego płotu) w module termowizyjnym wywoła preset w kamerze obrotowej.

Operator systemu monitoringu zarządzający 150 kamerami nie jest w stanie skutecznie chronić obiektu, dlatego coraz częściej inwestorzy wymagają od producentów systemów zabezpieczeń integracji oraz wykorzystania inteligentnych funkcji, np. wtargnięcia intruza w strefę, po którym zostanie wyzwolony preset w kamerze, a obraz pojawi się w głównym podglądzie na żywo.

Szybki rozwój oferty i spadek cen kamer termowizyjnych sprawia, że coraz częściej znajdują one zastosowanie w rozwiązaniach cywilnych. Ważnym aspektem dla inwestora jest też jakość oraz warunki gwarancji na produkty z serii termowizyjnej. Standardowo producent udziela gwarancje na 36 miesięcy, z możliwością przedłużenia do 60 miesięcy. Potwierdza to wysoką jakość systemów marki Hikvision.

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

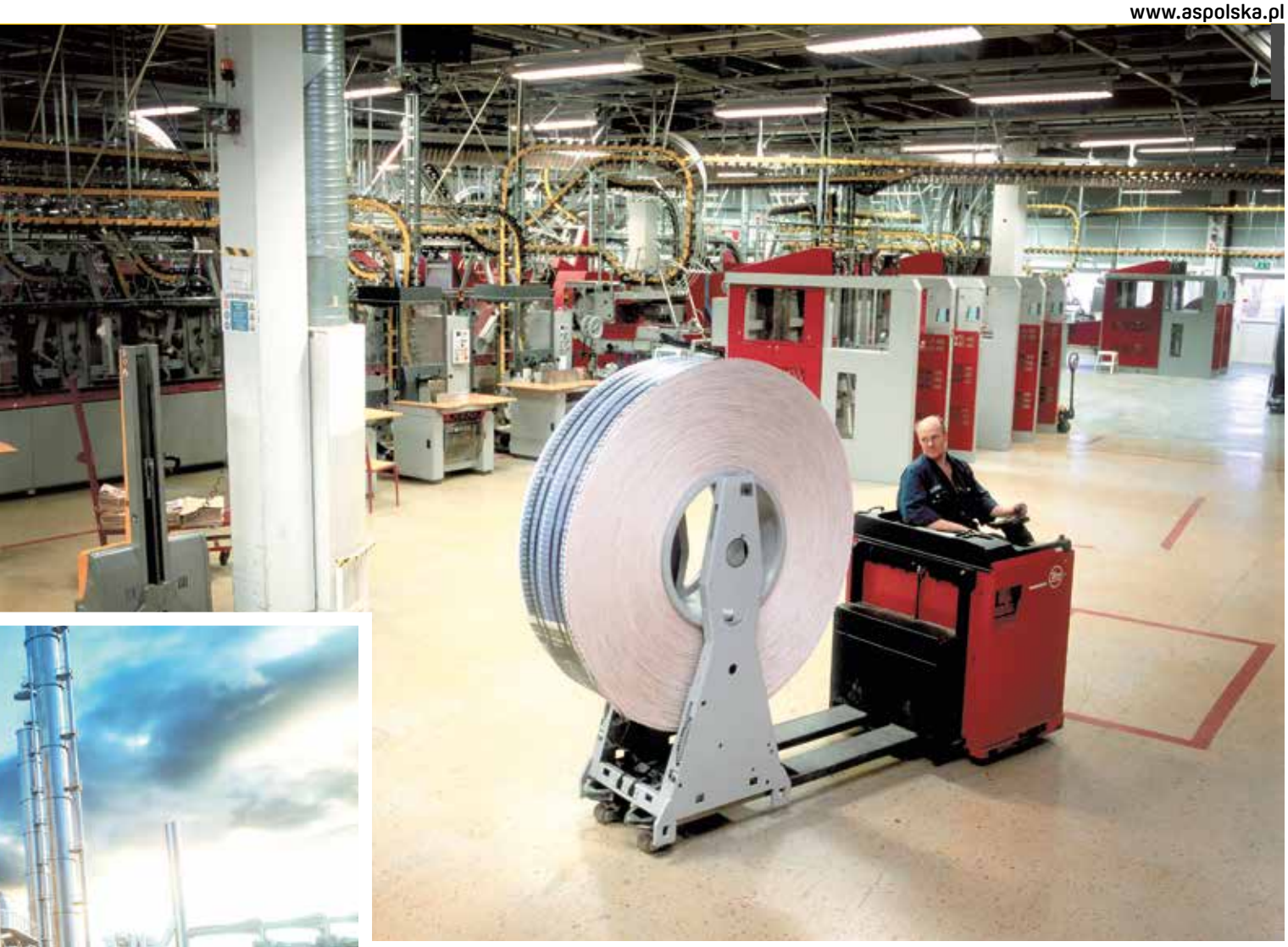
Rozwiązania w ochronie zewnętrznej obiektów przemysłowych

Odległe lokalizacje. Niebezpieczne warunki. Nieprzyjazne otoczenie. Zabezpieczenie, kontrola i zarządzanie bezpieczeństwem obiektów przemysłowych stanowi duże wyzwanie.

Zabezpieczenie obiektów przemysłowych wiąże się z pokryciem rozległych obszarów, a także patrolowaniem i ochroną długich ogrodzeń. Niezwykle istotne jest wykrywanie, lokalizacja i identyfikacja intruzów zarówno przy bramach, wzdłuż ogrodzeń, jak i na wszystkich trasach wiodących do zabezpieczanych obszarów. Kamery muszą szczegółowo objąć zasięgiem ogromne przestrzenie w celu wykrycia obiektu, zlokalizowania go i zweryfikowania, czy jest nim zwierzę, osoba uprawniona, czy też intruz. Spełnienie tego zadania umożliwiają szybkoobrotowe kamery PTZ, które zapewniają szeroki widok monitorowanego obszaru i możliwość zbliżenia każdego detalu. Patrolowanie z wykorzystaniem sterowania PTZ może być obsługiwane przez operatora lub realizowane przez automatyczne śledzenie, kiedy kamera samoistnie śledzi poruszające się osoby, bądź podążając wyznaczoną trasą dozorową przyjmuje automatycznie ustawione prepozycje. Rozwiązaniem może być seria AXIS Q60. Szybkoobrotowe kamery kopułkowe z 35-krotnym zoomem optycznym doskonale odwzorowują detale w najbardziej wymagających zastosowaniach dozorowych i zapewniają pełne pokrycie dużych obszarów.

Rozwiązania Axis do ochrony obwodowej opierają się również na kamerach termowizyjnych z wbudowanym oprogramowaniem do analizy obrazu. Ich zaletą jest to, że sprawdzają się w całkowitej ciemności i automatycznie wysyłają alarm, gdy ktoś wejdzie na określony obszar w polu widzenia kamery. Umożliwia to rozpoznanie podejrzanych działań jeszcze przed wtargnięciem intruza na chroniony teren oraz wzrokowe potwierdzenie zdarzeń, zanim operator podejmie odpowiednie czynności. Przykładem może być seria kamer AXIS Q19, które na monitorowanym obszarze wykrywają ludzi i przedmioty o temperaturze wyższej od otoczenia. Nowością jest seria kamer AXIS Q86 (AXIS Q8641-E PT oraz AXIS Q8642-E PT) stanowiących połączenie kamer termowizyjnych z głowicami PT (pochylenie/obrót). Idealnie sprawdza się w całodobowej ochronie obszarów wewnątrz obiektów i na zewnątrz. Urządzenie można łatwo zintegrować z innymi kamerami IP, reflektorami, głośnikami i istniejącymi systemami zabezpieczeń, aby zapewnić optymalne działanie systemu.

Kamery dozorowe w obiektach przemysłowych mogą nie tylko wykrywać zagrożenia i przeciwdziałać incydentom, ale także usprawniać monitorowanie procesów technologicznych. Dzięki aplikacjom wizyjnym Axis można zweryfikować występujące podczas produkcji problemy z ciśnieniem, przepływami, temperaturą czy wyciekami i podjąć działania, zanim powstaną straty. W takich zastosowaniach sprawdzi się sieciowa kamera termograficzna nowej serii AXIS Q29 umożliwiająca zdalny nadzór zmian temperatury. Pozwala na zdalną obserwację temperatury krytycznej



Kamery dozorowe mogą nie tylko wykrywać zagrożenia i przeciwdziałać incydentom, ale także usprawniać monitorowanie procesów technologicznych.

zarówno na krótkich, jak i długich dystansach. Model AXIS Q2901-E może całodobowo nadzorować temperaturę urządzeń w celu wyeliminowania ryzyka przegrzania. Stosując modele AXIS Q2901-E i AXIS Q2901-E PT Mount, można utworzyć wiele stref alarmowych, z których zostanie wysłane powiadomienie, gdy temperatura osiągnie poziom wyższy lub niższy od określonych wcześniej progów.

System zabezpieczeń będzie bardziej efektywny, gdy zastosuje się nowoczesne kamery megapikselowe ze strumieniowaniem wielokanałowym, a także zapisywanie nagrań w wysokiej rozdzielczości i jakości obrazu HDTV do dalszej analizy zawartości jego treści. Można wykorzystać serię AXIS P13, którą stanowią wytrzymałe, stałopozycyjne kamery sieciowe o znakomitej jakości obrazu i rozdzielczości do 5 megapikseli. Warte uwagi są też wandaloodporne, stałopozycyjne modele kopułkowe wyposażone w funkcje zdalnego ogniskowania i zbliżania (seria AXIS P33) oraz nowa sieciowa kamera typu *bullet* z wbudowanym oświetlaczem podczerwieni, oferująca obraz w wysokiej jakość HD oraz 18-krotny zoom optyczny (AXIS Q1765-LE). Doskonałym rozwiązaniem są również kamery serii AXIS Q16 (pierwsze na świecie kamery z inteligentnym obiektywem i-CS), które gwarantują doskonałą jakość obrazu w trudnych warunkach oświetlenia.

Rozwiązania Axis umożliwiają ponadto wdrożenie otwartej platformy, którą można stopniowo integrować z innymi systemami funkcjonującymi w obiekcie i korzystać z aplikacji analitycznych innych producentów. Przykładem takiego udanego wdrożenia rozwiązania opartego na kamerach Axis jest system zainstalowany w zakładach produkcyjnych Cadbury Wedel. *Szczególnie w branży FMCG efektywny system monitoringu wizyjnego odgrywa kluczową rolę ze względu na konieczność zapewnienia bezpieczeństwa i spełnienia rygorystycznych standardów. Aby był skuteczny, musi być dostosowany do potrzeb firmy i jej pracowników, efektywny kosztowo, sprawdzać się w każdych warunkach, a także być odpowiednio dyskretny oraz dopasowany do wystroju i aranżacji przestrzeni. Wymagania, jakie postawiliśmy, spełnił system monitoringu wizyjnego IP oparty na kamerach Axis Communications* – powiedział Michał Labocha, krajowy kierownik ds. bezpieczeństwa w Cadbury Wedel.

Miwi Urmet Sp. z o.o.
ul. Pojezierska 90A, 91-341 Łódź
tel. 42 616 21 00
miwi@miwiurmet.pl | www.miwiurmet.pl

Nowe bariery do ochrony perymetrycznej

MIWI URMET od wielu lat jest uznanym dostawcą barier podczerwieni oraz barier mikrofalowych do ochrony perymetrycznej obiektów. W ostatnim czasie oferta w tym zakresie została poszerzona o nowe produkty firmy Mitech®.

Mitech® jest włoskim producentem barier i czujników do ochrony perymetrycznej. Urządzenia te, produkowane i wytwarzane we Włoszech, charakteryzują się innowacyjnością, najwyższą niezawodnością oraz wysoką jakością wykonania. Pełna gama produktów pokrywa zapotrzebowanie budownictwa cywilnego, przemysłu, a także obiektów wrażliwych, takich jak więzienia, obiekty militarne czy odcinki granic.

MAGNUS Bariery dualne IR+MW

Urządzenia zapewniają najwyższy stopień zabezpieczenia perymetrycznego za pomocą technologii wiązek podczerwieni oraz mikrofali działających wspólnie. Kolumny są dostępne w wysokościach 1,5 m, 2,0 m, 2,5 m oraz 3,0 m. Część IR może tworzyć sieć maksymalnie 18 skrzyżowanych wiązek podczerwieni. Wiązki podczerwieni są cyfrowo kodowane, a synchronizacja następuje za pomocą sygnału optycznego. Wiązka mikrofalowa jest generowana przez nowoczesną antenę planarną – szerokość wiązki wynosi maksymalnie 1,0 m, a jej wysokość 2,5 m. Dzięki temu bariera nadaje się do zastosowań tam, gdzie dotychczas bariery mikrofalowe nie mogły być stosowane ze względu na zbyt dużą szerokość wiązki mikrofali w urządzeniach z anteną paraboliczną. Urządzenie oferuje 200 kanałów pracy wiązki mikrofalowej. Kolumny mogą być połączone magistralą RS485, dzięki czemu możliwe jest programowanie i monitorowanie torów mikrofalowych. Kolumny są wykonane z wytrzymałego profilu aluminiowego osłoniętego tubą poliwęglanową. Urządzenia wewnętrzne w kolumnie są zamontowane fabrycznie – bariera wymaga jedynie podłączenia zasilania, sygnałów alarmowych oraz zamocowania do podłoża. Kolumny bariery MAGNUS występują w wersjach jedno- oraz dwukierunkowej. W obu wersjach istnieje możliwość regulacji wiązek zarówno w pionie, jak i w poziomie. Kolumny są dostępne w dwóch opcjach: TOWER (kolumna zwieńczona pokrywą) oraz GARDEN (kolumna z możliwością montażu lampy ogrodowej). Dla kolumn TOWER dostępne są akcesoria w postaci pokrywy z czujnikiem nacisku oraz pokrywy z możliwością montażu kamery. Maksymalny zasięg barier MAGNUS wynosi 100 m.

MICRO bariera MW

Bariera MICRO wykorzystuje tę samą technologię mikrofalową co bariera MAGNUS – zawiera tylko tor MW. Nowoczesna antena planarna generuje wiązkę MW o szerokości ok. 1 m (dla zasięgu 100 m) i 2 m (dla zasięgu 200 m). Maksymalny zasięg barier MICRO wynosi 200 m (należy wybrać odpowiednią wersję). Bariera MICRO występuje w formie wysokich kolumn GARDEN i TOWER, lub mniejszych: MICRO 30 (o wysokości do 30 cm bez zasilacza) lub MICRO 50 (o wysokości do 50 cm, z zasilaczem buforowym).

Bariery podczerwieni GARDEN i TOWER IR

Do obiektów, gdzie nie jest wymagane zabezpieczenie za pomocą wiązki mikrofalowej, przeznaczone są kolumny GARDEN i TOWER wyposażone tylko w tory podczerwieni. W tej konfiguracji bariery mogą tworzyć siatkę nawet 50 skrzyżowanych wiązek.

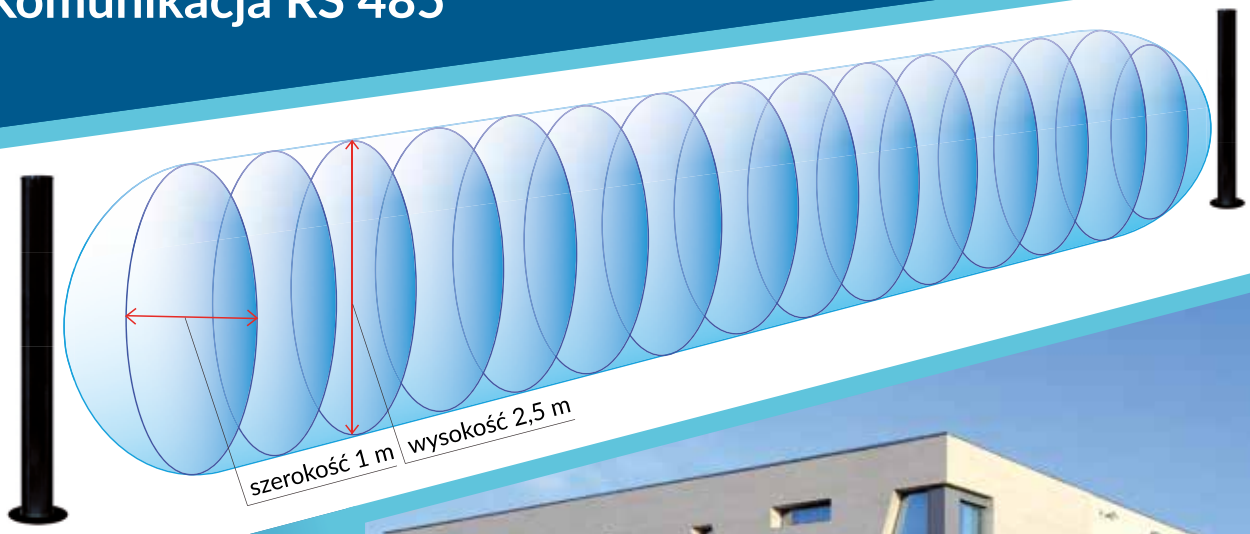
Bariery podczerwieni FOSTER

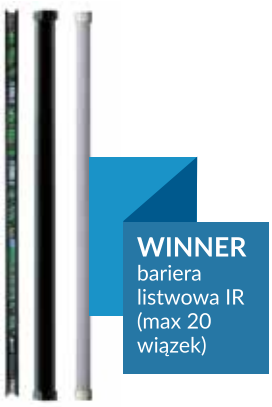
Bariery FOSTER występują w kolumnach o wysokościach od 1 do 3,5 m. Mogą tworzyć sieć maksymalnie 50 skrzyżowanych wiązek. Kompaktowy kształt kolumny ułatwia montaż na ścianie lub słupku. Bariery MAGNUS, TOWER i GARDEN IR, MICRO oraz FOSTER są fabrycznie wyposażone w grzałki i termostaty, dzięki czemu zakres temperatury ich pracy jest szeroki – od -35°C do 70°C. Ich zasięg wynosi maks. 100 m. Tory podczerwieni mogą być programowane do pracy AND (wymagane naruszenie co najmniej dwóch wiązek) lub OR (wymagane naruszenie co najmniej jednej wiązki). Tryb AND może być załączany zdalnie za pomocą dedykowanego wejścia sterującego.

MAGNUS

Nowoczesna bariera dualna IR+MW

- Cyfrowa technologia
- Nowoczesna antena planarna MW (tylko 1 m szerokości wiązki)
- 18 skrzyżowanych wiązek IR
- Dedykowane oprogramowanie PC
- Komunikacja RS 485





WINNER
bariera listwowa IR (max 20 wiązek)

FOSTER
bariera IR (max 50 skrzyżowanych wiązek)

GARDEN TOWER
bariera IR / dualna IR+MW (max 50 skrzyżowanych wiązek)

MIWI URMET Sp. z o. o.
91-341 Łódź, ul. Pojezierska 90a | tel. 42 616 10 94 | miwi@miwiurmet.pl | www.miwiurmet.pl

Aegton Systems
ul. Górecka 31/3, 60-201 Poznań
tel. +48 512 813 723
biuro@aegton.pl

BigEye
Distributed Security

Integrować czy nie?

Jakie problemy rozwiązuje integracja systemów zabezpieczeń?

Mamy system dozoru wizyjnego, system alarmowy, kontrolujemy dostęp do pomieszczeń, mamy też świetny system sygnalizacji pożarowej. **Nasz obiekt jest teoretycznie bezpieczny, a jednak nadal borykamy się z różnymi problemami.**

Skala

To, czy powinniśmy integrować, zależy od skali chronionego obiektu. Optymalne zarządzanie bezpieczeństwem oznacza co innego w małym budynku, co innego w zakładzie, w którym chronionych jest sześć dużych budynków, plac magazynowy i trzy bramy wjazdowe, jeszcze co innego w budynku, w którym pracuje wiele firm.

Problemy

Tworząc system integracyjny BigEye Distributed Security, odpowiadano na konkretne problemy działających firm. Systemy zabezpieczeń cały czas się rozwijają, jest też coraz większe zapotrzebowanie na ich wdrażanie. Im ich więcej, tym trudniej się nimi zarządza. Systemy wysyłają różne sygnały, ale ich identyfikacja, sprawdzenie i lokalizacja jest uciążliwa. Dochodzi do paradoksu – zautomatyzowana ochrona nie chroni skutecznie. Integracja systemów staje się w takich przypadkach narzędziem niezbędnym. Poprawia się wówczas czas reakcji na alarm, występuje powtarzalność postępowania w danych przypadkach (BigEye wyświetla scenariusze postępowania), mamy pewność, że do reakcji ochrony doszło (system informuje zwierzchników o alarmie, którego ochrona nie odwołała). Co więcej, łatwiejsza jest analiza, odszukiwanie i raportowanie, gdy zamiast zbierać dane z różnych systemów, wszystkie zostały zarejestrowane w jednym. Integracja usprawnia, optymalizuje, czyli gwarantuje bezpieczeństwo na jeszcze wyższym poziomie.

Problem	Rozwiązanie BigEye DS
W naszej firmie jest 6 budynków, każdy stawiany w innym czasie, w każdym są różne systemy SSWiN, KD oraz ppoż.	Integracja pozwala zarządzać wszystkimi systemami, nawet różnych producentów. BigEye „zbiera" wszystkie sygnały i prezentuje je na jednym ekranie, na jednej mapie, a ochrona uczy się obsługi jednego systemu.
Nasz budynek jest rozległy, mamy zainstalowanych kilkaset kamer, ale znalezienie tej, która pokazuje obraz pomieszczenia z wywołanym alarmem, trwa za długo.	BigEye „spina" elementy różnych systemów. Jeśli alarm wywołuje czujka X, to automatycznie wyświetla się obraz z kamery sparowanej z tą czujką. Natychmiast widać sytuację alarmową.
Codziennie wjeżdża do nas około 150 tirów dostawczych. Wprowadzamy system awizacji, ale ochrona na wjeździe obsługuje kierowców zbyt wolno.	Integracja systemu awizacji, sczytywania tablic rejestracyjnych, ramienia szlabanu i kiosku drukującego umożliwia automatyczną identyfikację podjeżdżającego tira (tablice rejestracyjne) z wpisem awizacyjnym, podniesienie szlabanu i wydruk dokumentów z instrukcją, dokąd ma jechać.
Mimo szczelnej ochrony towar ginie. Podejrzewamy, że jest wywożony.	BigEye integruje kamery bezprzewodowe (sportowe). System może uniemożliwić otwarcie bramy wyjazdowej, jeśli nie zarejestruje nagrania z mobilną inspekcją nagraną przez ochronę i nie przypisze do widocznej tablicy rejestracyjnej. Stąd pewność, że auto wyjechało puste.
Chcemy zautomatyzować ruch pojazdów wjeżdżających i wyjeżdżających.	BigEye umożliwia sczytanie tablic rejestracyjnych, tworzenie białych i czarnych list numerów oraz automatyczne otwieranie szlabanu lub bramy. Pojazdom z listy białej brama otworzy się automatycznie. Lista biała może być stała (pracownicy) lub zarządzana na bieżąco (zgłoszenie auta).

Więcej na: https://integracjesystemow.pl

Miwi Urmet Sp. z o.o.
ul. Pojezierska 90A, 91-341 Łódź
tel. 42 616 21 00
miwi@miwiurmet.pl | www.miwiurmet.pl

Sprzętowa realizacja zadań w systemie PROTEGE GX

PROTEGE GX jest zintegrowanym systemem bezpieczeństwa i automatyki przeznaczonym do różnych obiektów – od najmniejszych, po rozbudowane i rozległe systemy wielolokalizacyjne. Wpisuje się w coraz powszechniejsze systemy SMS *(Security Management Systems)*, jednak **wyróżnia go bardzo istotna zaleta: sprzętowa realizacja zadań.**

PROTEGE GX jest systemem składającym się z oprogramowania i urządzeń. Oferuje szeroką funkcjonalność obejmującą systemy kontroli dostępu, sygnalizacji włamania i napadu, CCTV, automatyki budynku, interkomunikacji, rejestracji czasu pracy, rejestracji gości, zarządzania windami, obsługę czujek REDWALL REDSCAN, obsługę urządzeń bezprzewodowych INOVONICS.
Oprócz wymienionych funkcji realizowanych bezpośrednio przez system integruje on systemy i urządzenia innych producentów: zewnętrzne systemy BMS, systemy zamków offline (np. SALTO SALLIS, ASSA ABLOY APERIO, KABA CENCON), systemy CCTV i systemy interkomowe SIP innych producentów, systemy zarządzania windami OTIS, KONE, SCHINDLER i THYSSEN KRUPP, Modbus, Automation & Control Protocol, DData Sync (integracja baz danych, WebSOAP, Microsoft Message Queue, Active Directory LDAP).

Cechą charakterystyczną systemu i wyróżniającą go na tle innych dostępnych na rynku rozwiązań jest SPRZĘTOWA REALIZACJA ZADAŃ. Polega ona na zapewnieniu pełnej funkcjonalności systemu dla użytkownika na poziomie urządzeń (kontrolerów). Dzięki takiemu rozwiązaniu system działa (udziela dostępu, zabezpiecza strefy alarmowe, steruje windami, zapewnia integrację z CCTV, BMS itp.) bez udziału serwera i oprogramowania.
Możliwość stosowania szerokiej gamy urządzeń, w tym kontrolerów z pełną funkcjonalnością pracy offline, umożliwia stworzenie systemu bezpieczeństwa, który może działać nieprzerwanie dzięki w pełni rozproszonej logice. Dopóki pojedynczy kontroler będzie działał, dopóty elementy do niego podłączone będą spełniały swoje zadanie.
Ta unikatowa właściwość systemu PROTEGE GX rozwiązuje bardzo ważny problem, z którym często spotykają się użytkownicy innych systemów – działanie systemu jest stale zapewnione, niezależnie od infrastruktury IT czy sprzętu komputerowego i oprogramowania.
Oprogramowanie systemu PROTEGE GX umożliwia aktywne i intuicyjne zarządzanie systemem. Występuje ono zarówno w wersji aplikacji dla systemu Windows, jak i w formie interfejsu Web dostępnego za pośrednictwem przeglądarki internetowej. Oprogramowanie jest intuicyjne i pozwala na łatwe dopasowanie wyświetlanych treści w zależności od zalogowanego użytkownika.
Już podstawowe wersje oprogramowania oferują więcej niż systemy klasy Enterprise. To, a także bezpłatna aktualizacja oprogramowania sprawia, że koszt posiadania i utrzymania systemu jest niewielki.
Skalowalność systemu jest jednym z jego atutów. Pojedynczy kontroler systemowy może obsłużyć nawet 5 mln użytkowników, 248 drzwi kontroli dostępu, ponad 5 tys. wejść alarmowych, 200 klawiatur itd. Liczba takich kontrolerów w systemie jest nieograniczona. Nieograniczona liczba stref, poziomów dostępu, kontrolerów w systemie, a także globalny i lokalny *anti-passback* sprawiają, że wielkość systemu nie ma limitu.
Funkcjonalność systemu i jego niezawodność sprawiają, że Protege GX cieszy się zaufaniem wielu klientów. Zapewnia on nie tylko nieprzerwane bezpieczeństwo, ale także umożliwia aktywne zarządzanie i redukcję kosztów operacyjnych – wszystko to dzięki swojej skalowalności. To z kolei pozwala na rozwój systemu wraz ze wzrostem oczekiwań.

System PROTEGE GX posiada certyfikaty bezpieczeństwa:

SSWiN: EN50131
Stopień Zabezpieczenia 3, Klasa Środowiskowa II

KD: EN50133
Klasa Rozpoznania 2 (czytniki bez klawiatury)
Klasa Rozpoznania 3 (czytniki z klawiaturą)
Klasa Dostępu B

Nedap Security Management Poland
Al. Niepodległości 69, 02-626 Warszawa
tel. +48 22 322 76 74
anna.twardowska@nedap.com

Nedap AEOS zabezpiecza holenderską sieć światłowodową

Prywatna spółka inwestycyjna Reggeborgh wraz z KPN – największym operatorem sieci w Holandii – nawiązały współpracę w celu budowy krajowej sieci światłowodowej. **Spółka joint venture o nazwie Reggefiber zbudowała nową siedzibę w Rijssen, a do jej zabezpieczenia wybrała rozwiązanie AEOS firmy Nedap.**

Reggefiber zbudowała niemal tysiąc punktów dostępowych (*Point of Presence* – POP) w całej Holandii. Spółka planuje w ciągu najbliższej dekady zwiększyć ich liczbę do czterech tysięcy. Wszystkie koncentratory światłowodowe są wyposażone w kontrolery AEOS, czytniki i najnowsze funkcje AEOS.

Gwarantowana ciągłość działalności biznesowej

Dotychczas Reggefiber zainstalowała światłowody w 150 holenderskich gminach. Oznacza to, że z nowego środka komunikacji korzysta już dziesięć procent obywateli Holandii, a ten odsetek rośnie z każdym dniem. Reggefiber wznosi budynki POP w centralnych lokalizacjach każdego regionu kraju. Punkty POP zawierają kable, switche, systemy chłodzenia i centra komunikacji. Stanowią koncentratory dla danego obszaru objętego światłowodami. Są najważniejszymi elementami w sieci. Dlatego bezpieczeństwo i monitorowanie punktów POP jest sprawą najwyższej wagi, jeśli chodzi o gwarancję ciągłości biznesowej.

W związku z tym Nedap ze swoim partnerem biznesowym Niscayah opracowały wspólnie z Reggefiber specjalny „kontroler POP", wykorzystując do tego standardowe elementy AEOS. Skrojony na miarę kontroler oferuje obecnie wszystkie potrzebne funkcjonalności oraz możliwości rozbudowy o wymagane w przyszłości opcje.

Zarządzanie kontrolerami POP i ich monitorowanie

„Kontroler POP" zmontowany dla Reggefiber zawiera standardowy sprzęt AEOS, dodatkowe czujki, kamery CCTV i wbudowane oprogramowanie realizujące funkcje zarządzania wykrywaniem

włamań i monitorowania go. Zastosowanie standardowych elementów do stworzenia indywidualnie dopasowanego systemu pozwoliło obniżyć koszty prac deweloperskich w porównaniu z systemem robionym na zamówienie od podstaw. Dodatkową zaletą jest fakt, że Reggefiber nie jest zależna od stworzonego indywidualnie oprogramowania i specjalnych interfejsów. Firma może więc dowolnie decydować o rozbudowie lub zmianie funkcjonalności w każdej chwili. Zmniejsza to całkowity koszt posiadania.

Reggefiber nie jest zależna od stworzonego indywidualnie oprogramowania i specjalnych interfejsów. Firma może więc dowolnie zdecydować o rozbudowie lub zmianie funkcjonalności w każdej chwili.

Skalowalność i stabilność

Projekt Reggefiber stanowił wyzwanie ze względu na dużą liczbę lokalizacji POP oraz autoryzacji na poziomie wykonawców i podwykonawców. Każda lokalizacja musiała być wyposażona w czytnik kart przy drzwiach, czujkę stykowa drzwi, czujkę włamania, czujnik wilgotności i czujnik termiczny. Innym wymogiem była konieczność odczytywania i monitorowania wszystkich zgromadzonych informacji przy użyciu najnowszych technologii.

Specjalne warunki środowiskowe i stopień rozbudowy projektu sprawiły, że pod względem technologicznym rozwiązanie AEOS znakomicie się w niego wpasowało: nowoczesna technologia bezpieczeństwa zastosowana do ochrony przyszłej sieci telekomunikacyjnej. AEOS stał się doskonałym wyborem dla projektu jeszcze z jednego powodu: jest skalowalny pod względem wielkości i wydajności oraz obecnie nieprzewidzianych obciążeń. Skalowalność AEOS umożliwiła firmie Reggefiber zwiększenie liczby POP w tempie wykładniczym, bez obaw o stabilność systemu.

Użyteczność

W siedzibie Reggefiber w pełni wyposażona sterownia (sieciowe centrum operacyjne) przez całą dobę monitoruje wszystkie POP. W sytuacji alertu systemu możliwe jest również podjęcie bezpośrednich działań kontroli. Alerty są generowane, gdy osoba nieupoważniona wejdzie do POP, gdy ktoś podejmuje próby sabotażu systemu, gdy wahania temperatury w budynku są zbyt duże, wilgotność wykracza poza ustawione limity lub występuje usterka zasilania. Ze sterowni w Rijssen można też otwierać drzwi POP, gdy technik konserwacji lub napraw odpowiednio się uwierzytelni. Ponadto wykonawcy i podwykonawcy mają specjalne identyfikatory z prawami dostępu do POP (również tymczasowymi lub ograniczonymi). Identyfikatory i uprawnienia przyznaje się z poziomu centralnego serwera AEOS w Rijssen, służącego również do zarządzania nimi. Platforma AEOS jest całkowicie obsługiwana przez sieć, dzięki czemu wydawanie identyfikatorów i zmianę autoryzacji można wykonać na każdej stacji roboczej.

> Platforma AEOS jest obsługiwana całkowicie przez sieć, dzięki czemu wydawanie identyfikatorów i zmianę autoryzacji można wykonać na każdej stacji roboczej.

Elastyczne środowisko

Fizyczną instalację sprzętu AEOS przeprowadzono we współpracy z Niscayah. W zakładzie produkcyjnym, w którym wytwarza się fizyczny sprzęt POP, Niscayah instaluje kontrolery POP. Gdy POP zostanie umieszczony w nowym obszarze objętym światłowodami, Niscayah podłącza kontrolery przez sieć UMTS. Dzięki temu można kontrolować POP i cały sprzęt, jeszcze zanim zostanie skonfigurowana sieć. Gdy sieć stanie się dostępna i będzie działała sprawnie, AEOS przełącza się na nowe, stałe łącze.

Reggefiber zapewnia zaawansowane systemy służące do tworzenia i utrzymywania idealnych warunków roboczych. Wszelkie odchylenia i zakłócenia są natychmiast wykrywane przez czujniki podłączone do elementów AEOS. W sieciowym centrum operacyjnym w Rijssen pracownicy Reggefiber, przy użyciu graficznego narzędzia do obsługi alarmów *(Graphical Alarm Handler)* AEOS, monitorują przychodzące alerty i zajmują się ich obsługą.

Nedap dostarcza ponadto inteligentny zasilacz bezprzerwowy (UPS), który bezpośrednio zasila czujniki i zamki oraz stanowi źródło zasilania awaryjnego. Dzięki centralnemu monitorowaniu stanu technicznego zasilacza personel może proaktywnie reagować na wszystkie problemy z zasilaniem. Proces zapewnienia ciągłości działalności biznesowej jest więc bardziej sprawny i efektywny.

Zabezpieczenie przeciwpożarowe wielkokubaturowych hal magazynowych. Cz. 1

Obiekty wielkokubaturowe przeznaczone na cele produkcyjne i magazynowe w świetle przepisów ppoż. są klasyfikowane jako budynki produkcyjno-magazynowe „PM”.

mgr inż. Edward Skiepko

Podstawowymi parametrami związanymi z określeniem wymagań dla wielkokubaturowych obiektów produkcyjno-magazynowych są:

- gęstość obciążenia, czyli energia wyrażona w megadżulach [MJ], wytworzona w efekcie spalania materiałów palnych znajdujących się w strefie pożarowej przypadająca na jednostkę powierzchni wyrażoną w metrach kwadratowych [m^2],
- zagrożenie wybuchem,
- wysokości (liczba kondygnacji),
- powierzchni budynku (strefy pożarowej).

Na podstawie wartości tych parametrów określa się klasę odporności pożarowej budynku produkcyjno-magazynowego oraz klasę odporności ogniowej elementów. Jest pięć klas (w kolejności od najwyższej do najniższej) „A”, „B”, „C”, „D” i „E”, które różnią się wymaganiami

Klasa odporności pożarowej budynku	Klasa odporności ogniowej elementów budynku					
	główna konstrukcja nośna	konstrukcja dachu	strop	ściana zewnętrzna	ściana wewnętrzna	przekrycie dachu
„A”	R 240	R 30	R E I 120	E I 120 (o↔i)	E I 60	R E 30
„B”	R 120	R 30	R E I 60	E I 60 (o↔i)	E I 30	R E 30
„C”	R 60	R 15	R E I 60	E I 30 (o↔i)	E I 15	R E 15
„D”	R 30	(–)	R E I 30	E I 30 (o↔i)	(–)	(–)
„E”	(–)	(–)	(–)	(–)	(–)	(–)

R – nośność ogniowa (w minutach): stan, w którym element przestaje spełniać swoją funkcję na skutek zniszczenia mechanicznego, utraty stateczności lub przekroczenia granicznych wartości przemieszczeń lub odkształceń;.
E – szczelność ogniowa (w minutach: stan, w którym element przestaje spełniać swoją funkcję na skutek odpadnięcia od konstrukcji lub powstania pęknięć i szczelin, przez które przedostają się płomienie lub gorące gazy;
I – izolacyjność ogniowa (w minutach): stan, w którym element przestaje spełniać swoją funkcję oddzielającą na skutek przekroczenia granicznej wartości temperatury powierzchni nienagrzewanej.
Dla ścian zewnętrznych wymagana jest też odporność na działanie ognia od wewnątrz i z zewnątrz (o↔i)

odporności ogniowej (przede wszystkim czasem funkcjonowania w warunkach pożaru i spełnieniem określonych kryteriów związanych z nośnością, szczelnością i izolacyjnością ogniową) dotyczącymi elementów konstrukcyjnych, takich jak główna konstrukcja nośna, konstrukcja dachu, strop, ściana zewnętrzna i wewnętrzna oraz przekrycie dachu (*tabela*).
Budynki te muszą spełniać określone wymagania w zakresie trwałości i wytrzymałości w warunkach pożaru. Ponieważ wykonanie ich w odpowiedniej klasie odporności pożarowej jest zadaniem trudnym i kosztownym, przepisy techniczno-budowlane dopuszczają zastosowanie urządzeń przeciwpożarowych, dzięki którym można złagodzić wymagania budowlane. Należą do nich: stałe samoczynne urządzenia gaśnicze wodne oraz instalacje służące do oddymiania i odprowadzania ciepła. Stosując np. instalację tryskaczową, można przyjąć klasę „E” bez względu na gęstość obciążenia ogniowego, a więc wykonać budynek praktycznie jedynie z elementów nierozprzestrzeniających ognia (np. ze stali zamiast z żelbetu).
Podobnie wykonując budynek z elementów nierozprzestrzeniających ognia i stosując samoczynne urządzenia oddymiające w strefach pożarowych o powierzchni >1000 m^2 i gęstości obciążenia ogniowego >500 MJ/m^2, również można przyjąć klasę „E” odporności ogniowej. W praktyce pomocne i niekiedy obowiązkowe są również inne instalacje, takie jak system sygnalizacji pożarowej, oświetlenie awaryjne, hydranty wewnętrzne.

Wybór sposobu (sposobów) zabezpieczenia obiektu

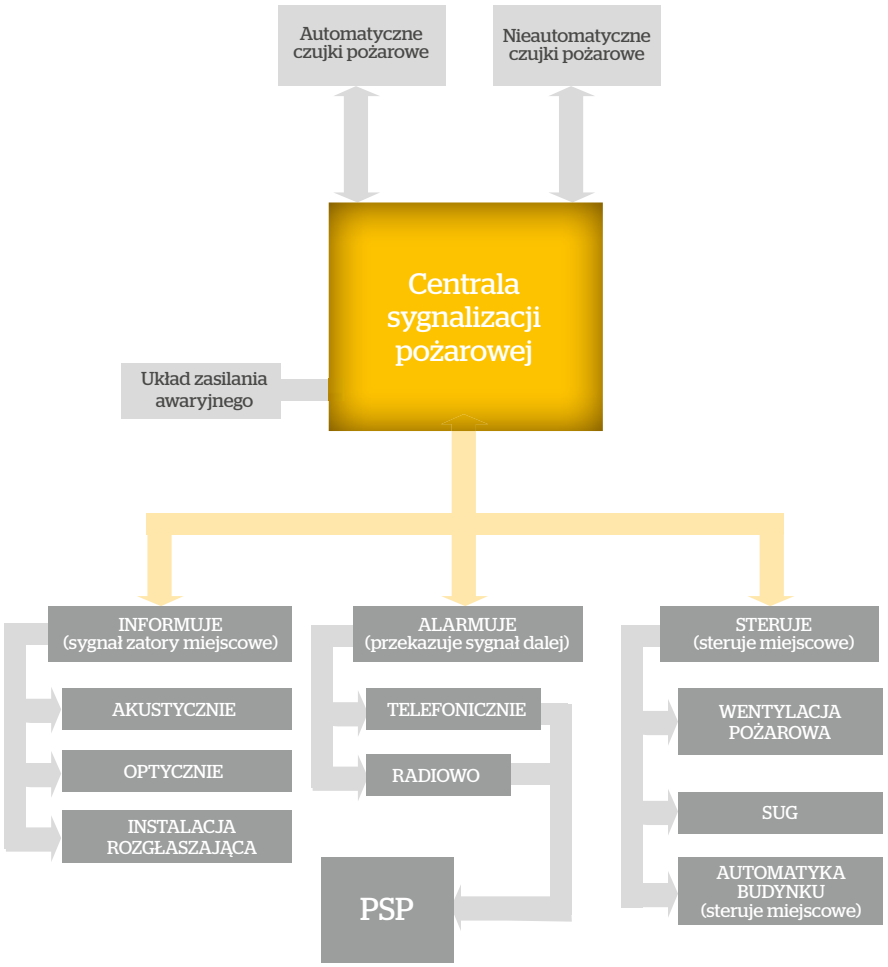
W zależności od przewidywanej gęstości obciążenia ogniowego oraz oceny zagrożenia wybuchem określa się dopuszczalne dla obiektów PM wielkości stref pożarowych, czyli powierzchni, jaką należy wydzielić elementami oddzieleń ppoż. lub pasami wolnego terenu, aby ogień nie przedostał się zarówno z tej strefy, jak i do niej.
Dopuszczalne powierzchnie stref pożarowych są określone w przepisach techniczno-budowlanych. Można je zwiększyć, stosując wymienione w przepisach techniczno-budowlanych urządzenia przeciwpożarowe i ochronę:
- stałymi samoczynnymi urządzeniami gaśniczymi wodnymi: o 100%,
- samoczynnymi urządzeniami oddymiającymi: o 50%,
- a przy jednoczesnym stosowaniu urządzeń wymienionych w ust. 1 dopuszcza się powiększenie stref pożarowych o 150%.

Z kolei:
- w budynku jednokondygnacyjnym lub na ostatniej kondygnacji budynku wielokondygnacyjnego wielkości stref pożarowych PM można powiększyć o 100%, jeżeli nie zawiera on pomieszczenia zagrożonego wybuchem i jest wykonany z elementów nierozprzestrzeniających ognia oraz zastosowano w nim samoczynne urządzenia oddymiające,
- w budynku jednokondygnacyjnym wielkości stref pożarowych PM (z wyjątkiem garażu) nie ogranicza się pod warunkiem zastosowania stałych urządzeń gaśniczych wodnych i samoczynnych urządzeń oddymiających.

Z przytoczonych przykładów wynika, że podstawowymi instalacjami mającymi wpływ na zabezpieczenie przeciwpożarowe są dwie instalacje: tryskaczowa i oddymiająca. Obie powinny działać samoczynnie, tzn. bez udziału człowieka, oczywiście z wyjątkiem przypadków szczególnych, kiedy mają współdziałać i są uruchamiane wg tego samego kryterium, jakim jest temperatura. Sposób współpracy określa się wówczas odrębnie na podstawie scenariusza współdziałania systemów i wiedzy technicznej w tym zakresie.

Urządzenia ppoż. w budynkach wielkokubaturowych

Wszystkie urządzenia przeciwpożarowe w budynkach powinny zostać wykonane zgodnie z projektem uzgodnionym pod względem ochrony ppoż. przez rzeczoznawcę ds. zabezpieczeń przeciwpożarowych. Warunkiem dopuszczenia do użytkowania jest przeprowadzenie odpowiednich prób i badań potwierdzających prawidłowość ich działania. W trakcie eksploatacji natomiast powinny być poddawane przeglądom i czynnościom konserwacyjnym nie rzadziej niż raz w roku zgodnie z zasadami określonymi w polskich normach, dokumentacji producenta itp.



RYS. 1. SCHEMAT INSTALACJI SYGNALIZACJI POŻAROWEJ

ELEMENTY DETEKCYJNE SYSTEMU SYGNALIZACJI POŻAROWEJ

PUNKTOWE CZUJKI CIEPŁA – ich zadziałanie następuje w wyniku wzrostu temperatury otoczenia.

PUNKTOWE CZUJKI DYMU – reagują na produkty spalania i/lub rozkładu termicznego. Ze względu na sposób wykrywania dymu dzielą się na jonizacyjne i optyczne (punktowe i liniowe).

OPTYCZNE LINIOWE CZUJKI DYMU NA ŚWIATŁO POCHŁANIANE – są przeznaczone do wykrywania dymu lub/i temperatury w pomieszczeniach zamkniętych, szczególnie w dużych halach lub pomieszczeniach zabytkowych. Czujka składa się z nadajnika i odbiornika światła podczerwonego, rozmieszczonych naprzeciw siebie, na przeciwległych ścianach kontrolowanego pomieszczenia. Zasada działania czujki polega na analizie przezroczystości optycznej powietrza w przestrzeni pomiędzy czujką a lustrem/reflektorem w odbiorniku. Jeżeli w powietrzu pojawi się określona zawartość aerozoli (dymu), zmniejszająca przezroczystość, to czujka, zgodnie z ustawionym progiem czułości, wejdzie w stan alarmowania.

CZUJKI PŁOMIENIA – wykorzystano w nich absorbent ultrafioletu UV, który pochłania słabe promieniowanie ultrafioletowe zawarte w płomieniach.

RĘCZNE OSTRZEGACZE POŻAROWE – stanowiące uzupełnienie czujek, ich zadziałanie następuje po wciśnięciu przycisku osłoniętego szybką.

URZĄDZENIA UZUPEŁNIAJĄCE – gniazda czujek, wskaźniki zadziałania czujek, adaptery czujek konwencjonalnych, izolatory zwarć, komory powietrzne czujek dymu moduły sterujące i monitorujące.

Wśród urządzeń ppoż. stosowanych w budynkach wielkokubaturowych oprócz wymienionych już można też wyróżnić:

Systemy sygnalizacji pożarowej

Stosowanie urządzeń automatycznej sygnalizacji pożarowej jest wymaganiem ustawowym, jednakże spośród wymienionych tam obiektów nie ma budynków wielkokubaturowych zakwalifikowanych jako PM.

Urządzenia wykrywające pożary w ich początkowej fazie przyczyniają się do ograniczenia szkód wywołanych pożarem, zwłaszcza że w obiektach coraz częściej występuje koncentracja dóbr o dużej wartości. Zachętą do wyposażania budynków w instalacje sygnalizacji pożarowej są zniżki w ubezpieczeniach oferowane przez firmy ubezpieczeniowe. Konieczność wyposażenia budynku w te instalacje może być również rozwiązaniem zamiennym, gdy obiekt nie spełnia niektórych wymagań (np. budowlanych w zakresie bezpieczeństwa pożarowego) oraz gdy nie są w nim zapewnione odpowiednie warunki ewakuacji ludzi.

ZASADA DZIAŁANIA

System sygnalizacji pożarowej (SAP lub SSP) jest kombinacją elementów i ich wyposażenia wraz ze źródłem energii elektrycznej i łączącymi je przewodami. Mają one na celu możliwie wczesne wykrycie, lokalizację oraz sygnalizowanie i alarmowanie o pożarze w fazie jego powstania, a także odróżnienia go od sytuacji podobnej do pożaru w celu podjęcia określonych działań.

Zasada działania systemów SSP jest następująca: uruchomienie instalacji następuje w wyniku zadziałania czujki lub ręcznie. Informacja dociera do centralki sygnalizacji pożarowej, która steruje różnymi funkcjami, np. alarmowaniem optycznym i akustycznym, uruchamianiem urządzeń ppoż. (klapy dymowe, drzwi pożarowe, urządzenia oddymiające, instalacje gaśnicze). Może także sterować zatrzymaniem urządzeń technologicznych. Jednocześnie sygnał alarmowy jest przekazywany za pośrednictwem urządzeń transmisji alarmu do Państwowej Straży Pożarnej (*rys. 1*).

Precyzyjną lokalizację miejsca wystąpienia zagrożenia umożliwia stosowanie adresowania polegającego na przypisaniu każdemu elementowi liniowemu bądź grupie elementów określonego adresu, numeru i rodzaju elementu zainstalowanego w adresowalnej linii dozorowej:

- **adresowanie kolektywne** (grupowe) polega na wskazaniu linii dozorowej, do której czujka pożarowa przesyła sygnał alarmu pożarowego,
- **adresowanie indywidualne** może dotyczyć pojedynczych czujek, ich grup oraz elementów sterujących zainstalowanych na linii dozorowej.

Instalacje tryskaczowe

Instalacja tryskaczowa jest stałym urządzeniem gaśniczym (SUG), w którym czynnikiem gaśniczym jest woda. W rurociągach instalacji ciśnienie czynnika jest utrzymywane na poziomie wynikającym z obliczeń hydraulicznych. W normalnych warunkach pracy rurociągi systemu mokrego są wypełnione wodą. W instalacjach suchych rurociągi – od tryskaczy aż do zaworu kontrolno-alarmowego – są wypełnione sprężonym powietrzem lub azotem. Stale ciśnienie utrzymują w nich pompa dobijająca lub sprężarka.

W momencie pojawienia się pożaru wydzielające się ciepło powoduje wzrost temperatury cieczy w ampułkach tryskaczy powyżej temperatury ich otwarcia. Otwierają się tylko tryskacze znajdujące się bezpośrednio w strefie ognia, co minimalizuje zakres szkód spowodowanych działaniem wody. Przepływająca przez zawór kontrolno-alarmowy woda uruchamia dzwon alarmowy i wyłączniki ciśnienia, które alarmują o pożarze i uruchamiają pompę tryskaczową. Woda jest tłoczona do systemu ze zbiornika ciśnieniowego lub przez pompę tryskaczowa zasilaną z niewyczerpywalnego źródła wody. System pracuje do momentu ręcznego odcięcia wody.

Przy wyborze rodzaju urządzenia tryskaczowego uwzględnia się:

- rodzaj produkcji,
- rodzaj składowanych materiałów,
- temperaturę występującą w ciągu całego roku w przestrzeniach przewidzianych do ochrony.

Rodzaje urządzeń tryskaczowych:

- urządzenie tryskaczowe wodne (mokre) stosowane do ochrony przestrzeni, w których nie występuje ryzyko zamarznięcia lub wyparowania wody i nie jest konieczne zastosowanie urządzenia tryskaczowego sterowanego,
- urządzenie tryskaczowe powietrzne (suche) stosowane do ochrony przestrzeni, w których występuje ryzyko zamarznięcia lub wyparowania wody,
- urządzenie tryskaczowe mieszane do ochrony przestrzeni, w których, poza pojedynczymi pomieszczeniami, nie występuje ryzyko zamarznięcia lub wyparowania wody,
- urządzenie tryskaczowe sterowane do ochrony przestrzeni, w których na skutek przypadkowego zadziałania urządzenia tryskaczowego mogłyby wystąpić duże straty.

Działanie

Pod wpływem wzrostu temperatury ciecz w ampułce się rozszerza. Ciśnienie wewnątrz ampułki rośnie. Po osiągnięciu określonej temperatury ampułka rozpada się na drobne kawałki, umożliwiając wypływ wody z **tryskacza**.

Instalacja

Tryskacze muszą być instalowane zgodnie z aktualnymi standardami światowymi wydawanymi przez FM, LPC, VdS, APSAD lub inne podobne instytucje.

Temperatura, przy której następuje uruchomienie tryskacza, może być bardzo zróżnicowana, dostosowana do temperatur maksymalnych, jakie mogą występować w chronionym obszarze, aby nie doszło do przypadkowego uruchomienia tryskacza. Przykładowo temperatury w sąsiedztwie grzewczych urządzeń przemysłowych są wyższe niż w dużym pomieszczeniu biurowym. Dlatego temperatura wyzwalania tryskacza musi być dostosowana do warunków występujących w strefie chronionej.

Przyjmuje się zazwyczaj, że temperatura uruchomienia tryskacza powinna być wyższa o 30°C od temperatury w pomieszczeniu w warunkach normalnych. O temperaturze, w jakiej pęka ampułka zamykająca, decyduje ciśnienie powietrza wewnątrz niej. Ampułki są oznakowane odpowiednim kolorem (*rys. 2*).

RYS. 2. OZNAKOWANIE AMPUŁEK TRYSKACZY

Tryskacz posiada kilka istotnych parametrów, decydujących o jego wyborze pod kątem różnych zagrożeń:

orientacja (wisząca, stojąca, pozioma)

- tryskacz stojący należy montować tylko w pozycji stojącej, a talerzyk rozbryzgowy nad rurą,
- tryskacz wiszący należy montować tylko w pozycji wiszącej, a talerzyk rozbryzgowy pod rurą,

- średnica przyłącza (DN10, DN15, DN20, DN25);
- współczynnik wypływu K (57, 80, 115, 160, 202, 242, 363);
- szybkość reagowania – standardowego reagowania, specjalnego reagowania, szybkiego reagowania;
- temperatura reagowania – 57, 68, 79, 93, 141, 182, 260 [°C];
- wykończenie – brąz, chrom, biały, czarny;
- zastosowanie – standardowe, magazynowe, domowe (residental), suche.

Skuteczność gaśnicza instalacji tryskaczowych to 98% przypadków w pełni skutecznego działania.

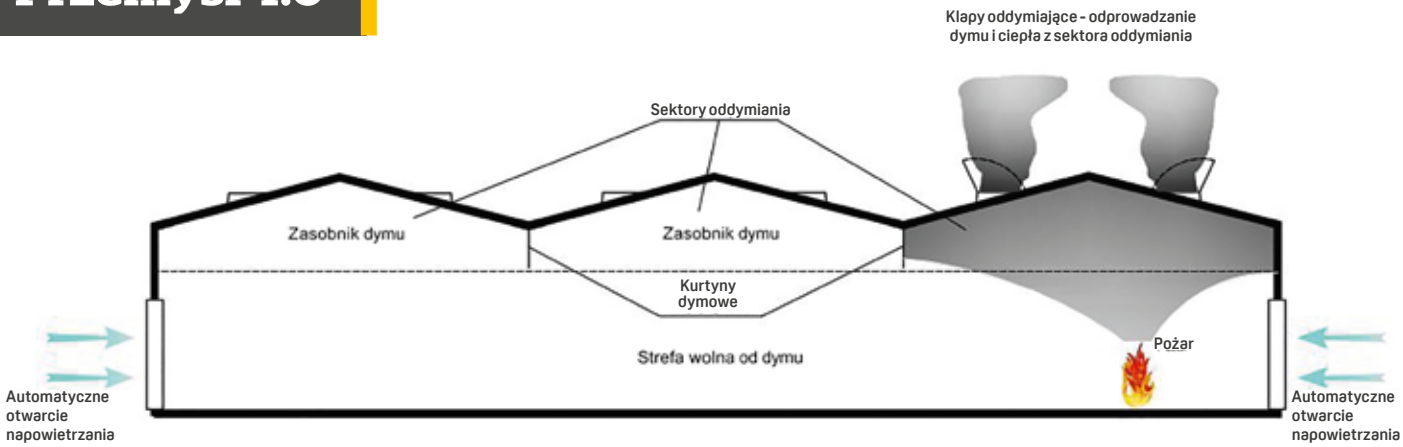
Systemy oddymiania

Cele i funkcje
systemu oddymiania grawitacyjnego

System oddymiania grawitacyjnego wykorzystuje przede wszystkim zjawisko unoszenia gorącego dymu i jego koncentrację w wyższych przestrzeniach pomieszczeń. Podstawowe zadania systemów oddymiania grawitacyjnego (i wszystkich systemów służących do usuwania dymu) są związane z ich działaniem w czasie pożaru.

Obejmują one:

- umożliwienie bezpiecznej ewakuacji z budynku objętego pożarem, pionowymi i poziomymi drogami ewakuacyjnymi,
- zwiększenie widoczności i umożliwienie działań ekipom ratowniczym w przypadku budynków produkcyjno-magazynowych,



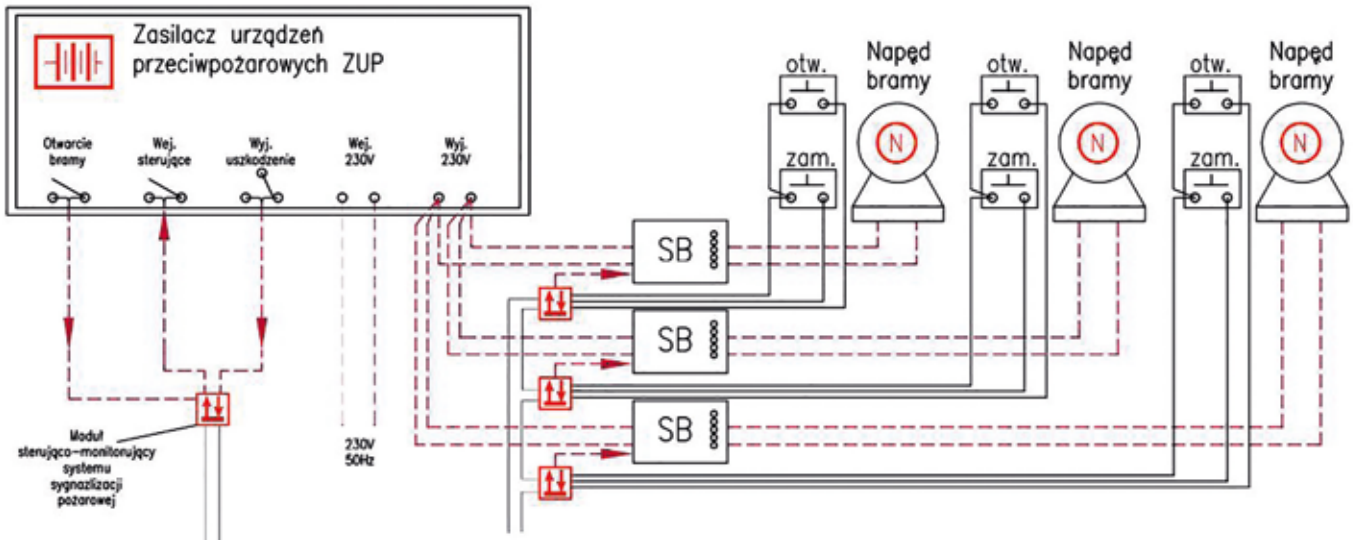
RYS. 3. SCHEMAT ODDYMIANIA HALI WIELKOKUBATUROWEJ

- ograniczenie stężenia toksycznych produktów spalania i rozkładu termicznego oraz ich temperatury poprzez usunięcie ich wraz z dymem, a także rozrzedzenie napływającym, świeżym powietrzem,
- zmniejszenie ryzyka zawalenia się budynku lub jego części poprzez usunięcie gorących gazów spod sufitu, mogących doprowadzić do nagrzania się elementów konstrukcyjnych budynku do wartości krytycznych, po których przekroczeniu następuje utrata ich właściwości nośnych,
- zmniejszenie strat materialnych wywołanych działaniem dymu i temperatury. Dym ma właściwości korozyjne i często zawiera dużo substancji smolistych, przez co może stać się przyczyną uszkodzeń konstrukcji lub wyposażenia budynku,
- opóźnienie rozprzestrzeniania się pożaru i uniemożliwienie wystąpienia zjawiska rozgorzenia – podczas spalania materiałów powstały strumień ciepła rozchodzi się we wszystkich kierunkach, jednak najwięcej energii cieplnej kumuluje się pod sufitem; część tego strumienia po dojściu do przegrody budowlanej (np. sufitu, ściany) zostaje pochłonięta przez przegrodę, część zaś ulega odbiciu i wraca do źródła pożaru, intensyfikując jego spalanie,
- poprawę właściwości dymu – napływające chłodniejsze powietrze wzmaga termiczny napęd dymu (zjawisko unoszenia) i powoduje zwiększenie szybkości jego usuwania,
- zwolnienie trzymaków elektromagnetycznych w drzwiach, które muszą się zamknąć podczas pożaru.

Szczególnym przypadkiem jest zastosowanie oddymiania grawitacyjnego do odprowadzania dymu i ciepła w obiektach wielkokubaturowych, takich jak hale magazynowe czy produkcyjne (*rys. 3*).

Oddymianie ma na celu przede wszystkim ochronę konstrukcji budynku. Hale są podzielone na strefy oddymiania za pomocą kurtyn dymowych, co ma na celu przede wszystkim odgraniczenie rozprzestrzeniania się dymu w warstwie podsufitowej i skuteczne usunięcie dymu z części hali bezpośrednio nad źródłem pożaru.

W systemach tych bardzo ważną rolę odgrywa możliwość dostarczenia świeżego powietrza w miejsce odprowadzanych gazów i dymów. Odbywa się to za pomocą specjalnych klap napowietrzających lub poprzez otwarcie bram i doków załadunkowych. Z praktycznego punktu widzenia nie powinno się to odbywać ręcznie, lecz za pośrednictwem siłowników zasilanych z rezerwowego źródła zasilania. Rozwiązanie takie sprawia, że nawet w przypadku zaniku napięcia czy odłączenia prądu wyłącznikiem przeciwpożarowym siłowniki bram nadal będą



RYS. 4. SCHEMAT ZASILANIA REZERWOWEGO BRAM NAPOWIETRZAJĄCYCH

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

dobrze zaprojektowane BEZPIECZEŃSTWO

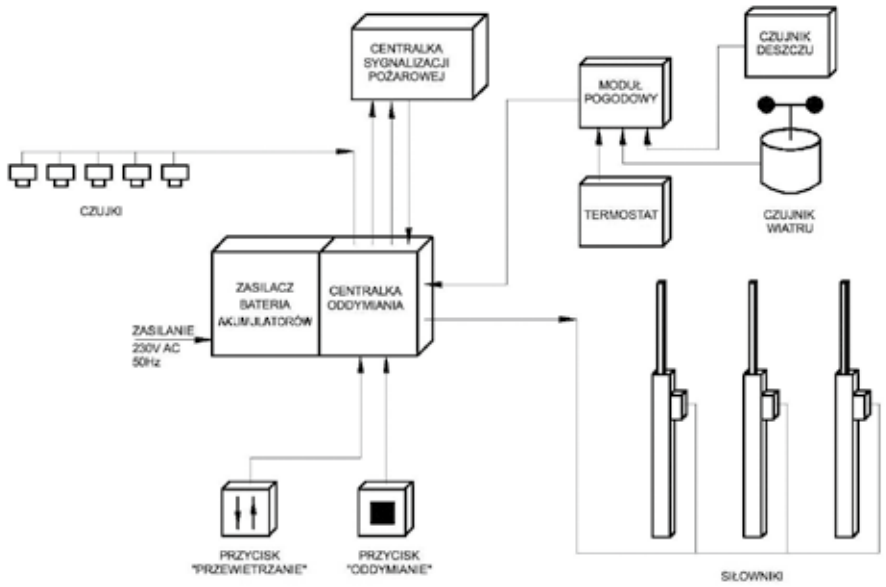
SYSTEMY SYGNALIZACJI POŻAROWEJ

- 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



RYS. 5. KONFIGURACJA ELEKTRYCZNEGO SYSTEMU ODDYMIANIA

zasilane i będzie można uruchomić napowietrzanie. Siłownik współpracuje z systemem sygnalizacji pożarowej lub może monitorować sygnały z wyłączników krańcowych klap. Rozwiązanie to zapewnia w przypadku braku napięcia w sieci zasilającej, że w momencie wykrycia pożaru lub zadziałania klap – kiedy następuje uruchomienie oddymiania – nastąpi przełączenie na źródło zasilania rezerwowego.

Na *rys. 4* przedstawiono układ sterowania z systemu sygnalizacji pożarowej, monitorowanie stanu zasilacza oraz sterowanie otwarciem bram do sterowników „SB". W systemie SSP jest również monitorowane położenie bram.

Rodzaje i zasada działania instalacji sterującej oddymianiem

Systemy sterowania oddymianiem są wyzwalane automatycznie przez urządzenia wykrywające pojawienie się dymu lub wzrost temperatury powietrza. Rozróżniamy:

- systemy pneumatyczne,
- systemy elektryczne,
- systemy mechaniczne
- systemy pneumatyczno-elektryczne, gdzie występuje połączenie funkcji oddymiania (uruchamiane pneumatycznie) i przewietrzania – wentylacji (uruchamiane elektrycznie).

Oprócz wyzwolenia automatycznego systemy są wyposażone w urządzenia wyzwalające ręcznie oraz z systemu sygnalizacji pożarowej. Współpraca instalacji oddymiającej często powinna być zsynchronizowana z pracą innych instalacji. Trudno to wykonać bez zastosowania dodatkowej instalacji integrującej, w tym przypadku w grę wchodzi jedynie system sygnalizacji pożarowej. Podłączenie systemu oddymiania do instalacji sygnalizacji pożarowej umożliwia zsynchronizowanie jej pracy z zadziałaniem instalacji tryskaczowej, uruchomieniem kurtyn dymowych, zamknięciem oddzieleń ppoż., zatrzymaniem działania instalacji użytkowych i – co jest bardzo ważne – otwarciem automatycznym otworów napowietrzających.

W zależności od zastosowanego rozwiązania zasada ich działania jest różna.

Instalacje pneumatyczne

Pneumatyczny system sterowania oddymianiem pracuje z wykorzystaniem energii kinetycznej CO_2, skupionej pod wysokim ciśnieniem w naboju. Klapy oddymiające w automatycznym systemie sterowania otwierają się za sprawą termowyzwalacza zamontowanego na podstawie lub zamocowanego na stelażu dolnym klapy. Termowyzwalacz został wyposażony w topikowy bezpiecznik, czyli nabój CO_2. Jego masa zależy od wielkości klapy. Bezpiecznik topikowy posiada mechanizm, który uwalnia iglicę przebijającą nabój.

W chwili wybuchu bezpiecznik topikowy powoduje otwarcie klap oddymiających. Do pęknięcia dochodzi w momencie, kiedy temperatura osiągnie 68–72°C (czerwony topik) lub 88–93°C (zielony topik) w starszych rozwiązaniach wyzwolenie następowało w momencie przetopienia spoiny łączącej dwie blaszki. Przy zbyt wysokiej temperaturze iglica termowyzwalacza przebija osłonę naboju CO_2 i wówczas dochodzi do uwolnienia gazu. Dwutlenek węgla, który wydostał się z naboju, przedostaje się przewodem instalacji pneumatycznej do siłownika znajdującego się pod klapą. W tym momencie ma miejsce wypchnięcie tłoczyska siłownika oraz jego zamknięcie na poziomie wysuniętym maksymalnie.

Sterowanie ręczne (manualne) w tym systemie jest oparte na dwóch systemach otwierania klap:

- system, w którym wypływ CO_2 z właściwych naboi następuje po ich przebiciu w skrzynce tzw. pilota – następuje wówczas wypływ gazu z jednej butli poprzez instalację pneumatyczną (przewody) przedostaje się do „właściwej" skrzynki. Tam znajduje się więcej naboi, dochodzi do uwolnienia dużej ilości gazu, który także instalacją pneumatyczną trafia do klap umieszczonych w przestrzeni oddymiania i otwiera je. Takie rozwiązanie umożliwia jednoczesne otwarcie dużej liczby klap w tym samym czasie;
- system, w którym nie ma skrzynki pośredniczącej, a uruchomienie klap następuje bezpośrednio ze skrzynki właściwej, wówczas również jest możliwe jednoczesne otwarcie jednej lub kilku klap.

Skrzynki sterujące mogą być opcjonalnie wyposażone w elektrozawór, który zostaje zasilony napięciem 24 V. Elektrozawór doprowadza do sprzężenia instalacji pneumatycznej z centralą sygnalizacji pożarowej. W tym momencie system oddymiania automatycznie zostaje uruchomiony, gdyż impuls elektryczny dotarł do skrzynki z CSP.

Instalacje mechaniczne

Spotyka się również rozwiązania, w których uruchomienie instalacji następuje w momencie przekroczenia temperatury w otoczeniu klapy i zadziałania elementu topikowego. Klapa jest uno-

szona do góry za pomocą siłowników pneumatycznych lub sprężynowych. W niektórych rozwiązaniach można też zastosować specjalny rygiel elektromagnetyczny do uruchomienia instalacji z systemu sygnalizacji pożarowej. Często jednak klapy są sterowane indywidualnie – w teorii oznacza to, że im większy pożar, tym więcej klap powinno się otworzyć, w praktyce bywa różnie.

Instalacje elektryczne

W momencie wykrycia produktów spalania przez czujki dymu lub przyrostu temperatury przez czujki temperatury, następuje ich pobudzenie. Sygnał alarmu dociera do centrali oddymiania, która za pośrednictwem siłowników steruje otwarciem okien lub klap oddymiających oraz napowietrzających. Jednocześnie sygnał może być przekazywany do centrali sygnalizacji pożarowej budynku (jeżeli taka jest w budynku) lub elementy detekcyjne i sterowanie pochodzi z systemu SSP. Uruchomienie systemu może też nastąpić poprzez wciśnięcie ręcznego przycisku oddymiania. Otwarcie klap jest sygnalizowane optycznie i akustycznie zazwyczaj w przyciskach alarmowych oddymiania lub za pomocą sygnalizatorów optyczno-akustycznych. Tego typu systemy mają też możliwość otwarcia klap w celu przewietrzenia pomieszczeń. Do tego celu służą specjalne przyciski przewietrzające, które umożliwiają ręczne otwarcie oraz zamknięcie klap i okien oddymiających. Dodatkowo w celu zabezpieczenia zarówno instalacji, jak i elementów budynku oraz materiałów w nim zgromadzonych stosuje się specjalne moduły pogodowe (*rys. 5*), które zapewniają automatyczne zamknięcie otworów przy silnym wietrze lub deszczu.

W kolejnym wydaniu „a&s Polska" opiszemy instalację zamknięć przeciwpożarowych oraz działanie ppoż. wyłączników prądu i oświetlenia awaryjnego.

BIO

mgr inż. Edward Skiepko
Rzeczoznawca ds. zabezpieczeń ppoż., rzeczoznawca NOT. Zajmuje się tematyką związaną z wymaganiami ochrony ppoż. oraz analizą zagrożeń wynikających z użytkowania urządzeń i instalacji elektrycznych.

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

SIS-FIRE

zabezpiecza ciągłość procesów technologicznych w obiekcie przemysłowym

Zapewnienie nieprzerwanego funkcjonowania obiektu przemysłowego – zarówno podczas jego codziennej eksploatacji, nadzorowania i sterowania pracą urządzeń technologicznych linii produkcyjnej, jak i reagowania w sytuacji zagrożenia (alarm pożarowy czy też dostanie się do obiektu osoby nieupoważnionej) – wymusza m.in. dobór odpowiednich systemów bezpieczeństwa i właściwy podział kompetencji pomiędzy nimi. Do tego celu można przyjąć podział na:

- system zarządzania i nadzorowania procesu technologicznego (SCADA) – najważniejszy z punktu widzenia utrzymania ciągłości produkcji,
- system integrujący urządzenia przeciwpożarowe (SIUP) oraz inne instalacje mające wpływ na bezpieczeństwo pożarowe (kryzysowe),
- system zarządzania bezpieczeństwem (*Security Management System* – SMS) – zarządza instalacjami SKD, CCTV, SSWiN itp.

Wprowadzenie takiego podziału pozwala na kontrolę funkcjonowania obiektu podczas jego normalnej eksploatacji, a także właściwą reakcję na pojawiające się zagrożenia. Podział kompetencji nie oznacza, że instalacje są od siebie niezależnie – celem nadrzędnym jest ich współdziałanie i przejmowanie roli wiodącej tego systemu, który w danej chwili jest najważniejszy dla zapewnienia bezpieczeństwa obiektu czy konkretnych procesów technologicznych.
Systemy integrujące urządzenia ppoż. ze względu na wspomnianą funkcję sterowania muszą przejść rygorystyczne badania atestacyjne przed wprowadzeniem do obrotu i użytkowania. Pomyślne ich zakończenie jest dokumentowane certyfikatem (od 1.01.2017 r. jest to krajowy certyfikat stałości właściwości użytkowych) oraz świadectwem dopuszczenia CNBOP-PIB potwierdzającym spełnienie wymagań dot. funkcji w zakresie np. centrali sterującej urządzeniami ppoż.

Przykładem systemu integrującego jest SIS-FIRE oferowany przez Schrack Seconet Polska. **Zintegrowany system zarządzania bezpieczeństwem pożarowym SIS-FIRE** jest stosowany do wizualizacji, sterowania i zarządzania urządzeniami ppoż., a także do integracji innych systemów mających wpływ na bezpieczeństwo pożarowe (kryzysowe) obiektu. Tworząc jedno, spójne, w pełni kompatybilne i kompleksowe narzędzie dozoru nad budynkiem, można zapewnić maksymalny poziom ochrony. SIS-FIRE powstał na bazie wieloletnich doświadczeń Schrack Seconet w zakresie produkcji systemów bezpieczeństwa pożarowego.
W jego skład wchodzą:

- platforma informatyczna do zarządzania bezpieczeństwem pożarowym SIS-FIRE/ SIS-FIRE Lite,
- centrala sygnalizacji pożarowej i sterowania urządzeniami ppoż. Integral IP MX, Integral IP CX, Integral IP BX wraz z modułami wejścia/wyjścia techniki X-LINE,
- sterowniki urządzeń technicznych i ppoż. SF-CONTROL (w różnych wersjach).

Podstawową zaletą systemu jest elastyczność, która umożliwia optymalny – dla konkretnego typu obiektu – dobór elemen-

tów i funkcji z zapewnieniem ścisłej współpracy i podziału kompetencji pomiędzy komponentami systemu. Redundancja komponentów bazujących na systemie Integral IP MX oraz (opcjonalnie) platformy informatycznej SIS-FIRE zapewnia ciągłość działania systemu również w przypadku wystąpienia awarii pojedynczych elementów całego układu.

Istotną cechą systemu integrującego (w przeciwieństwie do standardowego systemu sygnalizacji pożarowej) jest możliwość spełnienia nieograniczonej liczby zadań i funkcji logicznych związanych z obsługą, sterowaniem i nadzorowaniem zintegrowanych systemów w obiekcie. Elementy integratora są dowolnie programowalne i realizują funkcje bezpieczeństwa zgodnie ze scenariuszem pożarowym i przyjętymi założeniami, współpracując bezpośrednio z redundantnym systemem sygnalizacji pożarowej Integral IP. Ma to kluczowe znaczenie dla realizowanych projektów, SIS-FIRE umożliwia bowiem wykorzystanie central Integral IP oraz modułów pętlowych wejścia/wyjścia do sterowania i nadzorowania urządzeniami ppoż.
SIS-FIRE może obsługiwać wiele stanowisk operatorskich systemu, pozwalając na równoległy nadzór i obsługę przez wielu operatorów – ma to znaczenie w przypadku lokalnego wspierania operatora przez niezależne procedury postępowania. Ponadto może zostać wykorzystany do centralnego zarządzania niezależnymi systemami bezpieczeństwa pożarowego w obiektach rozproszonych. Integrator umożliwia wirtualne sieciowanie obiektów, co znacznie usprawnia centralny nadzór i wpływa na obniżenie kosztów obsługi i serwisu instalacji bezpieczeństwa.

Interfejs użytkownika zapewnia intuicyjną obsługę systemu przez operatora. Czytelny podział bloków funkcyjnych oprogramowania ułatwia realizację zadań związanych z nadzorem zintegrowanych systemów podczas normalnej eksploatacji, w przypadku alarmu pożarowego lub awarii. Stacja operatorska wskazuje stan alarmu lub uszkodzenia oraz inne wymagające reakcji stany niebezpieczne. W celu optymalizacji procedur obsługi nadzorowanych systemów stosuje się specjalne procedury wspomagające służby dozoru technicznego. Instrukcje powinny zawierać szczegółowe kroki postępowania dla operatora, z uporządkowanymi informacjami dot. ewakuacji osób z zagrożonego miejsca i ochrony (zabezpieczenia) procesów technologicznych obiektu (warunki decyzji o wyłączeniu produkcji lub przełączeniu zadań np. do zapasowych centrów produkcji lub działu przetwarzania danych). Istnieje też możliwość nadzorowania procedur sterowania urządzeniami ppoż. w odniesieniu do matrycy sterowań wynikających ze scenariusza pożarowego. Pozwala to na potwierdzenie skuteczności wykonanych sterowań i wskazanie niezgodnych z procedurą stanów urządzeń.
Dla ułatwienia lokalizacji pożaru i wskazania obszaru działania systemów detekcji (np. czujki zasysające dymu) czy też wizualizowania obszaru zadziałania urządzeń ppoż. (np. instalacji tryskaczowych) można wykorzystać graficzne mapy obszarów nadzorowanych (pola aktywności lub nadzoru), które pokazują, jaki obszar jest objęty jednocześnie zagrożeniem pożarowym i oddziaływaniem urządzeń zabezpieczających. Ma to szczególne znaczenie w przypadku konieczności dokonania szybkiej oceny ryzyka konkretnego zdarzenia.

W celu realizacji funkcji ochrony pożarowej system integrujący współpracuje z innymi instalacjami zabezpieczeń, jak SKD czy CCTV. Integracja SIUP z CCTV zapewnia wyświetlanie obrazu z kamery powiązanej z alarmującym elementem i przyspieszenie weryfikacji zagrożenia. Integracja z system KD pozwala natomiast na przesyłanie informacji potwierdzających drożność przejść ewakuacyjnych oraz przedstawienie raportu informującego o liczbie osób, które zostały bezpiecznie ewakuowane z obiektu lub nadal mogą przebywać w miejscu zagrożenia – to istotne dla prowadzącego akcję ratowniczo-gaśniczą.

> Należy pamiętać o zapewnieniu odpowiedniej koordynacji międzybranżowej na wszystkich etapach projektu, począwszy od etapu budowania koncepcji bezpieczeństwa, poprzez wykonanie projektu, skończywszy na uruchomieniu systemu i przeszkoleniu użytkowników.

Graficzny interfejs użytkownika umożliwia wprowadzenie do systemu i powiązanie z wizualizowanymi elementami wielu informacji dodatkowych, takich jak karty katalogowe urządzeń, dokumentacje techniczno-ruchowe, instrukcje serwisowe, schematy podłączenia i inne instrukcje ułatwiające obsługę urządzeń. Dzięki temu zarówno podczas codziennej eksploatacji oraz obsługi systemu, jak i w przypadku alarmu lub uszkodzenia operator ma dostęp do najważniejszych informacji. SIS-FIRE jest projektowany tak, by wskazywać najważniejsze stany pracy z nadzorowanych systemów i urządzeń przeciwpożarowych, takich jak alarm czy uszkodzenie, ale umożliwia też wskazywanie zmiennych typu ciągłego (wartości temperatury, poziom stężenia tlenku węgla czy inne dane odzwierciedlające np. stany procesów technologicznych produkcji), ważne m.in. dla zarządzania kryzysowego. Dzięki integracji cyfrowej SIS-FIRE z czujką liniową ciepła Listec istnieje możliwość wskazywania aktualnej temperatury w chronionym obszarze lub monitorowanie np. temperatury obudowy zabezpieczanego urządzenia produkcyjnego czy elementów ciernych linii technologicznej, co z kolei zapewnia wczesną reakcję operatora w przypadku zagrożenia.

Zastosowanie certyfikowanego systemu integrującego urządzenia ppoż. i inne instalacje techniczne mające wpływ na prawidłowe funkcjonowanie obiektu znacznie podnosi poziom bezpieczeństwa ludzi i mienia, a także umożliwia optymalną reakcję zabezpieczeń automatycznych i działań obsługi w przypadku konieczności ochrony procesu produkcji. Operatorzy, mając do dyspozycji system zapewniający pełny przegląd sytuacji oraz podpowiedzi w formie procedur postępowania, mogą szybko zareagować na zagrożenie i wykonać niezbędne czynności minimalizujące skutki pożaru.

Głos branży

Zapewnienie bezpieczeństwa w obiektach przemysłowych to proces bardzo złożony i wielowymiarowy. Równie istotna, jak utrzymanie ciągłości działania zakładu, jest tu dbałość o bezpieczeństwo ludzi pracujących w warunkach niebezpiecznych. Nie bez znaczenia jest także ochrona mienia.

Linc Polska dba o bezpieczeństwo techniczne i cybernetyczne

Jakub Sobek
certyfikowany trener techniczny, Linc Polska

Odpowiedni stopień zabezpieczenia obiektu przemysłowego jest gwarancją nie tylko jego bezpieczeństwa, ale także stabilności funkcjonowania i odporności na różnego rodzaju ataki lub awarie. Architektura systemu zabezpieczeń jest istotna w dwóch kluczowych obszarach: bezpieczeństwa fizycznego i wirtualnego.

Ataki cybernetyczne z roku na rok zyskują na sile. W czerwcu hakerzy włamali się do elektrowni atomowej w USA. Co prawda zdarzenie to dotyczyło części biznesowej, jednak pokazało, że sieci w takich obiektach są infiltrowane i narażone na włamania. Często mniejsze ataki mają na celu uzyskanie dodatkowych informacji, rozpoznanie mechanizmów zabezpieczeń czy metod detekcji zagrożeń sieciowych. Wiedza ta jest przydatna przy planowaniu większych uderzeń, które mogą zostać skierowane na elementy infrastruktury obiektu.

Pod koniec grudnia ub.r. został przeprowadzony celowy atak cybernetyczny na ukraińskie przedsiębiorstwa z sektora energetycznego. Efektem tych działań były kilkugodzinne przerwy w dostawie prądu dla prawie miliona mieszkańców. Atak został przeprowadzony z użyciem złośliwego oprogramowania przesyłanego pracownikom za pośrednictwem poczty elektronicznej.
Do historii przejdzie także użycie robaka Stuxnet, który miał zdestabilizować działanie sterowników PLC zainstalowanych w obiektach przemysłowych. Wielu specjalistów analizujących ten atak potwierdziło, że głównym jego celem były wirówki do wzbogacania uranu wykorzystywane przez Iran.

W obszarze zabezpieczeń technicznych rozległych obiektów przemysłowych istotne jest stworzenie skutecznego systemu ochrony perymetrycznej. W takich obiektach mamy zazwyczaj do czynienia z linią ogrodzenia o długości kilkunastu lub nawet kilkudziesięciu kilometrów, należy zatem wybierać rozwiązania przystosowane do takich odległości.
Złym pomysłem jest korzystanie z kamer światła widzialnego i analityki wideo jako podstawowego systemu detekcji – kamery musiałyby być instalowane co ok. 50 m. W przypadku rozległych obiektów dałoby to sumarycznie ogromną ich liczbę, wymagającą obsługi, serwisowania i napraw (większa liczba elementów to większa awaryjność).
Od strony technologicznej rozwiązaniem wiodącym w tego typu projektach są światłowodowe systemy ochrony perymetrycznej. Przewód światłowodowy może być prowadzony zarówno w gruncie, jak i na ogrodzeniu, a w miejscu centralnym instaluje się jedynie kontroler. System ten pozwala na detekcję przechodzenia, przebiegania czy kopania w pobliżu chronionego terenu. Nawet w przypadku przecięcia światłowodu nadal działa prawidłowo. Szczególnie istotną cechą jest też możliwość precyzyjnej detekcji intruza z informacją, gdzie nastąpiło przekroczenie strefy. Można wtedy automatycznie skierować tam kamerę (np. termowizyjną) w celu weryfikacji wizyjnej. Tak zbudowane systemy często są wspierane radarami krótkiego lub dalekiego zasięgu. To kolejne rozwiązanie technologiczne, które w ostatnich latach zyskało na popularności, a postępujący spadek cen tego typu produktów sprawi, że wkrótce staną się one integralnym elementem wielu systemów.

Myśląc o bezpieczeństwie obiektów przemysłowych, trzeba pamiętać o dwóch aspektach ich ochrony: fizycznej i cybernetycznej. Tylko całościowo przygotowana koncepcja zabezpieczenia danego obiektu może zapewnić właściwy poziom jego ochrony.

Ochrona obiektów przemysłowych z wykorzystaniem kamer sieciowych Axis

W obiektach przemysłowych kamera jest jednym z istotnych elementów zapewniających bezpieczeństwo pracowników i infrastruktury, wspierających ochronę przed wtargnięciem, kradzieżami lub wandalizmem. Środki ochrony obwodowej to zwykle urządzenia typu radar bliskiego zasięgu, lasery lub kable sensoryczne zakopywane pod ziemią czy montowane na ogrodzeniach, sygnalizujące ruch. Chociaż wszystkie spełniają swoją funkcję, mają oczywiste ograniczenia: nie pozwalają odróżnić alarmów rzeczywistych od fałszywych, a ponadto podają jedynie ograniczony zakres informacji. Dlatego firmy coraz częściej sięgają po kamery sieciowe, by wsparły ochronę obwodową. Zastosowanie kamer termowizyjnych jako czujek ruchu oraz kamer wysokiej rozdzielczości do weryfikacji zdarzenia pozwala uzyskać ważne informacje wizualne o przyczynie wyzwolenia alarmu i rodzaju aktywności bez generowania fałszywych alarmów.

W połączeniu z tradycyjnymi technologiami kamery sieciowe tworzą bardziej inteligentny i niezawodny sieciowy system dozorowy. Dzięki ogromnej różnorodności kamer dostępnych na rynku można precyzyjnie dobrać urządzenia do wymagań i oczekiwań. Nawet w trudnych warunkach atmosferycznych czy oświetleniowych wyraźny i klarowny obraz na żywo i z nagrania ułatwi wykrycie i zidentyfikowanie obiektów, osób oraz incydentów. Zautomatyzowane rozwiązania oraz oprogramowanie do analizy treści obrazu pozwolą zredukować konieczne interwencje człowieka, jak również liczebność personelu ochrony.

Pracujące równolegle dwa rodzaje kamer tworzą niezwykle skuteczny i precyzyjny mechanizm ochronny. W celu zapewnienia nieprzerwanego zapisu i maksymalnej funkcjonalności każda kamera pracuje niezależnie i umożliwia dostarczanie informacji podczas pracy w sieci IP. W przypadku awarii łącza sieciowego urządzenia mogą zapisywać dane na wbudowanej karcie SD na potrzeby ewentualnej przyszłej analizy.

Andrea Sorri,
dyrektor Business Development Government, City Surveillance and Critical Infrastructure, Axis Communications

Hikvision o termowizji, dronach i funkcjach inteligentnych

Bezpieczeństwo obiektów przemysłowych stanowi kluczowy element funkcjonowania przedsiębiorstwa. W przypadku każdego z nich bardzo ważną rolę odgrywa ochrona obwodowa, często wielopoziomowa: wysoki płot, elementy systemu alarmowego (czujki i bariery) oraz kamery. Przy tego typu zadaniach często niezastąpione są kamery bispektralne. Integracja w jednej obudowie kamery termowizyjnej i kamery wysokiej rozdzielczości pracującej w paśmie widzialnym pozwala na pełną identyfikację zdarzeń. Dzięki funkcjom VCA analizującym obraz termiczny można zredukować liczbę fałszywych alarmów docierających do operatorów.

Należy też zwracać uwagę na zagrożenia wewnętrzne, takie jak ignorancja personelu, sabotaż lub działanie pod silnym stresem w wyniku różnych zdarzeń, np. przestępstwo czy atak terrorystyczny. Aby złagodzić skutki lub (jeśli to możliwe) wyeliminować takie zdarzenia, personel powinien być odpowiednio przeszkolony. Polityka bezpieczeństwa, standardy i procedury operacyjne, jasno określające zasady i zadania dla wszystkich pracowników i gości, powinny być rygorystycznie przestrzegane.

Aby zabezpieczyć ciągłość działania zakładu przemysłowego, newralgiczne punkty są stale poddawane kontroli i konserwacji. Do tego celu idealnie nadają się drony wyposażone w kamerę termowizyjną lub kamerę PTZ o wysokiej rozdzielczości szybko dokonujące inspekcji. Pomagają w natychmiastowej ocenie sytuacji i podjęciu niezbędnych działań, ograniczając w ten sposób koszty i ryzyko wystąpienia zdarzeń niepożądanych.

Pomysłów na zastosowanie dronów w systemach zabezpieczeń może być znacznie więcej. Hamulcem jest system prawny, który nie nadąża za rozwojem technologii. Kamery megapikselowe, kamery termowizyjne, kamery Ex, a nawet drony są urządzeniami pracującymi z wykorzystaniem bezpiecznej transmisji danych w sieciach teleinformatycznych. Kluczowe jest nie tylko scalenie ich w jeden system, ale także tworzenie redundantnych centrów zarządzania bezpieczeństwem dużych obszarów. Wielozadaniowość systemu oraz możliwość centralizacji procesu obserwacji i wykrywania zagrożeń zarówno podnosi standardy bezpieczeństwa, jak i skutecznie redukuje koszty związane z działalnością obiektów przemysłowych.

Łukasz Lik
dyrektor ds. technicznych, Hikvision Poland

Dahua: profesjonalny monitor do telewizji dozorowej jest niezastąpiony

Czym się różni telewizor od monitora? Na pierwszy rzut oka oba urządzenia wyglądają tak samo, mają ekran, przyłącza audio i wideo, przyłącze zasilania. Oba są zamknięte w ładnej obudowie i wyświetlają wcześniej zdefiniowany obraz. I tu można by zakończyć dyskusję, ale czy na pewno? Telewizor jest wyposażony w dodatkowy układ elektroniczny, czyli tuner telewizyjny umożliwiający odbiór telewizji naziemnej lub satelitarnej, w zależności od zastosowanego tunera. Zazwyczaj cena telewizora proponowana przez sieci handlowe również jest „atrakcyjniejsza". Wybór wydaje się prosty, preferujemy telewizor konsumencki… To duży błąd.
Użycie ekranu konsumenckiego w systemie telewizji dozorowej, która wymaga zastosowania urządzeń profesjonalnych, może przysporzyć wiele problemów. Profesjonalne monitory do CCTV nie mają tunera telewizyjnego, więc nie wymagają opłaty za abonament telewizyjny. Standardowa gwarancja na urządzenia konsumenckie wynosi 24 miesiące, w przypadku monitorów jest to 36 miesięcy. Monitory są zazwyczaj wyposażone w matrycę o zwiększonej żywotności i mogą pracować 24 godz./7 dni w tygodniu, w przypadku standardowego telewizora jest to tylko 5–8 godz. dziennie. Podświetlenie matrycy monitora czy telewizora ulega z czasem gradacji, dlatego matryce w monitorach mają zwiększoną jasność, dzięki czemu można dostosować jego jasność do tych samych parametrów przez kilka lat użytkowania. Na przykład monitor o jasności 500–700 cd/m^2 (nit) w ciągu 5 lat działania może utracić nawet 50% jasności, dlatego pracuje zazwyczaj na poziomie 200–300 cd/m^2 (nit), nie męcząc wzroku operatora, i pozwala na utrzymanie jasności na tym poziomie do końca żywotności urządzenia.
Jeśli nadal myślimy o zastosowaniu telewizora konsumenckiego w profesjonalnych systemach, zastanówmy się dwa razy, czy kupując produkt konsumencki, nie przepłacamy, a ta oszczędność przy zakupie nie okaże się początkiem do zwiększenia kosztów operacyjnych w dłuższym okresie. Dahua w swojej linii produktowej posiada monitory do każdego typu zastosowań – od monitorów do tworzenia ścian wizyjnych (*Splicing Screen*), poprzez urządzenia o zwiększonej jasności i do zastosowań specjalnych (*High Protective Series* oraz 4K), po urządzenia z serii LITE, które zapewniają pracę 24 godz./7 dni w tygodniu i wysokiej jakości obraz bez obaw o dodatkowe opłaty abonamentowe. Przemysłową jakość panelu urządzenia potwierdza 36-miesięczna gwarancja.

Paweł Obrzud
Business Development Manager,
Dahua Technology Poland

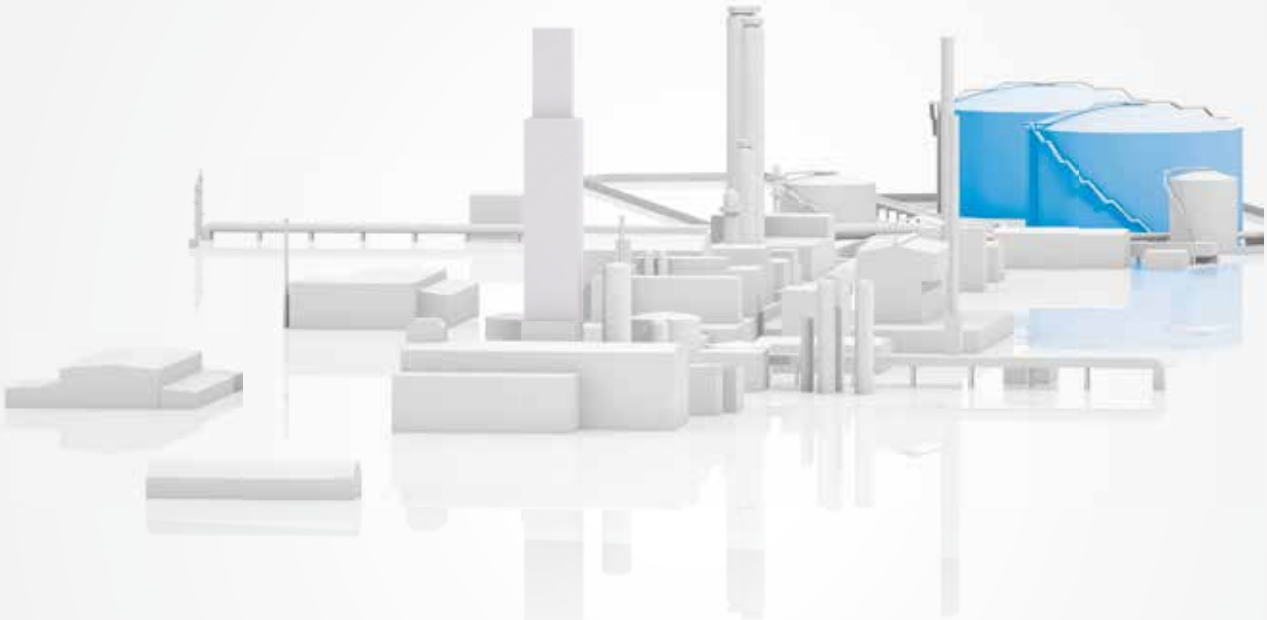
Schrack Seconet rekomenduje certyfikowany system integrujący

Grzegorz Ćwiek
prezes,
Schrack Seconet Polska

W przypadku obiektu przemysłowego najwyższym priorytetem jest zapewnienie bezpieczeństwa procesu produkcji. Dlatego też podczas codziennej eksploatacji rolę nadrzędną nad innymi systemami odgrywa system SCADA. Sytuacja się zmienia w momencie wystąpienia zdarzenia nagłego, o charakterze kryzysowym, np. alarmu pożarowego – wówczas rolę wiodącą w stosunku do innych systemów i instalacji w obiekcie przejmuje system sygnalizacji pożarowej, uzupełniony o system integrujący urządzenia przeciwpożarowe (SIUP). Należy jednak pamiętać, że w obiekcie przemysłowym ważna jest selektywność działania i jak najbardziej przemyślana ocena poziomu zagrożenia ludzi oraz mienia. Należy bowiem niezwykle ostrożnie podejmować decyzję o ewentualnym wyłączeniu urządzeń technologicznych i zatrzymaniu produkcji (co bywa bardzo kosztowne). Najczęściej jest to ostateczność w sytuacji, gdy alarm pożarowy został potwierdzony i nie ma innej możliwości rozwiązania problemu. Zastosowanie certyfikowanego systemu integrującego urządzenia przeciwpożarowe umożliwia nie tylko szczegółowe nadzorowanie (wizualizację) stanów pracy urządzeń ppoż., ale również ich obsługę i sterowanie ręczne wieloma funkcjami, a więc wprowadza możliwość korekty użycia procedur automatycznych, co ma kluczowe znaczenie w zestawieniu ze „zwyczajnie" działającym systemem sygnalizacji i wizualizacji zdarzeń.
Systemy bezpieczeństwa pracujące na tak wysokim poziomie integracji wymagają dobrze przeszkolonego personelu, który będzie potrafił wykorzystać wszystkie zalety takiego rozwiązania. Zastosowane w systemie automatyczne procedury z powodzeniem spełnią nawet najtrudniejsze wymagania użytkownika i ubezpieczyciela oraz przyniosą wymierne korzyści właścicielowi obiektu, jednak największą wartość mają one wtedy, gdy zakres ich pracy oraz działania w sytuacji awaryjnej będzie wykorzystany optymalnie przez dobrze przygotowaną do tego celu obsługę.

a&S POLSKA

ŚNIADANIE EKSPERTÓW



Bezpieczeństwo obiektów przemysłowych

dyskusja o bezpieczeństwie w luźnej atmosferze

ZAPRASZAMY:

- security managerów w obiektach przemysłowych
- specjalistów ds. bezpieczeństwa w zakładach wytwórczych
- specjalistów z zakresu kontroli jakości w produkcji
- osoby zainteresowane tematem spotkania

10 listopada 2017 r.
godz. 9.00–12.00
Hotel Westin Warszawa

Uczestnictwo w śniadaniu jest **bezpłatne!**

Rejestracja: www.aspolska.pl/sniadanie

organizator:

a&S POLSKA

partnerzy:

AXIS COMMUNICATIONS

alhua TECHNOLOGY

Hanwha Techwin

HIKVISION

Linc Polska Sp. z o.o.

SASMA

SCHRACK SECONET

Magia WYSOKICH ROZDZIELCZOŚCI

Czytelny i użyteczny obraz nie wynika tylko z większej liczby pikseli na przetworniku – wiedzą o tym uczestnicy prowadzonych przeze mnie kursów. Im dalej w rozdzielczość, tym więcej problemów, trudnych do rozwiązania na poziomie instalacji bez specjalistycznej wiedzy, narzędzi i technologii. Rozdzielczość full HD jest obecnie standardem, punktem odniesienia wielkości obrazu (kilka lat temu był nim format 4CIF). **Postęp technologiczny o funkcji wykładniczej każe twierdzić, że już w roku 2020 rozdzielczość 2160p (znana jako 4K) zastąpi 1080p (full HD). Spowoduje to kolejne zmiany w branży telewizji dozorowej. A ta jest bez wątpienia najszybciej rozwijającym się działem elektronicznych systemów zabezpieczeń.**

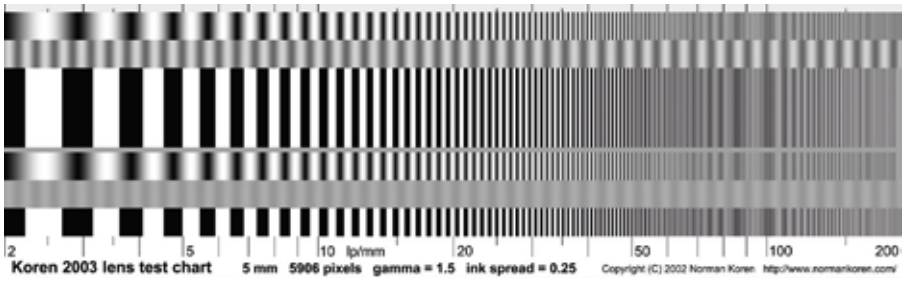
Jan T. Grusznic

Od wielu lat obserwujemy wyraźny wpływ zmian dokonujących się na rynku konsumenckich dóbr elektronicznych na rozwiązania proponowane przez producentów elementów systemów telewizji dozorowej. Pojawiły się w naszej branży produkty ze świata fotografii, kamer sportowych czy urządzeń mobilnych, głównie smartfonów. Wielu producentów tych urządzeń przeniosło ciężar przekazu reklamowego z rozdzielczości na elementy optyczne, takie jak stabilizacja optyczna, skuteczniejsze i szybsze ogniskowanie, zwiększona poklatkowość (zapewniająca uzyskanie efektu spowolnienia – *slow motion*) czy krótka głębia ostrości (tryb portretowy). Optyka stała się języczkiem u wagi nie tylko dla producentów dóbr konsumenckich, ale również producentów sprzętu profesjonalnego do pracy ciągłej przeznaczonego do przechwytywania obrazu.

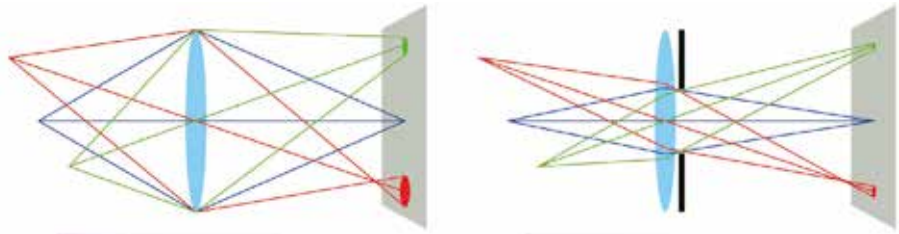
Waga optyki

Czytelny, szczegółowy obraz to wynik zgrania przede wszystkim dwóch elementów: układu optycznego i przetwornika obrazu. Okazuje się, że uzyskanie idealnego dopasowania nie jest takie proste, jak by się to wydawało na pierwszy rzut oka. Zwłaszcza dla wyższych roz-

RYS. 1. PRZYKŁAD EFEKTU MORY
źródło: www.visualabode.com.au



RYS. 2. PRZYKŁAD PLANSZY TESTOWEJ KOREN 2003 O SKALI OD 2 DO 200 LP/MM
źródło: www.normankoren.com



RYS. 3. SKUTEK ZAMKNIĘCIA PRZYSŁONY. PO LEWEJ – WYKORZYSTANA CAŁA SOCZEWKA, PO PRAWEJ – Z POWODU ZAMKNIĘCIA PRZYSŁONY TYLKO JEJ ŚRODKOWA CZĘŚĆ
źródło: materiały szkoleniowe Axis Communications

dzielczości. Ileż to razy do kamery 5-megapikselowej wkręcałeś obiektyw 5-megapikselowy, a obraz był daleki od ideału? Trochę bez ostrości (bo nawet z automatycznym i bardzo pomocnym asystentem ustawiania pozycji przetwornika nie udało jej się nigdzie w obrazie znaleźć), na dodatek z aberracją sferyczną i jeszcze mało kontrastowy. Opisane przeze mnie efekty są związane właśnie z nieprawidłowym dopasowaniem optyki do przetwornika kamery, a konkretnie – z punktem ogniskowania, który jest większy niż płaszczyzna pojedynczego piksela matrycy światłoczułej, przez co naświetla sąsiednie piksele. W rezultacie obserwujemy zmniejszenie czytelności detali w obrazie – rozdzielczość optyczna ulega degradacji. Jednocześnie gdy punkt ogniskowania jest mniejszy niż piksel, na obrazie będą widoczne błędy w postaci różnokolorowych fal interferujących ze sobą (*rys. 1*).
Efekt ten, zwany *morą*, jest dość często widziany na obrazach z kamer dostarczających sygnał analogowy Pojawia się, gdy rozdzielczość układu optycznego jest większa niż rozdzielczość przetwornika kamery. Można go zredukować lub pozbyć się całkowicie dzięki zastosowaniu filtrów dolnoprzepustowych, które powodują efekt lekkiego rozmycia i delikatną redukcję kontrastu. Redukcję efektu mory umożliwia również delikatne „rozostrzenie", tj. zgubienie ostrości.

Niestety w przypadku zastosowania obiektywu o mniejszej zdolności rozdzielczej niż wymaga tego przetwornik, obraz będzie miał gorszą czytelność detali. Teoretycznie można elektronicznie „doostrzać" obraz za pomocą odpowiednich filtrów cyfrowych, jednak efekt jest na ogół daleki od satysfakcjonującego.
Ponieważ niemal od dekady na rynku telewizji dozorowej obserwujemy erozję jakości podawanych danych (niekoniecznie wynikających ze złych intencji producentów, raczej z braku odpowiedniego unormowania wykonywanych badań), problem ten w końcu dotknął również deklarowanych rozdzielczości obiektywów. Na rynku są dostępne obiektywy megapikselowe: 5-Mpix, 3-Mpix lub full HD lub 4K. Tymczasem podłączenie wyraźnie dookreślonej optyki do kamery o „takiej samej" rozdzielczości daje często tak różne efekty, które obserwujemy na wynikowym obrazie. Skąd brak powtarzalności, skoro wartości się zgadzają? Powodem jest właśnie brak zgrania tych dwóch elementów.
Zacznijmy od powodu najprostszego: rozdzielczości obiektywów nie mierzy się w pikselach, ale w parach linii przypadających na 1 mm [lp/mm]. Rozdzielczość 180 lp/mm oznacza, że na 1 mm można dojrzeć 360 linii czarnych i białych ułożonych naprzemiennie. Na *rys. 2* pokazano przykładową planszę testową, za pomocą której testuje się rozdzielczość elementów optycznych (z powodu ograniczeń rozdzielczości wydruku część linii jest widoczna jako szary fragment). Rozdzielczość obiektywu *y* [lp/mm] dla przetwornika 1/2,5" o rozdzielczości 4K będzie wynosić ok. 308 lp/mm zgodnie ze wzorem:

$$\mathbf{y}\,[\mathrm{lp/mm}] = \frac{\dfrac{1[\mathrm{mm}]}{\text{wielkość piksela [mm]}}}{2}$$

Zakładając, że wielkość piksela dla przetwornika 1/2,5" o rozdzielczości 4K wyno-

si typowo 1,62 µm (UWAGA: warto tę wartość zweryfikować w karcie katalogowej producenta przetwornika) oraz ujednolicając jednostki 1,62 µm = 0,00162 mm (1 mm = 1000 µm), otrzymamy:

$$y = \frac{\frac{1mm}{0{,}00162\ mm}}{2} = 308{,}642\ lp/mm$$

Gdyby wielkość przetwornika była większa, tzn. piksel byłby większy i miał np. 4,09 µm, wtedy rozdzielczość obiektywu nie musiałaby przekraczać 122 lp/mm. Zatem dla większego piksela na przetworniku potrzebny jest obiektyw o mniejszej zdolności rozdzielczej. Należy przy tym zauważyć, że wyliczona wartość odnosi się do każdego punktu optyki. Niestety ze względu na obecne ograniczenia technologiczne na etapie produkcji zdolność rozdzielcza soczewek różni się między środkiem a sferą obiektywu. Dla przykładu firma Kowa, jako jeden z nielicznych producentów, dla obiektywu 1/2" LMVZ3510M-IR deklaruje rozdzielczość w środku optyki 200 lp/mm, zaś w rogu kadru 120 lp/mm. W jej karcie katalogowej ujęto również dopasowanie do wielkości piksela o wielkości 2,5 µm (przy czym wielkość plamki dla 120 lp/mm będzie wynosić ~4 µm). Teoretycznie oznacza to, że obiektyw nadaje się do kamer aż 5 Mpix, natomiast należy się spodziewać widocznego efektu rozmycia ostrości w rogach kadru. Efekt ten można próbować zredukować przez zamknięcie przysłony, aby ograniczyć przenikanie promieni tylko do środkowej części soczewki, co pokazano na *rys. 3*.

Niestety przy dużych rozdzielczościach pojawia się problem z efektem dyfrakcji, której moment ujawnienia w dużym stopniu zależy od wielkości piksela. Im mniejszy piksel, tym szybciej. Dyfrakcja, czyli ugięcie fali na krawędzi przeszkody – w omawianym przypadku w środowisku optycznym – ma wpływ na wielkość tzw. plamki Airy'ego, zwanej również krążkiem dyfrakcyjnym. Ostry, czytelny obraz powstaje wtedy, gdy plamka Airy'ego jest wielkości pojedynczego piksela. Im jest ona większa, tym mniej czytelny staje się obraz, co można zaobserwować na *rys. 4.*

Wielkość plamki Airy'ego można wyliczyć z uproszczonego wzoru $X = 1{,}22 \times \lambda \times F$ (gdzie X – wielkość plamki, λ – długość fali świetlnej, F – otwór przysłony), przy założeniu, że:

- przysłona ma kształt idealnego koła,
- obiektyw jest pozbawiony wszelkich wad optycznych (obliczenia są wykonywane dla obiektywu idealnego).

W przypadku kamery 2160p, dla której szacuje się, że pojedynczy piksel ma ok. 1,62 µm (dla przetwornika ~1/2.5") przysłona ograniczona dyfrakcją ma wartość F2.0. Natomiast zamknięcie przysłony do wartości F4.0 spowoduje dwukrotną stratę rozdzielczości obrazu. Oznacza to, że przy tej wartości przy-

Czytelny, szczegółowy obraz to wynik zgrania przede wszystkim dwóch elementów: układu optycznego i przetwornika obrazu. Uzyskanie idealnego dopasowania nie jest takie proste, jak by się to wydawało na pierwszy rzut oka. Zwłaszcza dla wyższych rozdzielczości.

RYS. 4. CZYTELNOŚĆ DETALI W OBRAZIE W ZALEŻNOŚCI OD WIELKOŚCI KRĄŻKA DYFRAKCYJNEGO

⇓ *Plamka Airy'ego wielkości jednego piksela przetwornika*

⇓ *Plamka Airy'ego pokrywająca kilka pikseli przetwornika*

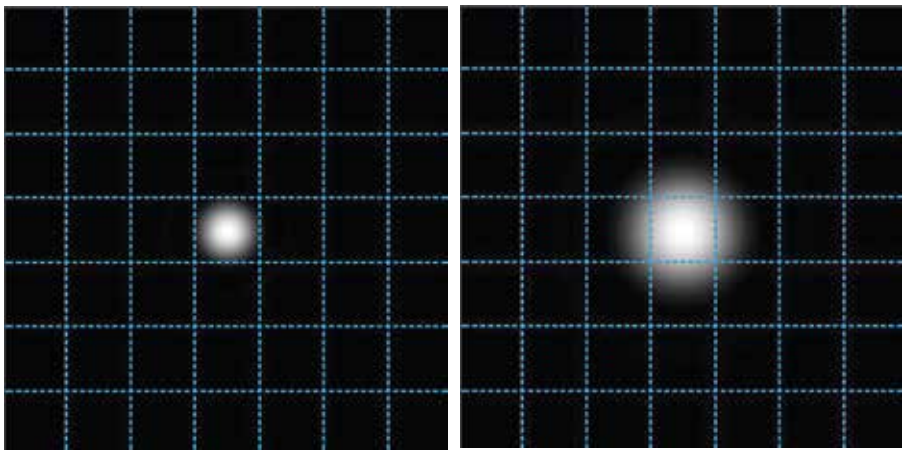
słony jeden punkt światła jest odbierany przez otaczające piksele matrycy (*rys. 5*).

Producenci kamer zauważyli istotę problemu już jakiś czas temu. W efekcie podjętych działań opracowano odpowiednie algorytmy i mechanizmy sterujące przysłoną. Przykładem może być opracowanie w 2009 r. przez firmę Kowa, we współpracy z Axis Communications, obiektywów z automatyką P-iris. Mechanizm jest oparty na silniku krokowym, a każdy krok oznacza konkretną wartość przysłony. Ponieważ nie istnieją standardy co do liczby kroków i przypisania doń konkretnych wartości F, każdy typ obiektywów wyposażonych w mechanizm P-iris będzie się różnił tymi wartościami między sobą. Stąd producenci tworzą pliki, które są swoistymi sterownikami. Po ich wgraniu do kamery ta porównuje wartości wielkości piksela (na ogół podane w oprogramowaniu układowym) z danymi zawartymi w pliku i określa optymalny poziom zamknięcia przysłony, który zapewnia maksymalną głębię ostrości, przy jednoczesnym utrzymaniu wysokiego kontrastu i czytelności szczegółów. Możliwość ustawienia precyzyjnie przysłony daje bardzo wymierne korzyści. Przede wszystkim wraz z zamykaniem przysłony zwiększa się głębia ostrości, czyli zakres obszaru na obrazie, który jest ostry. Zamknięcie przysłony pomaga również w usunięciu błędów optycznych, jakimi bez wątpienia jest aberracja sferyczna powodująca niewyraźny obraz na brzegach kadru.

Pojawienie się kamer wysokich rozdzielczości, które zmusiły do uznania wagi optyki w tworzeniu wysoko jakościowych obrazów i wykorzystania nowych standardów kompresji, to dopiero początek fascynujących zmian w CCTV.

Z drugiej strony P-iris zabezpiecza przed zbytnim domknięciem lamelek przysłony i obniżeniem szczegółowości obrazu przez uwidocznienie się efektu dyfrakcji właśnie. Co ciekawe, technologia ta nie została opatentowana, co pozwala wykorzystać to rozwiązanie przez wszystkie firmy producenckie.
Podobnie ma się sprawa z technologią i-CS, rozwiązaniem opracowanym również przez Axis, ale z firmą Computar. i-CS obok wykorzystania technologii precyzyjnego sterowania przysłoną P-iris zapewnia również zdalne sterowanie zakresem ogniskowych oraz ostrością. Zdalne ustawianie soczewek to nie luksus, tylko potrzeba. Już dla rozdzielczości full HD ręczne ustawianie ostrości jest męczące – dla rozdzielczości 4K to istny koszmar. i-CS jest rozwiązaniem dla obiektywów przeznaczonych do wszystkich kamer z montażem CS i obsługujących ten standard.

RYS. 5. ILUSTRACJA ZWIĘKSZONEJ PLAMKI AIRY'EGO NA SKUTEK ZAMKNIĘCIA PRZYSŁONY
Każdy z mniejszych kwadratów na obu rysunkach odpowiada wielkości piksela o długości boku 1,62 µm. Średnica wielkości plamki Airy'ego dla przysłony F2.0 (po lewej stronie) dla długości fali 650 nm wynosi 1,58 µm. Wielkość plamki dla przysłony F 4.0 (po prawej) wynosi 3,17 µm. Widoczne jest naświetlenie sąsiednich pikseli.



Ratunek we Fresnelu

Obecnie wybór modeli obiektywów oraz kamer zgodnych ze standardem UHD jest ograniczony (producent oferuje tylko kilka modeli). Niemniej sytuacja wydaje się rozwojowa, bowiem powoli wprowadzane są nowe przetworniki o większej dynamice i większej czułości. Wraz z nimi pojawiają się również obiektywy o rozdzielczościach zbliżonych do przykładowych ok. 308 lp/mm oraz tworzących plamkę Airy'ego dopasowaną do wielkości piksela (~1,62 µm). Dalsze zwiększanie rozdzielczości kamer będzie wymagać albo zwiększenia wielkości przetworników, a co za tym idzie rozmiarów pojedynczego piksela, albo zmiany koncepcji budowy obiektywów. Obecne obiektywy wykorzystują zjawisko załamania światła przez soczewki (skupiające lub rozpraszające), które wykonuje się ze specjalnych gatunków szkła lub innych przezroczystych materiałów (np. kwarcu, fluorytu lub plastiku). Łącząc kilka soczewek o odpowiednio dobranej krzywiźnie i współczynnikach załamania, można zbudować obiektyw dający wyraźny i pozbawiony zniekształceń obraz. Jednak obraz pochodzący z układu zwykłych soczewek refrakcyjnych traci z powodu znacznej aberracji chromatycznej (związanej z rozszczepieniem światła). Współczynnik załamania jest różny dla różnych długości fal, które po przejściu przez soczewkę skupiają się w różnych punktach. W rezultacie dyspersja chromatyczna musi zostać skompensowana przez wprowadzenie dodatkowych soczewek, jako że liczba fal do skorygowania wzrasta. Dublet achromatyczny koryguje dwie długości fal, apochromat – trzy, a superachromat – cztery. W efekcie wprowadzanie kolejnych środowisk korekcyjnych zwiększa masę i wielkość obiektywu. Nowy rodzaj soczewek opracowany przez zespół uczonych z Harvardu został zaprojektowany tak, aby skupiać trzy długości fal bez zwiększania grubości i wielkości soczewki. W zeszłym roku zespół profesora Federico Capasso opracował nową, płaską soczewkę, która jednakowo odchyla fale widzialne o różnej barwie, czyli światło. Dzięki temu tworzony jest obraz o wysokiej jakości. Dziesięciokrotnie cieńsza od włosa soczewka wykorzystuje zjawisko dyfrakcji – światło ugina się dzięki mikroskopijnym strukturom wytworzonym w materiale soczewki. Taka „superachromatyczna" soczewka może powstać z każdego przezroczystego mate-

riału – np. szkła lub plastiku. Cieńsze od papieru soczewki mogłyby znaleźć zastosowanie w obiektywach aparatów cyfrowych i smartfonów, kamerach dronów i satelitów, medycznych endoskopach, superlekkich okularach, jak również w kamerach CCTV.

Nowa kompresja, stare problemy

Wyższe rozdzielczości wymagają nowych metod kompresji. Obecnie stosowany standard dekodera H.264 jest ograniczony wielkością obrazu składającego się z maks. 9 437 184 pikseli, które jest w stanie zdekodować maks. 56,3 kl./s. Ograniczenie to wynika z samej konstrukcji dekodera, który do zdekodowania obrazów używa wirtualnego buforu o określonej pojemności. Dotychczas H.264 sprawdzał się bardzo dobrze, przede wszystkim ze względu na elastyczną budowę. Dzięki niej producenci mogli stworzyć różne rozwiązania zmniejszające liczbę przesyłanych danych, przy jednoczesnym utrzymaniu wysokiej jakości obrazu i zgodności z wymaganiami standardu. Do takich rozwiązań można zaliczyć zmienną w czasie wartość GOP czy dynamiczne ROI zwiększające lub zmniejszające poziom kompresji wybranych części obrazów. Niestety ograniczenia w budowie obecnie wykorzystywanego algorytmu kodowania sekwencji obrazów powodują, że trzeba będzie „przesiąść się" do nowego i niepoznanego jeszcze „w boju" standardu H.265 (HEVC – *High Efficiency Video Coding*), który przesuwa maksymalną wielkość obrazu z 2160p do 4320p (35 651 584 piksele).

Obecną wiedzę o nowym standardzie kompresji branża czerpie raczej z przekazów marketingowych aniżeli z fachowych czasopism. Dlatego jesteśmy zewsząd atakowani informacjami, jakoby H.265 miał zmniejszyć zapotrzebowanie na pamięć masową o 50%. Stwierdzenie to nie jest kłamliwe, jeżeli przyjmiemy kilka podstawowych założeń:

- poziom oświetlenia w scenie jest na tyle wysoki, że nie jest wymagane elektroniczne wzmacnianie sygnału;
- poklatkowość zapisywanego strumienia wizyjnego wynosi 25 kl./s;
- rozdzielczość obrazu wynosi co najmniej 1080p.

Warto zauważyć, że wspomniane zmniejszenie pamięci masowej o 50% w porównaniu do H.264 dotyczy standardu

RYS. 6. UJĘCIA POKAZUJĄCE RÓŻNICE W KONSTRUKCJI MAKROBLOKÓW W STANDARDZIE H.264 (NA GÓRZE) I H.265 (NA DOLE)
Widoczne kolory naniesione na bloki (czerwone w H.264 i niebieskie w H.265) wskazują na zawartość zmian względem ramki poprzedzającej. Źródło: ipvm.com

H.264 *High Profile* używanego w telewizji programowej, który zakłada chociażby wykorzystanie ramek B, raczej niewykorzystywanych w systemach dozoru wizyjnego ze względu na większe opóźnienia w prezentacji obrazu. Zatem deklarowana wartość redukcji liczby danych nie musi przełożyć się na ewentualne wyniki uzyskane w systemach CCTV. Tak czy inaczej, ograniczenie liczby przesyłanych danych w nowym standardzie kodowania będzie możliwe dzięki wprowadzeniu wielu unowocześnień do H.264. Zmianą pod względem technicznym wobec dotychczasowych rozwiązań jest przede wszystkim fakt, że w standardzie H.265 makrobloki zastąpiono złożoną konstrukcją CTB (*Coding Tree Block*) o maksymalnych rozmiarach 64 x 64 piksele (16 razy większe niż w H.264). Dzięki temu uzyskuje się bardziej wydajne kodowanie, szczególnie dla wyższych rozdzielczości obrazu, niestety przy dłuższym czasie ich przeliczania. Tak duże bloki mogą być odpowiednio podzielone na mniejsze w zależności od szczegółowości danego fragmentu obrazu (*rys. 6*). Ponadto

RYS. 7. WIZUALIZACJA WYKORZYSTANIA DYNAMICZNYCH ROZDZIELCZOŚCI DOPASOWUJĄCYCH SIĘ DO ROZDZIELCZOŚCI OKNA, W KTÓRYM JEST WYŚWIETLANY OBRAZ

wykorzystuje się tu równoległe dekodowanie, czyli jednoczesne przetwarzanie różnych części obrazu, co przyśpiesza odtwarzanie i umożliwia obsługę niekompatybilnych z H.264 procesorów wielordzeniowych. Pojawia się tu też *Clean Random Access*, czyli selektywna funkcja pomagająca zwiększyć szybkość transmisji. Niestety H.265 nadal nie pozwala na skalowanie wideo, choć funkcja ta jest planowana w przyszłości.

Wprowadzanie nowego standardu kodowania nie obędzie się bez zgrzytów. Rynek telewizji dozorowej ma już za sobą trudne doświadczenie przejścia z kompresji MPEG-4 na H.264. Zapoczątkowany proces zmiany technologicznej w 2006 r. zakończył się definitywnie w 2011 r., gdy na rynek weszły ostatnie kamery i rejestratory wykorzystujące kompresję MPEG-4. W tym 5-letnim okresie wielokrotnie okazywało się, że system dopasowany do starszego algorytmu kodowania międzyobrazowego nie współpracował z nowym. Brakowało pamięci, mocy obliczeniowej, właściwych kart graficznych, aby właściwie zaprezentować płynny strumień wideo H.264. Jednostka obliczeniowa przygotowana do współpracy z nowym algorytmem niekoniecznie radziła sobie z MPEG-4.
Jestem daleki od pesymizmu – z H.265 wiążę wielkie nadzieje – ale wiem, że czas „przesiadania się" z obecnego standardu H.264 na H.265 nie będzie okresem łatwym. Nie ukrywają tego zresztą producenci sprzętu audiowizualnego na rynkach profesjonalnym i amatorskim. Wysokie rozdzielczości już w standardzie dekodera H.264 wymagają ogromnych mocy obliczeniowych. W przypadku H.265 te zasoby będą musiały być jeszcze większe. W aplikacjach klienckich VMS oczywisty okaże się wymóg wykorzystania mocy obliczeniowej procesorów graficznych (GPU). Prezentacja obrazów w trybie wielopodziału będzie determinować wykorzystanie dynamicznych rozdzielczości dopasowujących się do wielkości segmentu, w którym jest prezentowany obraz (*rys. 7*). Być może wykorzystanie koncepcji chmury i tzw. cienkich klientów, polegające na przesyłaniu zawartości ekranu w postaci jednego strumienia wizyjnego między serwerem a klientem, stanie się powszechnym rozwiązaniem?

Szumy w układach wysokich mocy obliczeniowych

Gordon Moore, szef laboratorium firmy Fairchild Semiconductor, opublikował 50 lat temu w branżowym periodyku elektronicznym artykuł, w którym przedstawił wizjonerską prognozę. Stwierdził, że liczba dyskretnych komponentów możliwych do upakowania w pojedynczym czipie komputerowym będzie się co rok podwajała, podczas gdy cena tych czipów pozostanie stała. Mowa oczywiście o „prawie" Moore'a, które najpewniej będzie obowiązywało jeszcze około sześciu stuleci*, choć początkowo twórca tej zasady przewidział jej poprawność przez 10 lat. Podczas rozwoju technologii półprzewodnikowych w tempie zgodnym z Prawem Moore'a wyłoniła się druga, mniej znana zasada skalowania, sformułowana przez Roberta Dennarda. Mówiła ona, że w miarę zmniejszania się rozmiarów tranzystorów ich gęstość energetyczna pozostaje stała. Oznacza to, że zużycie energii zmienia się proporcjonalnie do zmian powierzchni (mniejsza powierzchnia to mniejsze zużycie energii). Mniejsze tranzystory potrzebują mniejszego napięcia i natężenia prądu, tak więc wraz z kolejnymi generacjami czipów o coraz większej liczbie tranzystorów, będą one wydzielały mniej ciepła i zużywały mniej energii. Ale to właśnie ta zasada zawiodła, a nie Prawo Moore'a. Nagle okazało się, że poniżej pewnych rozmiarów tranzystorów pojawiają się prądy upływu, prowadzące do eskalującego się nagrzewania układu. W przetwornikach obrazu kamer fotodiody tworzące matrycę generują elektrony nawet w zupełnej ciemności. Jest ich tym więcej, im układ jest bardziej rozgrzany. Te generowane samoistnie elektrony sumują się z elektronami generowanymi w trakcie naświetlania przetwornika. Prąd upływu jest różny dla poszczególnych pikseli, co daje dodatkowe zróżnicowanie jasności poszczególnych punktów obrazu. Ich jasność zależy od temperatury - im wyższa, tym jaśniejszy będzie punkt pochodzący z piksela.
Wzrost mocy obliczeniowych po stronie kamer jest oczywistą konsekwencją zwiększania rozdzielczości. Większa liczba pikseli na przetworniku, wydajniejsze kodowanie oraz tendencja przenoszenia obliczeń z centralnych jednostek do tzw. urządzeń brzegowych wymuszają stosowanie układów o większej mocy, która niestety generuje coraz więcej ciepła, a ono negatywnie wpływa na jakość obrazu w postaci widocznego szumu, który nie zależy od liczby fotonów padających na matrycę. Szum związany z temperaturą sensora CMOS ma charakter losowy i w każdej klatce inny rozkład przestrzenny. Nie ma prostej możliwości usunięcia szumu, można go jedynie uśrednić, stosując np. filtrację dolnoprzepustową, kosztem utraty części informacji. Drugą możliwością (acz ograniczoną do ujęć statycznych) jest wykonanie serii zdjęć i ich uśrednienie. Niedoskonałości obrazu stają się bardziej widoczne wraz ze wzrostem jego rozdzielczości. Oznacza to, że oprócz zwiększania mocy obliczeniowej to szybkie odprowadzanie ciepła z układu, a przede wszystkim jego separacja od obszaru instalacji układu CMOS staje się polem innowacyjnych rozwiązań inżynieryjnych, mających na celu utrzymanie wysokiej jakości obrazu.

* Granicą jest tzw. granica Bekensteina - maks. ilość informacji, którą można umieścić w skończonym obszarze przestrzeni o skończonej ilości energii. Z niej wynika granica Bremermanna, określająca maks. szybkość obliczeń możliwą dla fizycznego układu w naszym wszechświecie. Wynika z niej m.in. że układ o masie Ziemi byłby w stanie przeprowadzić ok. 10^{75} operacji na sekundę.

W najbliższych latach...

Liczba pikseli przestała być wyłącznym wyznacznikiem jakości. Stanowi jeden z elementów, które oddziałując na siebie, pozwalają na osiągnięcie spektakularnych rezultatów. Standaryzacja SMPTE, innowacje w świecie fotografii, optyki oraz rozwiązania kompresji obrazu na rynku multimediów będą głównymi siłami, które pokierują dalszymi losami rynku CCTV. Wysokie rozdzielczości wpłyną również na wiele elementów powiązanych, takie jak analiza obrazu, która od jakiegoś czasu zyskuje szersze uznanie w naszej branży. Do tego dojdzie wirtualizacja strumieni, zapewniająca uzyskanie z jednej fizycznej kamery wiele wirtualnych, dostarczających obrazy z wybranych pól obserwacji. Istotne staną się kwestie związane z dekodowaniem obrazów i ich odpowiednią prezentacją. Pojawienie się kamer wysokich rozdzielczości, które zmusiły do uznania wagi optyki w tworzeniu wysoko jakościowych obrazów i wykorzystania nowych standardów kompresji, to dopiero początek fascynujących zmian w CCTV.

BIO

Jan T. Grusznic
Z branżą wizyjnych systemów zabezpieczeń związany od 2004 r. Ma bogate doświadczenie w zakresie projektowania i wdrażania rozwiązań dozoru wizyjnego w aplikacjach o rozproszonej strukturze i skomplikowanej dystrybucji sygnałów. Ceniony diagnosta zintegrowanych systemów wspomagających bezpieczeństwo.

Literatura

[1] https://tools.ietf.org/html/draft-ietf-payload-rtp-h265-15
[2] http://www.tvprzemyslowa.pl/standard-kompresji-h265/
[3] Mike Callahan: *Elemental Insights Webcast* | HEVC / H.265, 7/02/2013
[4] Gary J. Sullivan, Jens-Rainer Ohm, Woo-Jin Han, and Thomas Wiegand: *Overview of the High Efficiency Video Coding (HEVC) Standard*, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 22, NO. 12, DECEMBER 2012
[5] M. Domański, T. Grajek, J. Marek, *Zaawansowana kompresja cyfrowych sygnałów wizyjnych – standard AVC/H.264*, „Systemy Alarmowe" nr 2/2005
[6] Andreas Unterweger, What is new in HEVC/"H.265"?, Department of Computer Sciences University of Salzburg, 17/10/2012
[7] Kalkulator: Limit rozdzielczości matrycy – dyfrakcja, alphacorner.eu
[8] *Initial Report of the UHDTV Ecosystem Study Group*, © 2013 by the Society of Motion Picture and Television Engineers (SMPTE)
[9] *Understanding ultra high definition television*, Ericsson white paper, Uen 284 23-3266 | November 2015
[10] *Limitations on Resolution and Contrast*: The Airy Disk, http://www.edmundoptics.com/ , 13/03/2016
[11] Mark Peterson: *How to calculate image resolution*, Theia Technologies, 2009
[12] M. Peterson, M.S. Wilson, *What's a Megapixel Lens and Why Would You Need One*? Theia Technologies, Infinova, 5/6/2011
[13] 4K CCTV Won't Deliver 4K Images without the Right Lenses – and that's a Huge Challenge, www.ifsecglobal.com, 6/10/2015
[14] 50 lat Parawa Moore'a. *Ile jeszcze wykładniczego postępu przed nami?, Adam Galański*, www.dobreprogramy.pl/50-lat-Prawa-Moorea.-Ile-jeszcze-wykladniczego-postepu-przed-nami,News,62451.html

Dahua Technology Poland
ul. Salsy 2
02-823 Warszawa
www.dahuasecurity.com/pl

4K Dla najbardziej wymagających

Rozdzielczość kamer stosowanych w systemach monitoringu wizyjnego stale się zwiększa. **Mimo że w wielu przypadkach 1920 x 1080 pikseli jest wartością wystarczającą i akceptowalną, to postęp w tym zakresie jest ciągły, a końca wyścigu nie widać.**

Marian Maroszek
Dahua Technology Poland

Sporą popularnością cieszą się więc kamery 3- oraz 4-megapikselowe. Swój kawałek rynkowego tortu mają także urządzenia 4K, wypełniając skutecznie wysokorozdzielczą lukę. Wzrost rozdzielczości niesie wyższe wymagania względem infrastruktury sieciowej i pamięci masowych, co dla niektórych klientów nie stanowi jednak istotnego kryterium przy wyborze kamery. Czy branża jest w stanie zaproponować coś jeszcze bardziej zaawansowanego?

Oczywiście, tak. Jednym z ciekawszych przykładów takich rozwiązań jest kamera kompaktowa IPC-HF81230E. Rozdzielczość 4000 x 3000 pikseli nie pozostawia wątpliwości – jest to urządzenie dla najbardziej wymagającego odbiorcy, oczekującego maksymalnej szczegółowości rejestrowanego obrazu. Aby ograniczyć wielkość strumienia danych pochodzących z 12-Mpix przetwornika, oprócz wsparcia dla kompresji H.264 (z profilem *High* włącznie), umożliwiono także wykorzystanie algorytmu H.265. Gdyby tego było mało, oba kodeki są również dostępne w wersji *Smart,* co pozwala na oszczędność pasma sieciowego i przestrzeni dyskowej. Dostępność trzech niezależnych strumieni stanowi elastyczne uzupełnienie. Produkt serii *Ultra* nie byłby kompletny, gdyby nie dostępność funkcji analitycznych, a kamera Dahua Technology HF81230E ma ich sporo. Znajdziemy tu przekroczenie linii, wtargnięcie do strefy, jak również pozostawienie i zniknięcie obiektu. Oprócz zestawu podstawowego IVS można wykorzystać także detekcję twarzy, zliczanie osób czy generowanie map ciepła, z kolei obecność wejść i wyjść alarmowych umożliwia wygodną integrację z innymi systemami w danej instalacji. Dopełnieniem jest elektroniczna stabilizacja obrazu, funkcja *Defog*, automatyczny backfocus czy algorytm *Smart Scene Adaptive.*

Kwestią często podnoszoną przez przeciwników kamer o tak wysokich rozdzielczościach jest ich czułość. W przeszłości wysoka rozdzielczość przetwornika mogła być utożsamiania ze słabszymi parametrami pracy w trudniejszych warunkach oświetleniowych, jednak w przypadku prezentowanego urządzenia zastosowano matrycę STARVIS™ 1/1,7", co rozwiązuje kwestię czułości. Co więcej, doskonałym uzupełnieniem jest dopasowany do kamery obiektyw DH-PLZ20C0-L, który jest w stanie sprostać najwyższym oczekiwaniom. Ogniskowa 7–34 mm zapewnia uniwersalny zakres kątów widzenia bez straty czułości, gdyż wartość przysłony wynosi F/0,9. Połączenie doskonałego przetwornika obrazu i bardzo jasnego obiektywu pozwala zrealizować dozór wizyjny w wyjątkowo niesprzyjających warunkach oświetleniowych. To z kolei pozycjonuje kamerę IPC-HF81230E w kategorii produktów pozwalających zaspokoić potrzeby nawet najbardziej wymagającego odbiorcy.

FUJIFILM
Value from Innovation

Bezpieczeństwo w nowym wymiarze:

4K

Pierwszy 4K obiektyw Fujinon typu Vari Focal

Day Night

Nowy DV2.2x4.1SR4A-SA2L firmy Fujifilm
Doskonała rozróżnialność szczegółów dzięki rozdzielczości obrazu 4K.
Nadający się do użytku 24 godziny na dobę dzięki technologii dzień/noc.
Więcej informacji na stronie www.fujifilm.eu/fujinon lub per scan.
Fujinon. Widzisz więcej. Wiesz więcej.

kremer agency

FUJINON

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

Kamery 4K
Skuteczny system dozoru wizyjnego

Firma Hanwha Techwin (wcześniej Samsung Techwin) oferuje kamery serii WiseNet P z kompresją H.265 i technologią WiseStream II, wspomagającą proces kompresji poprzez jego dynamiczne sterowanie zależne od zawartości ruchu w obserwowanej scenie.

Dzięki obu funkcjonalnościom zajętość pasma i zapotrzebowanie na pamięć masową do przechowywania obrazów o rozdzielczości 12 Mpix, wytwarzanych przez kamery WiseNet P, są na podobnym poziomie jak w kamerach full HD z kompresją H.264. – *Wyrazistość obrazów z kamer 4K naprawdę zaskakuje* – mówi Sławomir Szlufik, pełniący funkcję Country Managera na Polskę i Kraje Bałtyckie. – *Wielomegapikselowe obrazy HD transmitowane w pełnej rozdzielczości i liczbie klatek są w stanie bardzo szybko zapełnić pojemność dyskową dostępną w rejestratorze sieciowym lub serwerze. Nasi inżynierowie rozwiązali problem, opracowując unikatową technologię WiseStream II.*

Nowe kamery hemisferyczne serii WiseNet P oferują 6 trybów podglądu obrazu: obraz typu „rybie oko" (*fish eye*), pojedyncza panorama, podwójna panorama, panorama i dwa okna PTZ, obraz „rybie oko" i trzy okna PTZ, podgląd w czterech oknach. Zastosowanie obiektywu „rybie oko" pozwala uzyskać panoramiczne pole widzenia o kącie obserwacji 180° lub widok dookólny zawierający pełne pole widzenia. Rozwiązanie to doskonale sprawdza się w miejscach, gdzie konieczna jest szeroka perspektywa oglądu, czyli w sklepach, centrach handlowych, biurach, na dworcach itp. Ostry obraz z kamery można uzyskać dzięki funkcji *Simple Focus* i automatycznej regulacji ostrości obiektywu uruchamianej wciśnięciem przycisku, który wyzwala proces samoregulacji.

Kamery hemisferyczne klasy Premium mają zaimplementowane algorytmy analityki na potrzeby biznesu. Liczenie osób i mapy ciepła pozwalają określić miejsca w sklepie, które cieszą się największym zainteresowaniem klientów. Dzięki wbudowanej analityce wideo można wyznaczyć

przedziały czasu, kiedy pojawia się największa liczba klientów, i wykorzystać tę wiedzę do optymalizacji czasu pracy obsługi czy zrozumienia zachowań klientów.
Modele PNF-9010RV i PNR--9010RVM zaprojektowano do pracy w najbardziej wymagających warunkach środowiskowych. Kamery, mimo wbudowanego mikrofonu, mogą pracować w zakresie temperatury otoczenia od -40°C do 55°C, w kontakcie z wodą oraz warunkach wysokiej wilgotności.
Funkcja *WiseNet PTZ hand--over* pozwala kamerom PTZ odbierać informacje o pojawieniu się alarmu (detekcja ruchu) w kamerze hemisferycznej pracującej w tym samym systemie dozoru wizyjnego. Po odebraniu powiadomienia kamera PTZ wykonuje ruch w kierunku miejsca powstania alarmu i pokazuje zbliżenie sceny. Funkcjonalność ta poprawia wydajność pracy systemu monitoringu, ponieważ wychwycenie zdarzenia i jego udokumentowanie nagraniem o właściwej zawartości jest niezależne od pracy operatora systemu CCTV.

Wyjątkowa jakość obrazu 4K Ultra HD

Model PNM-9020V to tak naprawdę kamera typu *dome* w obudowie wandaloodpornej, ale pozwalająca obserwować obraz 180°, co w obecnych systemach jest bardzo ważne. Tam gdzie trzeba byłoby zastosować 3–4 kamery kopułkowe, teraz można je zastąpić jedną PNM-9020V. Zwiększa to zarówno skuteczność systemu dozoru wizyjnego, jak i jego efektywność dzięki obrazowi 4K zawierającemu dużą liczbę szczegółów. Kamera korzysta z nowatorskiej technologii WiseStream II (redukcja do 50% pasma zajmowanego przez kamery z kompresją H.265 czy H.264). Dzięki temu można zbudować system 4K, bazując na istniejącej infrastrukturze sieci, a tym samym obniżyć koszty systemu dozoru wizyjnego, nie rezygnując z doskonałej jakości obrazu. Funkcja WDR, zaimplementowana w kamerze, sprawia, że obrazy wyróżniają się wyjątkową dynamiką, a szum wokół poruszających się obiektów zostaje znacznie zredukowany w procesie obróbki obrazu. Kamera ma wbudowane następujące funkcje: *Defog*, detekcja ruchu, utraty ostrości czy próby sabotażu.

Kamera 3D: 360° obrazu w poziomie, 90° w pionie

Kamera panoramiczna WiseNet serii P – PNM-9081VQ 20 Mpix i 360° – jest oparta na czterech przetwornikach obrazu i obiektywach moto--zoom, co pozwala na dowolną konfigurację widzianego obrazu. W efekcie przy odpowiedniej konfiguracji można uzyskać efekt 3D, a technologia żyroskopowa zapewni obraz bez zakłóceń nawet przy instalacji na masztach czy ścianach wieżowców. Ponadto funkcje analityki obrazu w kamerze pozwalają zbudować zaawansowane rozwiązanie stanowiące uzupełnienie tradycyjnych kamer obrotowych PTZ, kamer stacjonarnych typu *bullet* (kamery w obudowach zewnętrznych ze integrowanym obiektywem) czy *dome* (kamery kopułkowe). Ważną cechą kamery jest szeroka dynamika obrazu – 120 dB. Dzięki takiej niekonwencjonalnej budowie zastosowane tzw. zdalne ustawianie ostrości *simple focus* pozwala uzyskać wysokiej jakości obraz niezależnie od miejsca instalacji.

Przegląd kamer 4K

AXIS Q6128-E PTZ

- Rozdzielczość 4K
- Technologia *Axis Sharpdome*
- Funkcja *Axis Speed Dry*
- Szybkość obrotu do 700°/s
- Możliwość przemalowania

AXIS Q6128-E to niewielka, gotowa do montażu na zewnątrz kopułkowa kamera PTZ, która udostępnia rozdzielczość 4K przy szybkości 30 kl./s, 12-krotny zoom optyczny i automatyczne ustawianie ostrości. Chcąc zmniejszyć wykorzystanie przepustowości, obraz na żywo można oglądać w rozdzielczości HDTV 1080p, jednocześnie nagrywając go w rozdzielczości 4K do celów analitycznych. Precyzyjna funkcja obrotu z szybkością do 700°/s umożliwia łatwą zmianę kierunku patrzenia i śledzenie szybko poruszających się obiektów. Kamera znakomicie sprawdzi się w instalacjach na stadionach, placach, skrzyżowaniach i w innych rozległych otwartych strefach. Elektroniczna stabilizacja obrazu zapewnia płynniejszy obraz wideo podczas wietrznej pogody.
Opracowana przez Axis technologia Sharpdome zapewnia wierne odwzorowanie sceny i idealną jakość obrazu we wszystkich kierunkach zarówno powyżej, jak i poniżej linii horyzontu, dzięki czemu kamera sprawdza się także w nierównym terenie. Technologia Sharpdome obejmuje również opracowaną przez Axis funkcję *Speed Dry*, która zapewnia wyraźny obraz podczas deszczu.

Kamera AXIS Q6128-E została zaprojektowana z myślą o niezawodnej pracy i odporności na warunki atmosferyczne. Obudowa kamery ma klasę ochrony IP66 i NEMA 4X oraz odporność na uderzenia klasy IK08. Ponadto kamera udostępnia kompensację mgły i funkcję wykrywania wstrząsów, która wysyła alarm w przypadku próby wandalizmu.
Wbudowane funkcje analizy wideo dostępne w modelu AXIS Q6128-E obejmują zaawansowaną funkcję strażnika, która umożliwia wykrywanie i przybliżanie obiektów w określonym obszarze. Ponadto kamera może współpracować z inteligentnymi aplikacjami wideo innych firm.

AXIS P1368-E

- Imponująca szczegółowość dzięki rozdzielczości 4K
- Zakres temperatur: -40°C... +55°C
- Funkcje *Lightfinder* i *Forensic WDR*
- Obiektyw i-CS zapewniający wyraźny obraz i sprawną instalację
- Technologia *Zipstream*

To wytrzymała kamera sieciowa do zastosowań zewnętrznych, dostarczająca znakomitej jakości obraz 4K bez względu na warunki oświetleniowe. Kamera doskonale sprawdza się w monitoringu miejskim oraz innych zastosowaniach wymagających bardzo dobrej widoczności detali. AXIS P1368-E ułatwia wybór obiektywu najlepiej dostosowanego do wymagań, np. umożliwiającego obserwację z dużej odległości. Doskonała czułość kamery oraz technologia *Axis Lightfinder* zapewniają wysokiej jakości kolorowy obraz nawet w niemal całkowitej ciemności. Inteligentna technologia obiektywów i-CS przekłada się na prostszą instalację i regulację. Zoom można dodatkowo ustawiać zdalnie. Dzięki temu można nadzwyczaj precyzyjnie sterować przysłoną, uzyskując wyraźny obraz nawet przy zmiennym oświetleniu. Funkcja *Forensic WDR* zapewnia szczegółowy obraz również wtedy, gdy w scenie występują jasne i ciemne obszary.
Kamera jest przystosowana do pracy w niekorzystnych warunkach atmosferycznych w temperaturze od -40°C do nawet 55°C. Spełnienie wymagań klasy ochrony obudowy IP66, NEMA 4X oraz IK10 oznacza, że jest ona odporna na skrajne warunki atmosferyczne i wandalizm. W obudowie zaprojektowano miejsce na większe obiektywy. Przełączanie w ramach funkcji *Corridor Format* jest niezwykle łatwe.
Kamera jest wyposażona w technologię *Axis Zipstream*, zmniejszającą zapotrzebowanie na przepustowość i pamięć masową o 50% lub więcej. Rezultatem jest wysokiej jakości obraz i znaczące oszczędności.

AXIS P3228-LVE

- Transmisja pełnoklatkowa w rozdzielczości 4K
- Do użytku na zewnątrz, klasa ochrony obudowy IK10
- *Forensic WDR*, *Lightfinder* i *OptimizedIR*
- Zdalne ustawianie zoomu i ostrości
- Technologia *Zipstream* zmniejszająca zapotrzebowanie na przepustowość i zasoby pamięci

Niezależnie od pory dnia czy nocy sieciowa kamera AXIS P3228-LVE zapewnia wyraźne i szczegółowe obrazy. AXIS P3228-LVE to doskonały wybór do lokalizacji, w których wymagana jest wysoka szczegółowość obrazu, takich jak instytucje publiczne, uniwersytety, banki czy hotele. Potrzebujesz pewnej i niezawodnej identyfikacji osób, pojazdów lub innych obiektów przy słabym oświetleniu?

Ta kamera o rozdzielczości 4K zapewnia żywe kolory nawet w warunkach słabego oświetlenia. Choć wyższa rozdzielczość nie zawsze jest równoznaczna z lepszą jakością obrazu, dzięki kamerze AXIS P3228-LVE zawsze otrzymujesz najwyższą jakość materiału wideo. Kamera AXIS P3228-LVE ma przystępną cenę, łatwo ją zamontować i obsługiwać, dzięki czemu szybko ją skonfigurujesz i ustawisz ostrość, nawet zdalnie. Technologia *Zipstream* firmy Axis zmniejsza zapotrzebowanie na przepustowość i pamięć nawet o 50%, zapewniając przechwytywanie ważnych szczegółów w pełnej jakości obrazu, pozwalając jeszcze bardziej zmniejszyć koszty.
Tę wodoodporną kamerę można łatwo zamontować na ścianie, suficie lub skrzynce przyłączeniowej. Jest ona odporna na działanie warunków atmosferycznych i uderzenia. Obudowa zabezpieczająca przed kurzem, ze stopniem ochrony IK-10 i ochroną przeciwsabotażową zapewnia kamerze bezpieczeństwo nawet w miejscach, do których łatwo sięgnąć. W przypadku próby uszkodzenia kamery wysyłane jest powiadomienie, nie trzeba więc się martwić o uszkodzenie sprzętu.

AXIS Q3709-PVE

- 180-stopniowy panoramiczny widok ogólny
- Płynny obraz wideo przesyłany z szybkością do 30kl./s i rozdzielczością 3 x 4K
- Obiektywy z fabrycznie ustawioną ostrością
- Sprawna instalacja jednej kamery
- Gotowość do montażu na zewnątrz

Kamera AXIS Q3709-PVE zawiera trzy przetworniki obrazu, które udostępniają szczegółowy, 180-stopniowy ogólny widok rozległego obszaru, zapewniając wiedzę sytuacyjną potrzebną np. w dozorze miejskim.
Instalacja jest łatwa, niezawodna i ekonomiczna. Obiektywy są dostarczane z fabrycznie ustawioną ostrością. Kamera charakteryzuje się stylową i dyskretną konstrukcją. Zdejmowana osłona, którą można łatwo przemalowywać, chroni przed deszczem, śniegiem i światłem słonecznym oraz pozwala kamerze wtopić się w otoczenie. Dzięki widokowi panoramicznemu kamera AXIS Q3709-PVE może być optymalnym rozwiązaniem tam, gdzie jest wymagane pełne i szczegółowe dozorowanie rozległego obszaru oraz sprawne zainstalowanie jednej kamery. Kamera charakteryzuje się niezrównaną wydajnością transmisji strumieniowych: przekazuje płynny, szczegółowy obraz ruchu z szybkością 30 kl./s w rozdzielczości 3 x 4K Ultra HD lub 20 kl./s w rozdzielczości 3 x 11 Mpix. Jest przystosowana do montażu na zewnątrz budynków dzięki obudowie chroniącej przed wnikaniem kurzu i strumieniami wody padającymi pod wysokim ciśnieniem z dowolnego kierunku (klasa ochrony IP66). Jest odporna na pył przenoszony z wiatrem, rozpyloną sól, deszcz, wodę polewaną z węża i uszkodzenia powodowane gromadzeniem się lodu na zewnątrz (klasa NEMA 4X).
Obudowa kamery AXIS Q3709-PVE ma klasę ochrony IK10 gwarantującą odporność na uderzenia i akty wandalizmu.

CBC: GenSTAR ZN8-BB12M412-N

Kolejną nowością uzupełniającą popularną rodzinę GANZ IP GenSTAR jest 12-Mpix kamera typu *big-bullet*. Premiera serii GenSTAR odbyła się pod koniec 2015 r. i od tamtej pory sukcesywnie zdobywa uznanie wielu instalatorów. *Image is Everything* – to hasło doskonale korespondujące z serią kamer, które są wyposażone w wiele zaawansowanych funkcji wspierających jakość obrazu.

Kamera ZN8-BB12M412-N została wyposażona w obiektyw typu moto-zoom (4,1–12,8 mm) umożliwiający zdalną regulację zbliżenia z poziomu rejestratora lub kamery. Sterowanie obiektywem odbywa się dzięki zastosowaniu napędu zmiany położenia elementów optycznych obiektywu. Funkcjonalność ta jest szczególnie doceniana przez instalatorów ze względu na oszczędność czasu podczas regulacji kamery, jak również w przypadku lokalizacji, które wymagają okresowej zmiany zakresu pola widzenia kamery.

Nowy *bullet* jest wyposażony w cyfrową funkcję WDR oraz HLC – funkcję pozwalającą na zablokowanie (przyciemnienie) silnie oświetlonych obiektów w celu zwiększenia ich wyrazistości. Funkcja SMART-IR umożliwia dostosowanie natężenia światła IR emitowanego przez trzy niezależne sekcje diod IR-LED w celu uniknięcia efektu prześwietlenia obiektów znajdujących się w pobliżu kamery (np. twarz osoby). Do cech wyróżniających serię kamer GenSTAR, w tym również nowego modelu *bullet* można zaliczyć też ROI *(Region of Interest)* – funkcję umożliwiającą selektywną zmianę jakości nagrywanego obrazu wyłącznie w uprzednio zdefiniowanych, priorytetowych obszarach obserwowanej sceny. ROI ma realny wpływ na redukcję zajętości nagrań, co daje wymierną oszczędność fizycznej pamięci masowej (dyski HDD).

Funkcja ta sprawdza się wszędzie tam, gdzie wybrane obszary obrazu wideo powinny być rejestrowane z najwyższą rozdzielczością, przy jednoczesnej redukcji zajętości nagrań z pozostałych części obszaru. Możliwość dopasowania pola widzenia do sceny charakteryzującej się znaczną dysproporcją pomiędzy wysokością a szerokością powierzchni użytkowej obrazu, czyli tzw. tryb korytarzowy to kolejna cecha wyróżniająca tę kamerę spośród oferty rynkowej.

Dahua Technology: DH- HAC-HF3805G

Obiektyw sprzedawany osobno

Historia miejskich systemów monitoringu wizyjnego w naszym otoczeniu liczy już kilkadziesiąt lat. Mieliśmy okazję obserwować rozwój i odejście do lamusa magnetowidów, bezprecedensowy rozwój kamer analogowych, następnie szybkie rozpowszechnienie systemów sieciowych, które jako jedyne zapewniały wysokie rozdzielczości. Ale to już przeszłość.

Wraz z wprowadzeniem przez Dahua Technology standardu HDCVI 4.0 sytuacja się zmieniła. Przykładem jest innowacyjna kamera. Urządzenie to zawiera przetwornik SONY STARVIS nowej generacji, o rozmiarze 4/3" i niespotykanej dotychczas w systemach analogowych rozdzielczości 8 Mpix. Dzięki ponad 10-krotnie większej powierzchni w porównaniu z tradycyjnymi przetwornikami 1/2,8" stosowanymi w CCTV zapewnia nieporównywalnie lepszą czułość. Kamera korzysta z technologii *Quad Bayer Coding* HDR (HDR –*High Dynamic Range*), znacznie ulepszającej tradycyjny WDR stosowany w tradycyjnych kamerach i eliminującej efekty poruszenia i smużenia.

Kolejną unikatową cechą jest system mocowania obiektywów: zdecydowano się na zastosowanie znanego od lat standardu M43, umożliwiającego montaż obiektywów używanych zazwyczaj w profesjonalnych aparatach fotograficznych.

Kamera współpracuje z nową serią rejestratorów DVR 4K, a także ze starszymi modelami, które obsługiwały analogowe kamery HDCVI o rozdzielczości 4 Mpix. Dodatkowe wyjście HDMI pozwala na bezpośrednie podłączenie monitora.

DH-HAC3805G spełnia podstawowe założenia standardu HDCVI, pozwalając na przesył przewodem koncentrycznym czterech sygnałów, tj. obrazu, dźwięku, danych i zasilania. Ogromny przetwornik, profesjonalna optyka i HDR, a do tego funkcje inteligentnej analizy obrazu, możliwość bezstratnej transmisji sygnału po przewodzie koncentrycznym na dystansie do 700 m – otrzymujemy produkt unikatowy i w zasadzie kompletny.

Dahua Technology: IPC-HFW5831EP-ZE

Instalator często stoi przed trudnym wyborem: wyższa rozdzielczość czy wyższa czułość? Aby rozwiązać ten dylemat, Dahua Technology rozszerza ofertę popularnych kamer EcoSavvy o nową generację modeli 4K IPC-HFW5831EP-ZE.
Przetwornik nowej generacji SONY STARVIS zapewnia wysoką rozdzielczość 8 Mpix, zachowując przy tym bardzo dobrą czułość. Ulepszono także procesor obrazu oferujący użytkownikowi zarówno szeroki zakres dynamiki (WDR 120 dB), funkcję HLC, jak i ulepszone algorytmy redukcji szumów przy scenach o dużym ruchu.
Kamery wyposażono w nowe megapikselowe obiektywy moto-zoom, do wyboru są dwie wersje 2,7...13,5 mm oraz 7...35 mm. Zwiększył się do 100 m zasięg promienników podczerwieni. Wysoką rozdzielczość, dynamikę obrazu i szeroki zakres ogniskowych obiektywu uzupełnia kompresja H.265 lub H.265+ pozwalająca zredukować *bitrate* kamery do znanego z kamer 4 Mpix, bez utraty szczegółów, większa rozdzielczość nie musi więc wiązać się z zakupem większej liczby dysków twardych. Czas archiwizacji można zoptymalizować, wykorzystując do nagrywania jedną z funkcji analityki wideo zaimplementowaną w urządzeniu – wykrycie intruza, przekroczenie wirtualnego płotu, zniknięcie obiektu, wykrycie pozostawionego obiektu czy detekcja twarzy.
Dahua Technology wielokrotnie udowodniła, że jest liderem w wyznaczaniu nowych standardów i ścieżek rozwoju branży CCTV. Tym razem również zapowiada się prawdziwa rewolucja na rynku. Wszystkie kamery z nowej serii EcoSavvy wykorzystują nowy standard Dahua ePoE. Dotychczas używany standard PoE umożliwiał zasilanie i transmisję z kamer na maks. odległość 100 m. Nowe rozwiązanie producenta zwiększa ten dystans do 300 m przy zachowaniu 100 Mb/s i mocy 24 W! Maksymalna odległość może wynieść nawet 800 m! Nie ma potrzeby stosowania światłowodu, a co za tym idzie mediakonwerterów, wkładek oraz zasilania przy punkcie kamerowym, a to przekłada się na możliwość bardziej elastycznego budowania systemów, zapewniając jednocześnie ogromne oszczędności!

Dahua Technology: HAC-PFW3601-A180

Wysoka rozdzielczość w systemach dozoru wizyjnego zagościła na dobre, większa liczba pikseli pozwala bowiem na obserwację znacznie większego obszaru, a to przekłada się na redukcję liczby kamer w systemie. Dlatego tak popularne stały się kamery typu „rybie-oko" oferujące obraz 180° x 180°. Mają one jednak wady – zniekształcony obraz musi zostać „wyprostowany", a to obciąża stację kliencką i co gorsza, sprawia, że z megapikseli oferowanych przez przetwornik do użytku pozostaje czasami mniej niż połowa. Wielu producentów wiąże przyszłość z kamerami wieloprzetwornikowymi, w których obraz z kilku przetworników łączą w jeden widok panoramiczny. To rozwiązanie sprawdza się doskonale nie tylko w miejskich systemach dozoru wizyjnego, ale także w dozorze parkingów, stacji benzynowych, lotnisk czy magazynów. Wydaje się, że jest to naturalna ewolucja w systemach dozoru wizyjnego i tak naprawdę mało kto spodziewał się, że tak szybko będziemy świadkami prawdziwej rewolucji.
Dahua Technology łamie kolejną barierę, dowodząc, że przyszłość jest teraz. Wraz z wprowadzeniem standardu HDCVI 4.0 do oferty trafiły wieloprzetwornikowe, panoramiczne kamery analogowe o rozdzielczości 4K! Jedną z nich jest HAC-PFW3601-A180. Kamera ta zawiera trzy superczułe przetworniki obrazu SONY STARVIS o podwyższonej dynamice obrazu. Obraz z nich jest łączony w kamerze i dostępny na jednym z wyjść BNC. Po podłączeniu do rejestratora CVI operator może cieszyć się obrazem panoramicznym 180° o rozdzielczości 8 Mpix! Kamera współpracuje nie tylko z rejestratorami 4K, ale także z tradycyjnymi modelami DVR obsługującymi rozdzielczość fullHD, ponieważ każdy z przetworników ma dodatkowe wyjście BNC i umożliwia podłączenie ich z osobna.
Standard HDCVI kamery umożliwia przesył przewodem koncentrycznym czterech sygnałów, tj. obrazu, dźwięku, danych i zasilania. Uzupełniając przedstawioną charakterystykę tego modelu o funkcje inteligentnej analizy oraz wirtualnego PTZ, otrzymamy produkt unikatowy i w zasadzie kompletny.

Hikvision: DS-2DF8836IX-AELW

To model należący do nowej generacji kamer PTZ z linii profesjonalnej firmy Hikvision. To pierwsza kamera obrotowa o rozdzielczości 4K w ofercie Hikvision wyposażona w technologię *DarkFighter*. Bardzo czuły przetwornik CMOS o przekątnej 2/3" wspomagany przez najnowocześniejszy procesor generuje płynny obraz w najwyższej rozdzielczości z szybkością 30 kl./s, a dzięki technologii *DarkFighter* kamera może pracować nawet przy bardzo słabym oświetleniu, nie tracąc kolorów.

Na uwagę zasługuje także układ optyczny. Obiektyw o 36-krotnym zoomie optycznym zapewnia wyjątkowy poziom szczegółów, a funkcja *Optical Defog* pozwala dostrzec obiekty nawet przez mgłę. Układ optyczny został wyposażony w funkcję *Rapid Focus*, która ustawia ostrość podczas zmiany parametrów ogniskowej tak szybko, że użytkownik ma wrażenie ciągłego ostrego obrazu. Uniwersalność kamery podkreślają silny WDR o mocy 120 dB oraz promiennik IR o zasięgu 200 lub 500 m w zależności od wybranej wersji sprzętu. Model DS-2DF8836IX-AELW został wyposażony w procesor odpowiadający za pracę algorytmów *Deep Learning*, wzbogacając kamerę w funkcjonalność inteligentnego rozpoznania, identyfikacji i śledzenia obiektów.

Hikvision: DS-2CD5085G0-AP

To 8-Mpix kamera typu box reprezentująca nową linię profesjonalnych kamer stałopozycyjnych (seria 5). W porównaniu do poprzedniej wersji model ten zapewnia większą wydajność, m.in. możliwe jest generowanie aż 5 strumieni wizji jednocześnie, z czego pierwszy strumień o rozdzielczości 4K@30 kl./s w kodeku H.265, drugi strumień (pomocniczy) o rozdzielczości 4CIF@30 kl./s, trzeci strumień – 1080p@30 kl./s w H.265 oraz czwarty i piąty w kodeku MJPEG lub także w H.265, odpowiednio 1080p@30 kl./s i 4Cif@30 kl./s. Dostępny protokół ONVIF zapewnia bezproblemową integrację kamery z każdym systemem telewizji dozorowej.

Kamera została wyposażona w rzadko spotykane w tego typu urządzeniach wyjście napięciowe 12 VDC, umożliwiające lokalne zasilanie mikrofonu lub czujki PIR. W kamerze z nowej linii projektowej nie mogło zabraknąć takich funkcji, jak *DarkFighter* czy sprzętowego WDR o mocy 120 dB. Prezentowany model jako kamera typu box wymaga instalacji obiektywu, obsługuje zarówno obiektywy DC-IRIS, jak i P-IRIS. Dodatkowo funkcja *Auto Back Focus* umożliwia szybkie dostrojenie ostrości.

Hikvision: DS-2DP1636ZIX/236

Rozwiązania 4K (8 Mpix) to nie tylko kamery oparte na jednym przetworniku. Hikvision umożliwia osiągnięcie takich rozdzielczości także dzięki cyfrowemu połączeniu ze sobą obrazów z czterech przetworników 2-megapikselowych – przykładem może być np. seria kamer PanoVu. Nowy model DS-2DP1636ZIX/236 został wyposażony w osiem 2-megapikselowych modułów kamerowych o ogniskowej 5 mm, z których urządzenie składa obraz w dwie 8-megapikselowe panoramy. Są one wspomagane kamerą PTZ o rozdzielczości 2 Mpix z promiennikiem podczerwieni o zasięgu 200 m. Wszystkie moduły kamerowe wykorzystują technologię *DarkFighter,* więc idealnie sprawdzą się nawet w trudnych warunkach oświetleniowych.

Kamera PanoVu ma ponadto bardzo przydatną funkcję sterowania kamerą obrotową. Operator, klikając punkt na obrazie panoramicznym, sprawia, że kamera obrotowa automatycznie obraca się i przybliża (wykonuje zoom) wskazane miejsce. Dzięki temu DS-2DP1636ZIX/236 doskonale sprawdza się do monitorowania dużych przestrzeni, zapewniając stały podgląd tego, co się dzieje wokół punktu kamerowego z bardzo dużą liczbą detali w tym samym czasie.

Na przyszły rok zaplanowano premierę modelu DS-2DP1636ZIX/836 serii PanoVu. 2-megapikselową kamerę PTZ zastąpi w nim kamera PTZ o rozdzielczości 4K, co umożliwi rejestrację jeszcze większej liczby szczegółów.

Hikvision: DS-2CD2685FWD-IZS

Rozdzielczość 4K nie jest już tylko domeną drogich, projektowych rozwiązań. Wraz z wprowadzeniem na rynek serii Easy IP 3.0 firma Hikvision zaprezentowała interesujące kamery wyposażone w przetwornik o takiej rozdzielczości. Przykładem może być model DS-2CD2685FWD-IZS. Oprócz dużej rozdzielczości charakteryzuje się sprzętowym WDR-em o mocy 120 dB oraz podstawowymi funkcjami analizy obrazu, takimi jak wykrycie wtargnięcia czy detekcja przekroczenia linii.

Układ optyczny to obiektyw 2,8–12 mm z funkcją motozoom. Ponadto kamera została wyposażona w promiennik IR o zasięgu do 50 m oparty na nowej technologii diod IR – EXIR 2.0 o długości fali 850 nm. Całość obudowy wykonano zgodnie ze standardami IK10 oraz IP67. Obraz w rozdzielczości 4K jest generowany z szybkością 20 kl./s z użyciem kodeka H.265. Ten model jest idealnym rozwiązaniem do małych i średnich instalacji, gdzie trzeba dostarczyć bardzo dobrej jakości obraz w najlepszej cenie.

Honeywell: EquIP® 4K HBD8GR1

W miejscach wymagających ponadprzeciętnej jakości i szczegółowości nagrywanego obrazu idealnie sprawdzi się kamera Honeywell serii EquIP® 4K. Generuje ona obraz w proporcjach zarówno 4:3, jak i 16:9 w najwyższej rozdzielczości z wydajnością 20 kl./s. Wszystko to sprawia, iż użytkownik otrzymuje wysokiej jakości, idealny i płynny obraz. Dzięki temu nawet najbardziej wymagający klienci będą usatysfakcjonowani pracą tego modelu.
HBD8GR1 został wyposażony w specjalny moduł bezpieczeństwa – sprzętowy układ wmontowany w kamerę, który odpowiada m.in. za bezpieczne połączenie użytkownika do kamery (https). Z uwagi, że jest to rozwiązanie sprzętowe, kamera EquIP® jest nieporównywalnie lepiej zabezpieczona niż inne standardowe kamery wyposażone w programową funkcję odpowiedzialną za bezpieczeństwo w sieci. W dobie cyberterroryzmu i cyberataków to niezwykle ważne.
Kamera ma wbudowane funkcje wspomagające wykrywanie zagrożeń. Oprócz podstawowej funkcji detekcji ruchu użytkownik znajdzie w opcjach kamery możliwość włączenia detekcji twarzy oraz zmiany sceny (sabotaż). Jest także możliwa rozbudowa kamery o funkcje analityczne. Analiza obrazu oparta na rozwiązaniach firmy Xtralis® oferuje wiele zaawansowanych funkcji VCA. Użytkownik może sam decydować, do których kamer HBD8GR1 zainstalowanych w obiekcie chce dodać opcję analityczną. Dzięki temu optymalizuje pracę całego systemu.
Model HBD8GR1 został ponadto wyposażony w szereg złączy, m.in. wejście/wyjście alarmowe, złącze na kartę microSDHC do 128 GB czy wejście/wyjście audio. W tej serii występują również modele: wandaloodporna kamera kopułowa oraz kamera klasyczna.

Panasonic: WV-SPV781L

Wandaloodporna kamera WV-SPV781L oferuje rozdzielczość 4K oraz technologię kompresji zapewniającą najwyższą jakość obrazu w plikach o 7-krotnie mniejszym rozmiarze niż w przypadku innych modeli 4K. Kamera jest wyposażona w obiektyw z 6-krotnym zoomem optycznym oraz wysokiej czułości przetwornik obrazu 12 Mpix. Umożliwia pracę przy słabym świetle na poziomie 0,3 luksa (obraz kolorowy) oraz 0,03 luksa (obraz czarno-biały). Ponadto zainstalowana dioda IR LED zapewnia uzyskanie obrazu przy całkowitej ciemności Model WV-SPV781L idealnie nadaje się do zastosowań na zewnątrz, np. w miejskim systemie monitoringu wizyjnego, na skrzyżowaniach, w dozorze zakładów karnych lub na parkingach. Sprawdzi się także w dozorze lotnisk, dworców, terminali przeładunkowych, a także obiektów przemysłowych.
Kamera ma pole widzenia o kącie od 17° do 96° w poziomie i proporcjach obrazu 16:9 lub o kącie od 17° do 100° w poziomie i proporcjach 4:3. Jest odporna na warunki atmosferyczne i wstrząsy (zgodnie z IP66, NEMA4x i IK10), a dzięki powłoce przeciwdeszczowej zapewnia dobrą widoczność w czasie opadów.
Obraz może być rejestrowany w rozdzielczości 4K (3840 x 2160) z szybkością do 30 kl./s lub w 12 Mpix (4000 x 3000) z szybkością do 15 kl./s. Za doskonałą jakość odpowiada także funkcja kompensacji mgły oraz technologia HLC *(High Light Compensation)*, redukująca efekt oślepienia przez mocne źródła światła, np. reflektory samochodowe.
Oszczędność miejsca na dysku gwarantuje technologia VIQS *(Variable Image Quality on Specified area)*, która umożliwia wskazanie ośmiu miejsc o wyższej jakości rejestrowania obrazu i obniżenie jakości w pozostałych obszarach, dzięki czemu zmniejsza się rozmiar plików obrazu i szybkość bitowa. Co więcej, kamera WV-SPV781L zapewnia równoczesną transmisję strumieni w formatach H.264 *(High profile)* i JPEG, umożliwiając dozór w czasie rzeczywistym i jednoczesne nagrywanie obrazu o wysokiej rozdzielczości.

SONY: SNC-VB770 (dystrybucja: Suma)

Kamera sieciowa 4K SONY SNC-VB770 wyróżnia się niespotykanym poziomem minimalnego oświetlenia: 0,004 luksa, dzięki bardzo dużej czułości, nawet do ISO 409 600. Oznacza to możliwość rejestracji kolorowego obrazu 4K z prędkością 30 kl./s nawet nocą i w innych skrajnych warunkach oświetlenia, gdzie problem z dostrzeżeniem obiektów miałoby również oko ludzkie. Kamera osiąga ten poziom czułości dzięki 35-mm pełnoklatkowemu przetwornikowi obrazu SONY Exmor oraz wykorzystującym jego potencjał obiektywom z mocowaniem typu E (kilka typów do wyboru) i procesorowi sygnału, także opracowanym przez SONY. Szybka migawka elektroniczna zapobiega rozmazywaniu obrazu, dzięki czemu na nagraniach z ciemnych miejsc wyraźnie widać litery, cyfry i mimikę twarzy. Kamera obsługuje pięć niezależnych strumieni, które w połączeniu z innymi funkcjami pozwalają na efektywne wykorzystanie możliwości kamery oraz poprawiają skuteczność i opłacalność systemu monitoringu wizyjnego w różnych zastosowaniach.

Funkcje inteligentnego śledzenia oraz śledzenia wielu obiektów umożliwiają rozpoznanie i dynamiczne śledzenie wielu obiektów w niezależnych oknach – w połączeniu z podglądem sytuacyjnym całej sceny (tzw. *Intelligent Cropping* i *Multi Tracking*). System inteligentnego kodowania zapewnia maksymalną szczegółowość fragmentów o kluczowym znaczeniu (tzw. ROI – *Region Of Interest*) i niższą przepływność w pozostałych częściach obrazu. Takie rozwiązanie pozwala znacząco ograniczyć wykorzystanie przepustowości sieci (do ok. 6 Mb/s przy rozdzielczości 4K) oraz przestrzeni dyskowych do zapisu nagrań. Funkcja inteligentnej rejestracji sceny (*Intelligent Scene Capture*) automatycznie dobiera optymalne ustawienia obrazu, z uwzględnieniem różnych warunków środowiskowych, takich jak pogoda, pora dnia czy oświetlenie. Kamera zawiera także pakiet funkci analitycznych DEPA Advanced i ma wyjście HDMI. Instalację kamery ułatwia SNC Toolbox Mobile – mobilna aplikacja i klucz USB, umożliwiająca podgląd obrazu z kamery na telefonie. Kamera jest zgodna z ONVIF.

SONY: SNC-VM772R (dystrybucja: Suma)

Kamera 4K SNC-VM772R jest przeznaczona do pracy w trudnych warunkach w całodobowym wideomonitoringu wewnętrznym i zewnętrznym. Dzięki bardzo wysokiej czułości i dobrej czytelności obrazu model ten idealnie nadaje się do systemów dozorowych o szczególnym znaczeniu. Kamera jest wyposażona w duży 1-calowy i bardzo czuły przetwornik obrazu CMOS Exmor R™, którego uzupełnienie stanowią szybki procesor obrazu oraz zmiennoogniskowy obiektyw także opracowane przez SONY. Taki zestaw elementów umożliwia rejestrację szczegółowego i płynnego obrazu 4K z prędkością 30 kl./s nawet w złych warunkach oświetleniowych (od 0,06 lx). Kamera obsługuje pięć niezależnych strumieni, które w połączeniu z innymi funkcjami pozwalają na efektywne wykorzystanie jej możliwości. Funkcje inteligentnego śledzenia obiektu oraz śledzenia wielu obiektów umożliwiają rozpoznawanie i dynamiczne śledzenie wielu obiektów w niezależnych oknach – w połączeniu z podglądem sytuacyjnym całej sceny (tzw. *Intelligent Cropping i Multi Tracking*). Funkcja inteligentnego kodowania zapewnia maksymalną szczegółowość fragmentów o kluczowym znaczeniu, a obniża przepływność w pozostałych częściach obrazu. Pozwala to znacząco ograniczyć wykorzystanie przepustowości sieci (do ok. 6 Mb/s przy rozdzielczości 4K). Przetwornik 20 Mpix umożliwia rejestrowanie fotografii (tzw. *evidence shot*) o wysokiej jakości, w rozdzielczości 5472 x 3648. Mogą one posłużyć do szczegółowej analizy sceny lub celów dowodowych. Aby zapewnić najlepszą możliwą jakość obrazu, dobór ustawień odbywa się automatycznie, uwzględniając szeroki wachlarz warunków pracy (warunki atmosferyczne, oświetlenie). Kamera jest wyposażona w wysokiej jakości obiektyw (odpowiedni do zdjęć 20 Mpix), stabilizację obrazu, oświetlacz IR, wyjście HDMI. Obudowa IP66, IK10 oraz zakres temperatury pracy -40°C ... 50°C, umożliwiając pracę kamery w trudnych warunkach środowiskowych. Kamera jest zgodna z ONVIF. Jej instalację ułatwia SNC Toolbox Mobile – mobilna aplikacja i klucz USB, zapewniająca podgląd obrazu z kamery na telefonie.

Więcej światła...
a może mniej
czyli o oświetleniu planu Cz.1

Coraz lepsze parametry kamer używanych w systemach dozoru wizyjnego, coraz szybsze procesory i skuteczniejsze algorytmy cyfrowej korekty wpływają na poprawę jakości obrazu. Projektując system CCTV, współczesny projektant i instalator nie musi w zasadzie martwić się o zastane w obiekcie oświetlenie. To prawda czy mit?

Maciej Grzondkowski

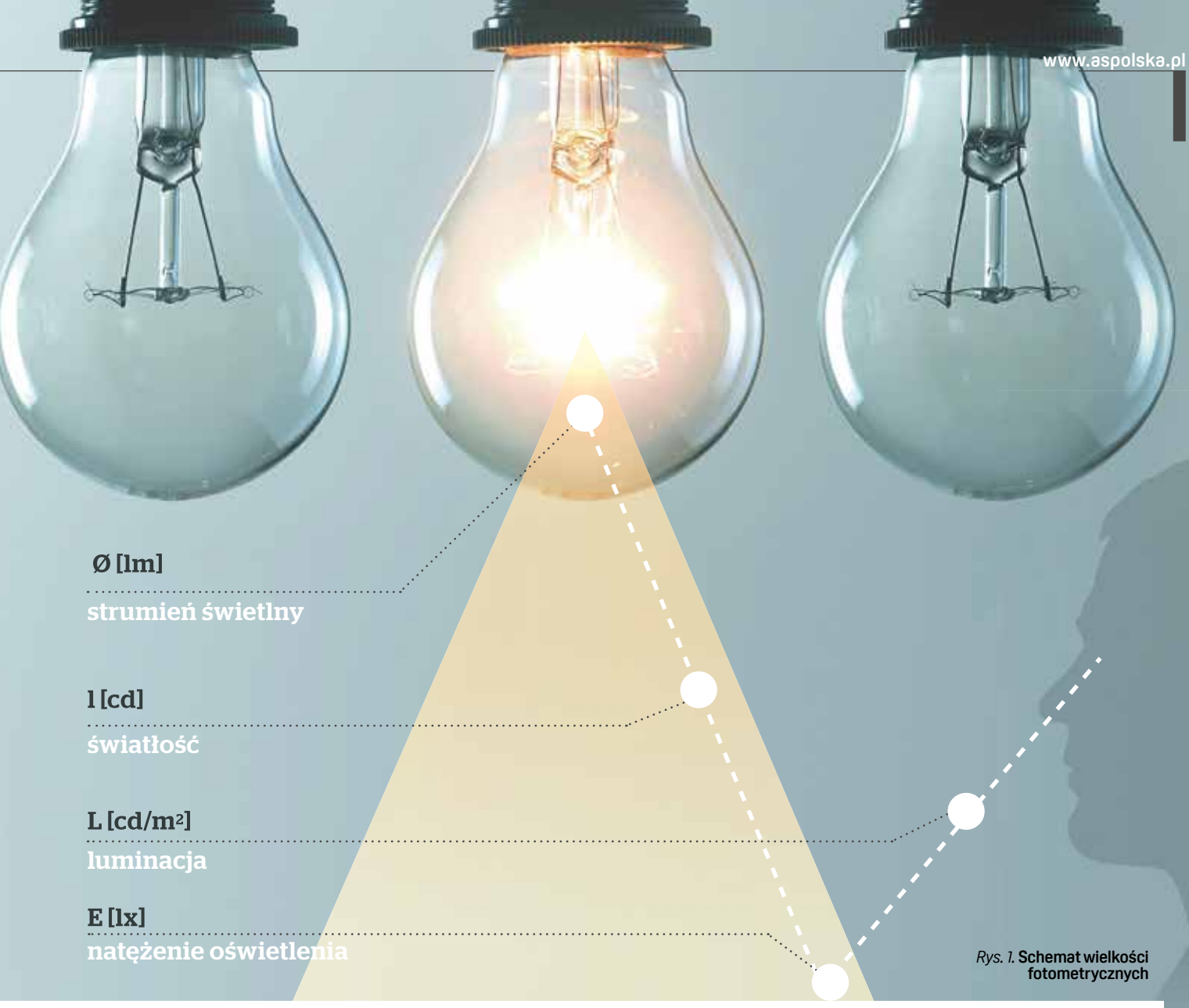
Współczesne modele kamer „rozleniwiły" osoby zajmujące się instalacją i projektowaniem systemów CCTV. W zasadzie nawet tani model daje sobie radę zarówno w czasie słonecznego dnia, jak i po zmroku. Bardzo czułe przetworniki obrazu oraz dedykowane procesory wizyjne gwarantują prawidłowy, wysokiej jakości obraz. Stąd pytanie, dlaczego tak rzadko materiał nagrany przez te punkty kamerowe pozwala rozpoznać twarz, numery rejestracyjne lub inne istotne szczegóły obrazu. Moją diagnozą są niestety braki w wiedzy dotyczącej projektowania oświetlenia planu obserwacyjnego.

Zacznijmy od początku, czyli od wiedzy podstawowej opisującej środowisko oświetleniowe. Współczesna fizyka (dział fotometrii) i technika opisują światło i jego jakość, korzystając z kilku podstawowych jednostek, wielkości fizycznych i parametrów *(rys. 1)*, które każdy branżysta powinien znać. Pierwszą jest światłość.

Światłość (natężenie strumienia źródła światła) to w fotometrii wielkość charakteryzująca wzrokowe wrażenie jasności źródła światła. Jest podstawową wielkością w fotometrii wizualnej. Jednostką światłości jest **kandela**, która należy do jednostek podstawowych układu jednostek SI. Światłość opisuje „energię" światła, jaka jest promieniowana przez dane źródło światła i zależy od skupienia wiązki.

Strumień świetlny to wielkość fizyczna określająca całkowitą moc światła emitowanego przez źródło światła, wywołująca określone wrażenie wzrokowe. W przeciwieństwie do światłości nie zależy od sposobu skupienia lub prowadzenia wiązki. Strumień świetlny służy do opisania ilości światła, jaką dane źródło światła (np. żarówka) jest w stanie wyemitować. Jednostką jest **lumen** – parametr z pewnością znany, gdyż występuje w każdej karcie katalogowej żarówek, świetlówek, lamp typu LED lub innych źródeł światła dostępnych w handlu. Należy pamiętać, że podobnie jak dla dźwięku wrażenie wzrokowe ilości światła jest nieliniowe i np. dwukrotne zwiększenie mocy żarówki wcale nie oznacza dwukrotnie większej zauważalności ilości światła. Stąd takie a nie inne typoszeregi źródeł światła, np. żarówek: 40 W, 60 W, 75 W, gdyż oko ludzkie nie zauważyłoby w zasadzie żadnej różnicy dla żarówki o mocy np. 40 lub 48 W.

Rozpoczynamy cykl artykułów, których celem jest ukazanie czytelnikom, że oświetlenie na planie obserwacyjnym jest niezwykle ważne i to ono w większości przypadków decyduje o jakości obrazu uzyskiwanego za pomocą systemu monitoringu wizyjnego.



Rys. 1. **Schemat wielkości fotometrycznych**

Kolejna wielkość to **natężenie oświetlenia**. Jest to iloraz natężenia strumienia świetlnego padającego na daną powierzchnię („gęstość" strumienia światła). Opisywane jest następującym wzorem:

$$E = I/r^2 \cos \alpha \ [lx]$$

gdzie:
E – natężenie oświetlenia,
I – światłość,
r – odległość punktu powierzchni od źródła światła,
α – kąt między normalną do powierzchni a wektorem skierowanym na źródło światła (kierunek padania światła).

Jednostką natężenia oświetlenia jest lux [lx] Poziom natężenia oświetlenia i jego rozkład w obszarze pracy i jego otoczeniu w dużym stopniu decyduje o sprawnym wykonywaniu pracy wzrokowej. Podobnie jak w przypadku strumienia świetlnego, odczucie światła przez obserwatora nie jest liniowe, dlatego zaleca się następujące stopniowanie poziomów natężenia oświetlenia: 20-30-50-100-150-200-300-500-750-1000-1500-2000-3000-5000 lx. Poziomy natężenia oświetlania w środowisku pracy są znormalizowane, np. według polskiej normy PN-EN 12 464-1: 2004 są następujące:
- rozpoznanie rysów twarzy – 20 lx,
- wykonywanie prostych czynności – 50 lx,
- warsztat – 200 lx,
- obsługa komputera – 500 lx,
- montaż precyzyjny, zakład jubilerski – 1000 lx.

Rys. 2. **Przykładowe wartości luminancji**

Dla porównania kilka przykładów
- oświetlenie powierzchni Ziemi przez Księżyc w pełni – 0,2 lx,
- oświetlenie uliczne w nocy – 5–10 lx,
- zachmurzone niebo – 5000 lx,
- słoneczny letni dzień (bezchmurne niebo) – 100 000 lx.

W przypadku kamer CCTV parametr czułość jest wartością (minimalnego) natężenia oświetlenia planu obserwacyjnego.

Luminancja to kolejna, niezwykle istotna wielkość fotometryczna, która jest miarą natężenia oświetlenia padającego

w danym kierunku. Określa ilość światła, które przechodzi lub jest emitowane przez daną powierzchnię, i mieści się w zadanym kącie bryłowym. Co istotne, jest to wielkość odpowiadająca wrażeniu wzrokowemu, które odbiera oko patrzące na świecącą powierzchnię, np. ekran monitora lub oświetloną ścianę. W układzie SI jednostką luminancji jest kandela na metr kwadratowy [cd/m^2] (dawniej nit [nt]). Przykładowe wartości luminancji przedstawiono na *rys. 2.*

Z punktu widzenia branży telewizji dozorowej luminancja wydaje się bardzo przydatną wielkością fotometryczną, jednak niewielu instalatorów ma świadomość jej wagi i nie potrafi jej prawidłowo wykorzystać. Dzięki znajomości luminancji łatwiej dobrać miejsce umieszczenia punktów kamerowych lub układu planu obserwacyjnego.

Temperatura barwowa to bardzo ważny parametr, dzięki któremu projektant oświetlenia potrafi prawidłowo dobrać rodzaj źródła światła dla danego obiektu. Zgodnie z definicją to kolor „świecenia" tzw. ciała czarnego podgrzanego do danej temperatury. Temperatura barwowa jest podawana w stopniach kelwina (K). Im niższa temperatura, tym „cieplejszy" odcień, poczynając od czerwieni, kończąc na wartościach wysokich z odcieniami niebieskiego. Przykładowo temperatura barwowa żarówki halogenowej to 2600–2700 K, a lampy LED typu dziennego około 5000 K *(tab. 1).* Parametr obecnie bardzo popularny, jest podawany przez producentów źródeł światła, np. popularnych obecnie lamp typu LED.

Współczynnik oddawania barwy to z kolei parametr, o którym wiedzą nieliczni, a decydujący o jakości postrzegania barw przy oświetleniu danym typem źródła światła. Im współczynnik jest bliższy 100 (wartość idealna, porównywalna do postrzegania przez nas barw przy oświetleniu światłem słonecznym), tym kolor obiektów na planie jest bardziej naturalny *(rys. 3, tab. 2).*

Obecnie tylko lampy żarowe (czyli zwykła żarówka lub żarówka halogenowa) zbliżają się do tej wartości, pozostałe źródła światła, w tym lampy LED, świetlówki czy lampy metalohalogenkowe, nie są w stanie osiągnąć tej wartości. Stąd czasami dramatycznie różne postrzeganie pewnych kolorów, np. czerwieni na planach. Lampy typu sodowego czy rtęciowego (stosowane bardzo często do oświetlenia terenów zewnętrznych) mają bardzo niskie współczynniki oddawania barwy i w tym przypadku nie ma co liczyć, że barwa na planie postrzegana przez oko lub kamerę będzie naturalna.

W następnym wydaniu a&s Polska opiszemy projektowanie planu oświetleniowego.

Tab. 1. **Tabela temperatur barwowych**

2000K	Świeczka
2700K	Ciepło –biała (żarówka)
3000K	Zachód słońca
3500K	Lampy studyjne
4000K	Biała
5000K	Chłodno-biała
6500K	Dzienna
10000K	Bezchmurne niebo

Tab. 2. **Współczynnik oddawania barwy**

Oświetlenie terenów zewnętrznych		Oświetlenie wnętrz
	100	Idealne
	80	Bardzo dobre
Bardzo dobre		Dobre
	60	Umiarkowane
Dobre		
	40	Nieakceptowalne
Umiarkowane		
	20	
Złe, ale akceptowalne		

Rys. 3. **Współczynnik RA**

BIO

Maciej Grzondkowski
W branży security od ponad 17 lat, związany przede wszystkim z systemami wizyjnymi. Wdrożył wiele produktów i linii produktowych na rynek krajowy. Krzewi dobre zasady projektowania oświetlenia w systemach telewizji dozorowej.

www.aspolska.pl

a&S POLSKA

Magazyn

teraz również w wersji na tablet i telefon

Dostępne w App Store

DOSTĘPNE W Google play

Trzeba mieć koncepcję

Praca związana z przygotowaniem projektu czy złożonego zadania wymaga zarówno wysiłku umysłowego, koncentracji i oparcia się na przyjętej wcześniej logistyce, jak i zaplanowania czasu na jej wykonanie. **W obecnych, jakże „szybkich" czasach, praca koncepcyjna często jest zastępowana rozwiązaniem spośród dostępnych oraz decyzją kierownictwa firmy czy instytucji o natychmiastowym wdrożeniu wybranego rozwiązania, najczęściej w trybie „zaprojektuj i zbuduj".**

Maciej Jaszczuk

Dokonując wyboru konkretnego systemu zabezpieczenia technicznego mającego wspierać system bezpieczeństwa firmy, najczęściej kierujemy się atrakcyjnością ofert dostępnych na rynku oraz informacją o walorach danego systemu przekazywaną przez osoby zajmujące się sprzedażą i marketingiem. Ponadto wybór ten zazwyczaj jest obwarowany zasadami polityki dotyczącej zakupów w organizacji. Etap prac analitycznych i koncepcyjnych jest zatem często pomijany i w praktyce koncepcję zabezpieczenia buduje się na wybranym, zainstalowanym i wdrożonym systemie. Powoduje to znaczne ograniczenie – zazwyczaj do możliwości posiadanego już systemu.

Osoby odpowiedzialne za bezpieczeństwo lub ochronę fizyczną w danej instytucji nierzadko wpadają w taką pułapkę. Po pierwsze pułap podejmowania decyzji związanych z zastosowaniem określonej technologii czy techniki jest nieodpowiedni. Najczęściej bowiem decyzja o wydatkowaniu środków na konkretne zabezpieczenia zapada na szczeblu kierownictwa wyższego szczebla, które dokonując wyboru, kieruje się atrakcyjną ceną danego produktu, a nie jego przydatnością. To prawda, że szef nie musi się znać na wszystkim, musi jednak posiadać kompleksowe informacje przekazane przez menedżera odpowiedzialnego za bezpieczeństwo o tym, jakie zabezpieczenia w danym momencie są potrzebne. Nierzadko jednak się zdarza, że osoby odpowiedzialne za bezpieczeństwo nie mają wystarczającej wiedzy w zakresie poszczególnych systemów, a także środków i mocy przerobowych, aby wykonać rzetelną pracę koncepcyjną w danym zakresie.

Kolejnym problemem jest premiowanie szybkości wykonania zadania – jakże często podstawowym kryterium jest czas realizacji systemu zabezpieczeń, przy jednoczesnym zaniedbaniu analizy traktującej o tym, czy ten system jest rzeczywiście niezbędny i odpowiedni. Tego typu sytuacja jest zazwyczaj akceptowana lub co najmniej traktowana z przymrużeniem oka dopóty, dopóki organizacja w wyniku wadliwego działania systemu nie poniesie określonej straty. Równie często ścisłemu kierownictwu firmy wydaje się, że instalacja systemu zabezpieczenia rozwiązuje wszelkie problemy z bezpieczeństwem. Nic bardziej mylnego, ponieważ system choćby najbardziej złożony, inteligentny i zaawansowany musi działać na podstawie stosownych procedur, przepisów i przy udziale personelu ochrony, a te wszystkie aspekty należy przewidzieć podczas opracowywania koncepcji bezpieczeństwa określonej firmy czy organizacji. Świadome kierownictwo zleci wykonanie pracy koncepcyjnej wykwalifikowanym pracownikom, jeśli taki personel posiada. Jeśli nie, powinno rozważyć zamówienie opracowania w firmie specjalizującej się

w wykonywaniu takich usług. Nie oznacza to jednak, że cała praca odbędzie się bez udziału podmiotów związanych z zamawiającym. Warto zastanowić się, co powinna zawierać przedmiotowa koncepcja. Pomijając atrybuty formalno-prawne, takie jak podstawa i cel opracowania, informacje o jego autorach czy też charakterystyka użytej metody analitycznej, koncepcja powinna opierać się na podanych niżej zagadnieniach.

Trzeba zacząć od wskazania, co w danej firmie ma być chronione, czyli od zdefiniowania zasobów wrażliwych lub krytycznych, jeśli występują. Zespół ekspertów takie informacje powinien uzyskać od wyznaczonych przez kierownictwo firmy pracowników, na podstawie przygotowanych wcześniej ankiet lub wywiadu środowiskowego i wizji lokalnych, a następnie poprzeć je i uzupełnić informacjami zaczerpniętymi z własnej wiedzy i doświadczenia.

Wiedząc, jakie zasoby mają być chronione, należy oszacować potencjalne zagrożenia, w których efekcie firma może ponieść straty. Porównanie zasobów i zagrożeń powinno już przynajmniej w zarysie określić poziom ochrony, jaki należy zastosować w instytucji. Często zdarza się bowiem, że nakłady na zabezpieczenia (sprzęt i ludzie) znacznie przekraczają wartość poniesionych strat w wyniku wystąpienia danego zagrożenia.

Proces definiowania zarówno zasobów, jak i zagrożeń wymaga ścisłej współpracy zespołu wykonawczego z pracownikami firmy, która zleciła przygotowanie tej koncepcji. Można wtedy efektywnie wykorzystać wiedzę i doświadczenie ekspertów zewnętrznych oraz doświadczenie i wiedzę pracowników, ich znajomość firmy, a także jej wrażliwych punktów. Efektem takiego działania będzie wypracowanie optymalnego rozwiązania w kwestii organizacji bezpieczeństwa.

Mając zdefiniowane zasoby i zagrożenia, można określić warunki brzegowe w zakresie wymagań odnośnie do systemów zabezpieczenia technicznego i ochrony fizycznej w sposób adekwatny do wskazanych wcześniej potrzeb. Pozwoli to także na przynajmniej wstępne oszacowanie kosztów, jakie firma będzie musiała ponieść w związku z organizacją systemu bezpieczeństwa.

Jeśli w obiekcie znajdują się już zainstalowane systemy zabezpieczenia technicznego, nie można ich pominąć w pracach koncepcyjnych. Kluczowym zadaniem jest opis ich charakterystyki i ewentualnej przydatności dla nowo projektowanego systemu bezpieczeństwa. Bardzo istotne jest też zwrócenie uwagi na możliwość integracji istniejących systemów z planowanymi za pośrednictwem narzędzia integrującego, jeżeli mają zostać wykorzystane. Charakteryzując i opisując systemy zabezpieczenia technicznego, należy zwrócić uwagę także na personel, który nimi zarządza, a więc służbę ochrony. Trzeba wykazać, czy wszystkie czynności związane z sygnalizacjami systemów mają odzwierciedlenie w odpowiednich procedurach postępowania pracowników ochrony fizycznej. Dokumentacja regulująca zakres odpowiedzialności służby ochronnej i pracowników, których system ma chronić, lub wykazanie braku takiej dokumentacji jest równie ważnym elementem części analitycznej koncepcji, co zdefiniowanie zasobów i zagrożeń.

Analiza czy też swojego rodzaju audyt powinien kończyć się jasną dla użytkownika końcowego, np. zarządu firmy, oceną stanu bezpieczeństwa oraz rekomendacjami zespołu ekspertów, które wytyczą tryb postępowania w celu podniesienia czy też zapewnienia stanu bezpieczeństwa w danej organizacji.

Szczegółowo określone potrzeby organizacji w zakresie bezpieczeństwa pozwalają rozpocząć rzeczywiste prace nad przygotowaniem wzorcowej koncepcji zabezpieczenia, przyjęcie wymaganej strategii i jej realizację. Zespół ekspertów przedstawia klientowi optymalne rozwiązanie, jakie trzeba zastosować na wskazanym przez niego obszarze.

Etap prac analitycznych jest często pomijany i koncepcję zabezpieczenia buduje się na zainstalowanym i wdrożonym systemie.

Do najważniejszych elementów tej części zadania należy określenie formy i zakresu dokumentacji niezbędnej do prawidłowego funkcjonowania przedmiotowego modelu bezpieczeństwa, a więc wszelkich przepisów wewnętrznych regulujących zadania i obowiązki całego personelu uczestniczącego w systemie bezpieczeństwa firmy, takich jak instrukcje ochrony obiektów, instrukcje ruchu osobowego i materiałowego, bezpiecznej eksploatacji i administracji systemami zabezpieczenia technicznego itp. Ponadto zostaną wskazane systemy niezbędne do podniesienia poziomu zabezpieczeń wraz ze szczegółowymi wymaganiami dotyczącymi ich instalacji i eksploatacji. Określenie szczegółowych wymagań odnośnie do systemu znacznie ułatwi inwestorowi sporządzenie dokumentacji przetargowej, takiej jak Szczególne Istotne Warunki Zamówienia.

Gotowy produkt, jakim jest koncepcja zabezpieczenia danej organizacji, powinien w podsumowaniu zawierać opis sposobu wdrożenia wzorcowego modelu bezpieczeństwa wraz z szacunkowym jego kosztem, aby np. zarząd firmy zlecającej wykonanie koncepcji mógł ująć ten koszt w strategii budżetowej firmy.

Warto także zadbać, aby integralną częścią koncepcji był przykładowy opis przedmiotu zamówienia czy też program funkcjonalno-użytkowy.

Odwołując się do swojego długoletniego doświadczenia w branży, jestem przekonany, że zaangażowanie i poświęcenie czasu lub środków finansowych na sporządzenie koncepcji dotyczącej rozwiązań stosowanych w systemie bezpieczeństwa organizacji znacznie pomoże w określeniu strategii i budowie, a także późniejszej eksploatacji. W zakresie systemów zabezpieczenia natomiast zatwierdzona przez kierownictwo firmy koncepcja może posłużyć jako zestaw szczegółowych wytycznych do opracowania dokładnych projektów wykonawczych poszczególnych systemów.

BIO

Maciej Jaszczuk
Członek Zarządu POLALARM, naczelnik Wydziału Bezpieczeństwa Fizycznego Biura Bezpieczeństwa i Spraw Obronnych PKP PLK SA.

C&C PARTNERS
17 Stycznia 119, 121, 64-100 Leszno
tel. 65 525 55 00
info@ccpartners.pl

Najważniejszym rynkiem jest Polska

Z okazji 25-lecia istnienia firmy C&C Partners o dotychczasowych sukcesach i planach na przyszłość rozmawiamy z prezesem Zarządu Arturem Hejdyszem.

25 lat działania firmy to dobry moment na podsumowania. Proszę powiedzieć, z czego w historii C&C Partners jest Pan szczególnie dumny?
Naszym największym sukcesem jest to, że udawało nam się dostosowywać do wciąż zmieniającego się otoczenia biznesowego i technologicznego. Dumni jesteśmy z tego, że jako firma dołożyliśmy swoją cegiełkę do wielu kluczowych i prestiżowych projektów, choćby w zakresie tworzenia infrastruktury sieci telekomunikacyjnych, dawniej miedzianych, obecnie światłowodowych w całej Polsce czy systemów zabezpieczeń w tak znaczących inwestycjach jak Pomorska Kolej Metropolitalna, budynki Q22 czy Sky Tower, a także największe stadiony sportowe, szpitale i uczelnie. Wykonujemy naszą pracę z pasją, dzięki czemu zaufało nam liczne grono klientów, którzy stali się naszymi partnerami. Serdecznie im za to dziękuję. Dumni jesteśmy także z zespołu, który udało nam się stworzyć i którego praca pozwoliła na osiągnięcie wszystkich naszych sukcesów.

Jakie były pierwsze sukcesy C&C Partners?
Firma C&C Partners powstała w 1992 r., by dostarczać klientom nowoczesne rozwiązania telekomunikacyjne. W miarę szybko nawiązaliśmy współpracę z ówcześnie działającą na rynku firmą ADC KRONE, a w 1994 r. zostaliśmy jej generalnym przedstawicielem. Z dzisiejszej perspektywy przekonanie klientów do ustandaryzowania swoich sieci telekomunikacyjnych w oparciu o sprzęt KRONE było dla nas kluczowym elementem sukcesu i spowodowało, że praktycznie w każdej szafie czy na każdym słupku telekomunikacyjnym pojawiły się dystrybuowane przez nas produkty. To doświadczenie dawało nam paliwo do dalszego rozwoju. Zaczęliśmy rozszerzać ofertę o okablowanie strukturalne i systemy zabezpieczeń.

Kolejnym przełomem był rok 1998.
Rzeczywiście, wtedy C&C Partners przystąpiło do holenderskiego holdingu TKH. TKH był nie tylko inwestorem finansowym, zapewniał nam również dostęp do nowoczesnych technologii i potencjału produkcyjnego. Dzięki temu z roli dystrybutora innych producentów staliśmy się częścią handlową firm, które działały w ramach holdingu na całym świecie. Zrobiliśmy ogromny krok i uzyskaliśmy wielkie wsparcie, które procentuje do dzisiaj.

Jak dziś holding TKH jest obecny na rynku polskim?
Oprócz działalności związanej z wprowadzaniem na nasz rynek produktów sektora telekomunikacyjnego czy systemów bezpieczeństwa, C&C Partners zawsze było swojego rodzaju inkubatorem i ambasadorem TKH w Polsce. Bardzo mocno zabiegaliśmy o to, aby wiele możliwości, jakie holding posiada, znajdowało swoje odzwierciedlenie także u nas. Obecnie w ramach TKH pracuje w Polsce ponad

400 osób w firmach C&C Partners, C&C Technology, TKH Kabeltechniek, VMI Polska oraz TKD Polska. Dzisiaj TKH w regionie Leszna należy do głównych pracodawców. Rozbudowujemy swoje fabryki, a perspektywy są bardzo obiecujące. Także dzisiaj nasza sprzedaż w większości opiera się na technologiach własnych grupy TKH. Pozycjonujemy się na rynku jako producent tych wszystkich systemów, z dostępem do produktów oraz z szerokim zakresem wiedzy technologicznej i inżynieryjnej niezbędnej, aby te produkty z sukcesem wdrażać już u klientów.

Które branże są kluczowymi odbiorcami rozwiązań C&C Partners?
Naszą działalność koncentrujemy na rynkach, na których jest największy potencjał wzrostu. To m.in. telekomunikacja, rozwiązania budynkowe, parkingi czy przemysł wizji maszynowej. Niemniej ponieważ działamy w bardzo dynamicznym otoczeniu, nieustannie staramy się do niego dostosować. Dzisiaj duża część firmy działa w sektorze telekomunikacji oraz inwestycjach związanych z budową sieci szerokopasmowych. Jednocześnie naszym celem handlowym są wszystkie instalacje budynkowe, zwłaszcza te obiekty, które wymagają większego poziomu bezpieczeństwa. Jeśli klient nie zadowala się standardowym systemem zabezpieczeń, oczekuje dopasowania rozwiązań do swoich – często specyficznych – wymagań, to właśnie w tym upatrujemy naszej przewagi i na takich rynkach chcemy działać.

Jaka jest dziś pozycja C&C Partners na rynku?
Bardzo dobra. Jesteśmy jednym z liderów zintegrowanych systemów zabezpieczeń na rynkach polskim, litewskim, łotewskim i estońskim. Dokładamy starań, aby w najbliższym czasie umocnić naszą pozycję, jednocześnie analizujemy i rozpoczynamy działania w innych krajach Europy Wschodniej, w których planujemy stać się liderem rynków wertykalnych z dedykowanymi dla nich technologiami. Aktywnie korzystamy z zasobów w ramach grupy. Jesteśmy trzecią najszybciej rosnącą firmą w Europie w zakresie systemów zabezpieczeń wg rankingu TOP 50 branży security na świecie opublikowanej przez miesięcznik „a&s International".

Z jakich krajów pochodzą klienci C&C Partners? Gdzie upatrujecie większych potencjałów – w Polsce czy za granicą?
Bez dwóch zdań naszym najważniejszym rynkiem jest Polska. Niemniej staramy się dywersyfikować działalność firmy w sensie produktowym i geograficznym. Chcemy, aby w naturalny sposób obie te sfery się rozwijały. Liczę, że w ciągu 3–4 lat około 30% obrotu firmy będzie stanowiła sprzedaż zagranicą, ale mam też nadzieję, że wzrośnie wartość globalna sprzedawanych przez nas rozwiązań.

Czy firma planuje wejście na kolejne rynki?
W tym roku podjęliśmy już takie działania, weryfikując z naszymi partnerami i dostawcami możliwość rozszerzenia współpracy. Interesujemy się krajami leżącymi na południe od Polski, ale wierzymy też w potencjał biznesowy Ukrainy.

Porozmawiajmy jeszcze o systemach zabezpieczeń i technologii. Jak ocenia Pan zmiany w tej branży?
Przede wszystkim rynek zabezpieczeń w tej chwili jednoznacznie podąża w kierunku IP. Tutaj nie ma odwrotu, a tradycyjny rynek zabezpieczeń należy już do przeszłości. Na nasze urządzenia w zakresie bezpieczeństwa patrzy się teraz jak na kolejne urządzenia w sieci. I to jest dominujący trend, najważniejszy. W dużym stopniu zmienia się telewizja dozorowa. To największy rynek w zakresie zabezpieczeń – tu widać odejście od klasycznego systemu telewizji analogowej, w którym człowiek weryfikuje to, co się dzieje na obrazie, w stronę analityki, a operator podejmuje reakcję dopiero po wskazaniu przez system, że pojawiły się – zdefiniowane uprzednio – anomalia w obrazie. Taki kierunek wyznacza rynek pracy, wzrost zatrudnienia i rosnąca w bardzo szybkim tempie liczba urządzeń, które trzeba obsługiwać.

Jakie błędy klienci popełniają najczęściej podczas zakupu systemów zabezpieczeń?
Generalnie klienci zapominają, że kluczem – zanim zacznie się jakiekolwiek prace – jest przemyślany sposób budowy systemu bezpieczeństwa w danym obiekcie, ponieważ w przypadku systemów zabezpieczeń późniejsza „optymalizacja" zazwyczaj wiąże się z tym, że traci się wiele funkcji. Ważne są też modułowość pozwalająca rozbudowywać systemy oraz wybór takiej technologii, która pozwoli bezpiecznie rozwijać go w przyszłości. Dlatego partner biznesowy, z którym realizuje się system zabezpieczeń, musi być zaufany. Trzeba móc liczyć na niego w przyszłości.
Istnieją różnego rodzaju instrumenty, które pozwalają zabezpieczyć interes zamawiającego. Przykładowo z zasady oprogramowanie jest oferowane na licencji i klient nie może go samodzielnie rozwijać, ale jeśli chce strategicznie zabezpieczyć swoje interesy i mieć dostęp do kodu źródłowego, może wykupić usługę poprzez kancelarie notarialne, w których zdeponowany jest kod źródłowy danego oprogramowania. Jeśli zajdą określone wydarzenia, może wejść w posiadanie software'u i rozwijać go we własnym zakresie. Jesteśmy jedną z niewielu firm oferujących tego rodzaju usługę.

Jakie wyzwania stawia sobie firma na najbliższe lata? I jakie plany ma C&C Partners?
Dotrzymanie kroku konkurencji technologicznej. Dzisiaj to jest niesamowicie szybki rozwój, produkty są kreowane w dużej mierze przez klientów, adaptuje się je do ich potrzeb. Wyzwaniem jest też rozwijanie zespołu inżynieryjnego, który daje przewagę we wszystkich projektach, które realizujemy.
Plany? Na pewno skupimy się na wybranych strategicznych rynkach, na których połączenie produktów z naszego portfolio i wiedzy inżynieryjnej stanowi największą wartość dla klienta. Będziemy też na bieżąco weryfikować te rynki. Bardzo ważny dla nas jest również rozwój w sąsiednich krajach.

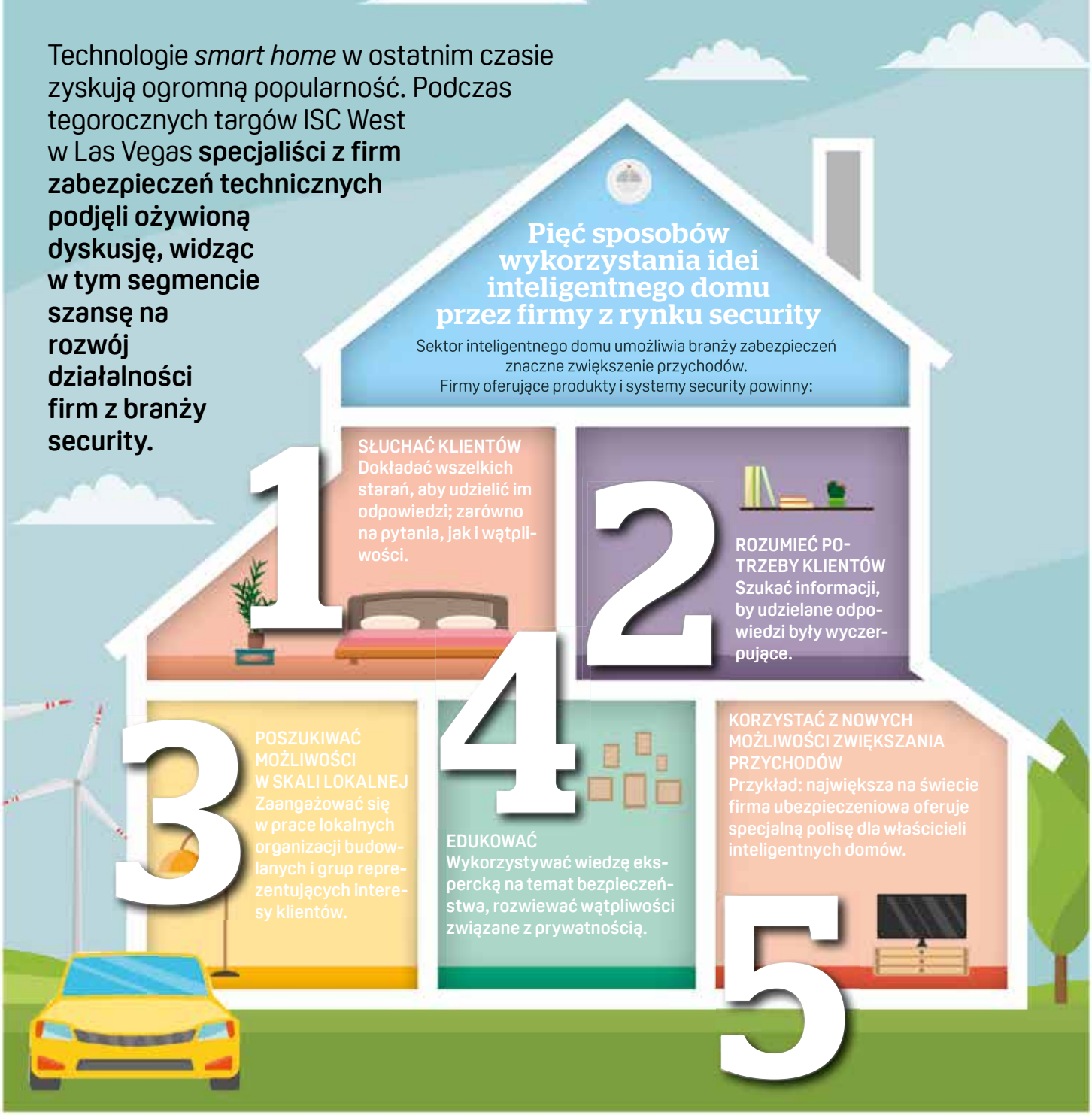
BIO

Artur Hejdysz – prezes Zarządu spółki C&C Partners. Związany z firmą od ponad 20 lat. Był m.in. dyrektorem ds. rozwoju, dyrektorem handlowym oraz dyrektorem operacyjnym spółki. Od 2010 r. pełnił funkcję członka Zarządu w C&C Partners, a w roku 2012 został prezesem należącej do grupy C&C Partners spółki C&C Technology. Funkcję prezesa Zarządu w C&C Partners objął w 2017 r.

Technologie inteligentnego domu

motorem rozwoju rynku security

Technologie *smart home* w ostatnim czasie zyskują ogromną popularność. Podczas tegorocznych targów ISC West w Las Vegas **specjaliści z firm zabezpieczeń technicznych podjęli ożywioną dyskusję, widząc w tym segmencie szansę na rozwój działalności firm z branży security.**



Obszar zabezpieczeń i ochrony ma największy potencjał ofertowy na rynku *smart home,* tymczasem firmy z branży security nie wykorzystują w pełni możliwości, jakie otwiera przed nimi ten sektor. Podczas tegorocznych targów ISC dyskutowali o tym Tom Kerber (Parks Associates), Jeremy McLerran (Qolsys) oraz Avi Rosenthal (IoT Consulting). Omówili oni możliwości, na jakie powinni zwrócić uwagę dostawcy rozwiązań z dziedziny zabezpieczeń, by pojawiające się technologie inteligentnego domu wykorzystać do rozwoju własnej działalności.

Przesunięcie środka ciężkości

Produkty inteligentnego domu to oferta nowa na rynku masowym. Tom Kerber uważa, że we wczesnym stadium rozwoju rynku strategia integracji wertykalnej była bardziej skuteczna. *Oznacza to tyle, że dotychczas jedna firma kontrolowała wszystkie aspekty działalności* – mówi T. Kerber. Z czasem, w obliczu wprowadzania na rynek nowych produktów, które adaptuje się w coraz większej liczbie, użytkownicy będą oczekiwać ich kompatybilności z innymi systemami, w tym z systemami zabezpieczeń. *Odchodzi się od podejścia integracji wertykalnej w stronę podejścia bardziej dojrzałego, które pozwala na integrację większej liczby produktów w ekosystemie* – wyjaśnia T. Kerber. – *Jeśli miałbym wskazać wyzwania w tym zakresie, ujmę to następująco: zaczynasz z systemem integracji wertykalnej, ponieważ zapewnia to wyjątkowe doznania użytkownika, tzw. user experience. Pytanie: kto przesunie środek ciężkości, nadal zachowując ten wyjątkowy user experience?* T. Kerber uważa, że firmy spoza branży zabezpieczeń, zajmujące się inteligentnymi domami i próbujące znaleźć swoje miejsce na rynku, mają doświadczenie w kreowaniu wysokiej jakości *user experience.* Firmy z branży security są otwarte na aplikacje i produkty, lecz w obszarze *user experience* muszą jeszcze sporo zrobić. Gdy produkty stają się coraz powszechniejsze, a wraz z tym rośnie gałąź usług interaktywnych, ci sami klienci coraz częściej sięgają po produkty z obu tych obszarów. W tej sytuacji w rozwoju biznesu sprawą kluczową będzie odejście od modelu integracji wertykalnej.

Przezwyciężenie trudności związanych z rozwojem

Jak podkreśla J. McLerran, branża zabezpieczeń będzie się rozwijać dzięki technologiom inteligentnego domu, jeśli poradzi sobie z trzema kwestiami: wygodnictwem użytkownika, aspektem *smart* oraz rekomendacją. Im łatwiejsza osługa urządzenia, tym szybsza jego akceptacja na rynku. *Jeśli użytkownicy otrzymają aplikację prostą w obsłudze, będą z niej korzystać bez przerwy. To samo dotyczy panelu bezpieczeństwa czy panelu sterującego w domu* – wyjaśnia J. McLerran. – *Im łatwiejsza obsługa danej funkcji, tym częściej jest ona wykorzystywana. Z kolei bardziej skomplikowana wymaga zalogowania się do sieci, rejestracji wielu elementów, tworzenia licznych zasad, a to zniechęca do jej używania.*

W dużej mierze jest to kwestia decyzji, czy system ma być instalowany i konfigurowany przez technika, czy też technik powinien go tylko zainstalować. Pierwsza opcja oznacza wyższy poziom *user experience,* ale wtedy technik spędzi w terenie więcej czasu. Opcja druga pozwoli uzyskać wyższy dochód. – *Mając na względzie własną działalność, trzeba wybrać optymalny sposób. Zamiast wykonywać kompleksową konfigurację, wystarczy pokazać użytkownikowi, jak ma się zalogować i jakie powinien wykonać działania, żeby później w razie potrzeby samemu doprecyzować ustawienia. Ten czynnik określający wygodnictwo użytkowników jest bardzo ważny* – podkreśla J. McLerran.

Przejdźmy do aspektu *smart*. Każde urządzenie podłączone do sieci jest obsługiwane przez aplikację, natomiast urządzenie *smart* stanowi element inteligentnego ekosystemu. To istotna różnica. *Dysponujesz świetną siecią urządzeń Z-Wave współpracujących ze sobą w ramach ogromnego ekosystemu, ale gdy umieścisz je poza systemem zdolnym tym wszystkim sterować... Idea tworzenia ekosystemu urządzeń jest następująca: jeżeli masz ekosystem, który użytkownicy polubili i będą go udostępniać znajomym, to tym samym będą go polecać innym, ale też zechcą coraz więcej dla siebie* – mówi J. McLerran.

> Firmy z rynku security nie mogą kierować się dewizą: „Jeżeli nie mogę tego sprzedać, nie będę tego wspierać". Wręcz przeciwnie, powinny traktować nowe technologie jako szansę na rozwój.

Innym sposobem na przyspieszenie rozpowszechniania i rozbudowy systemu są zmiany w programie rekomendacji, np. zastosowanie motywatora w postaci darmowych *upgrade'ów* zamiast bezpłatnego miesięcznego abonamentu. *Upgrade'y* potrafią zainteresować użytkownika usługami, przedstawiając jednocześnie nowe produkty, a tym samym zwiększając szansę rekomendowania ich kolejnym osobom.

Przejście do kolejnego etapu – naśladowania

Nowe technologie są obecnie bardziej przystępne cenowo niż 20 lat temu, co przekłada się również na ich szybszą adaptację przez użytkowników. Jako przykład mogą posłużyć urządzenia przetwarzające mowę, takie jak Amazon Alexa. Amazon sprzedał 8 mln urządzeń Alexa w ciągu trzech lat. Według A. Rosenthala z IoT Consulting znaczny udział w ich doskonałej sprzedaży miała prostota obsługi.

Tego typu technologie otwierają nowe możliwości przed sprzedawcami usług bezpieczeństwa. Dostawcy nie mogą kierować się dewizą: „Jeżeli nie mogę tego sprzedać, nie będę też tego wspierać". Wręcz przeciwnie, powinni traktować nowe technologie jako szansę na rozwój. *Wspieranie urządzenia, bycie jego „ambasadorem", pomoc ludziom w zrozumieniu jego zalet i wad: oto sposób na zwiększenie przychodu, a tym samym pozyskanie kolejnych klientów. To także możliwość monitorowania domów i pomoc w zrozumieniu niektórych technicznych, politycznych i społecznych bolączek* – podsumowuje A. Rosenthal.

Rozwój biznesu

Około 85% ludzi nie wie, na czym polega idea inteligentnego domu. Tom Kerber uważa, że najlepiej może ją przybli-

żyć właśnie branża security, z bardziej indywidualnym podejściem ułatwiającym zrozumienie. Należy również pamiętać, że na etapie instalacji 99% klientów nie decyduje się na kompleksowy zakup wszystkich elementów. Dokonują wyboru sprzętu i usług na podstawie budżetu i priorytetów. *Po upływie trzech do sześciu miesięcy mogą już być gotowi na więcej* – twierdzi J. McLerran. – *Jeśli zamontujesz system i później już nie skontaktujesz się z klientem, tracisz możliwość wprowadzenia dodatkowych usług, zwiększenia intensywności użytkowania oraz pomnożenia własnych przychodów. Nie utrzymując kontaktu z klientami, tracisz wiele możliwości, które są na wyciągnięcie ręki. To właśnie od dostawców rozwiązań zabezpieczeń zależy, czy z nich skorzystają.*

AMERYKA PÓŁNOCNA I EUROPA LIDERAMI NA RYNKU *SMART HOME*

Firma Transparency Market Research, zajmująca się badaniami rynku, opublikowała prognozy dotyczące globalnego rynku smart home na lata 2017–2025. Według raportu Ameryka Północna ma pozostać liderem w branży, a obszar Azji i Pacyfiku odnotuje wyższy wzrost niż pozostałe obszary. Jako czynniki napędzające globalny rozwój rynku inteligentnego domu wymieniono poziom wykorzystywania Internetu, dostępność szybkich łączy oraz spadek cen procesorów i czujników. Z perspektywy klienta konieczność oszczędnego korzystania z energii będzie stymulować sprzedaż w kategorii inteligentnych termostatów i rozwiązań do zarządzania energią.

W raporcie podano, że globalny rynek rozwiązań dla inteligentnego domu wzrośnie z poziomu 30 mld dol. w roku 2016 do 97,6 mld dol. w roku 2025, osiągając skumulowany roczny wskaźnik wzrostu CAGR wynoszący 14,6%. W ujęciu regionalnym Ameryka Północna będzie liderem pod względem udziału w rynku ze wskaźnikiem 38,7% w 2016 r. Wspierany przez Europę, czyli drugi największy rynek smart home, świat zachodni stworzy najszersze możliwości producentom rozwiązań dla inteligentnego domu.

RYNEK *SMART HOME* W WIELKIEJ BRYTANII DO 2021 R. BĘDZIE RÓSŁ W TEMPIE 24% ROCZNIE

Według raportu agencji Technavio zajmującej się analizą rynku branża M2M *(Machine to Machine)* inteligentnego domu w Wielkiej Brytanii odnotuje w latach 2017–2021 wzrost na poziomie 24% rocznie. M2M w obszarze inteligentnego domu jest definiowane jako technologia oparta na sieci wewnętrznej, posiadająca inteligentny system sterowania oraz system automatyki domowej.
Sześć najważniejszych obszarów zastosowań w Wielkiej Brytanii stanowią systemy do zarządzania energią i klimatyzacji, urządzenia AGD, sterowanie oświetleniem, urządzeniami rozrywki domowej, bezpieczeństwo i kontrola dostępu oraz systemy opieki zdrowotnej. Wymienia się trzy czynniki mające wpływ na wzrost rynku M2M w branży *smart home.* Są to: wzrost liczby inteligentnych mierników, częstsze korzystanie z termostatów oraz adaptacja technologii w chmurze. Inteligentny miernik połączony z interfejsem *in-home display,* czyli urządzenie z wyświetlaczem lub aplikacja służąca do odczytu danych z inteligentnych mierników i do sterowania zarządzaniem energią, przekazuje w czasie rzeczywistym dane o zużyciu gazu i energii elektrycznej. Te inteligentne mierniki umożliwiają klientom monitorowanie urządzeń pobierających prąd za pomocą systemów zarządzania energią i sterowanie nimi. Stosowanie tej technologii zamiast rozwiązań tradycyjnych pozwala wyeliminować zużycie energii w godzinach obowiązywania stawek szczytowych, a także pomaga zapobiegać awariom zasilania.

RYNEK *SMART HOME* M2M W WIELKIEJ BRYTANII *(źródło: technavio)*

KLUCZOWY TREND
Wykorzystanie „kieszonkowych" dronów do zastosowań *personal security.*

TO NAPĘDZA RYNEK
Oszczędności dzięki zastosowaniu efektywnego monitorowania.

ŚWIADOMOŚĆ KONSUMENTÓW
Wzrost liczby instalacji inteligentnych mierników.

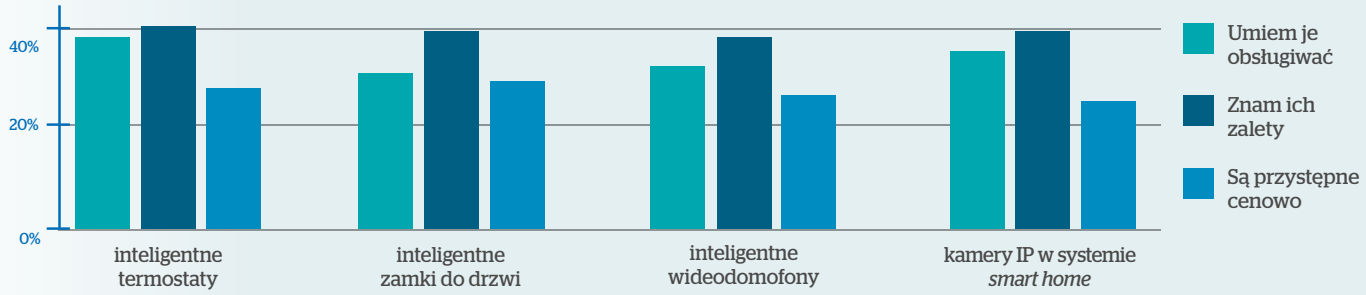
DOBRE PROGNOZY
Wzrost rynku *smart home* o ponad 23 proc. do 2021 r.

W USA 33% GOSPODARSTW DOMOWYCH Z DOSTĘPEM DO INTERNETU KORZYSTA Z URZĄDZEŃ *SMART HOME*

Według badań Parks Associates około jednej trzeciej amerykańskich gospodarstw domowych mających dostęp do Internetu szerokopasmowego korzysta z urządzeń inteligentnego domu. Jeszcze większy odsetek mieszkańców dostrzega wartość w tego typu urządzeniach, włączając w to inteligentne zamki, dzwonki do drzwi z kamerą wideo i kamery sieciowe. Wskazuje to na duże możliwości poprawy stopnia wykorzystywania urządzeń w inteligentnym domu i ich rozpowszechniania.

Ponad jedna czwarta gospodarstw korzysta z co najmniej jednego inteligentnego produktu, jednak tylko 12% posiada system inteligentnego domu – mówi T. Kerber, dyrektor ds. strategii IoT w firmie Parks Associates. W opracowaniu przygotowanym przez tę firmę (*Inteligentny dom: pogoń za pomysłowymi zastosowaniami*) podano, że prawie 70% właścicieli inteligentnych urządzeń nie podłączyło ich do systemu *smart home,* a jedynie u 35% zostały one z nim zintegrowane.

URZĄDZENIA INTELIGENTNE W AMERYKAŃSKICH GOSPODARSTWACH DOMOWYCH Z DOSTĘPEM DO INTERNETU



WCZESNA DOJRZAŁOŚĆ RYNKU INTELIGENTNEGO DOMU

Rynek inteligentnego domu rośnie w szybkim tempie. Z etapu wczesnego przystosowania przechodzi do poziomu wczesnej dojrzałości – podkreśla T. Kerber, dyrektor ds. strategii IoT w firmie Parks Associates. – *Sterowanie głosem i automatyzacja oparta na funkcjach analityki przyczyniają się do zwiększenia poziomu user experience, przyspieszając zarazem dynamikę rynku inteligentnego domu* – dodaje.

Jak podano w raporcie Parks Associates, ponad 100 mln gospodarstw domowych spośród ogólnej liczby 117 mln w USA nie korzysta z inteligentnych gadżetów. Stopień adaptacji jest niski, choć firma analityczna dostrzega w tym zakresie potencjał. Inteligentne oświetlenie stanie się najpowszechniejszym inteligentnym gadżetem w domu – obecnie zajmuje drugie miejsce pod względem zużycia energii, tuż za systemami ogrzewania, wentylacji i klimatyzacji. Według prognoz do 2020 r. ok. 50 mln gospodarstw domowych w USA będzie używać co najmniej jednej inteligentnej żarówki. Użytkownicy poszukują łatwiejszych sposobów sterowania oświetleniem przy jednoczesnym oszczędzaniu poboru energii.

W USA 55% gospodarstw domowych jest zainteresowanych sterowaniem głosowym swoich urządzeń inteligentnego domu.

Technologia sterowania głosem nabiera przyspieszenia w świecie aplikacji *smart home,* co zauważyli również klienci. Według analityków Parks Associates 55% gospodarstw domowych w USA z dostępem do Internetu wyraża chęć sterowania urządzeniami inteligentnego domu i gadżetami rozrywkowymi za pomocą głosu. Odsetek ten jest wyższy w gospodarstwach domowych używających inteligentnych żarówek, programowalnych termostatów, inteligentnych detektorów dymu lub tlenku węgla czy inteligentnych urządzeń do otwierania bram garażowych.

W Stanach Zjednoczonych cyfrowi „asystenci głosowi" spotkali się z bardziej pozytywnym przyjęciem niż inne nowinki ze świata elektroniki. Według opublikowanego w marcu br. raportu Parks Associates stopień adaptacji asystentów głosowych przez gospodarstwa z dostępem do Internetu szerokopasmowego wzrósł z 5% w IV kwartale 2015 r. do 12% w IV kwartale 2016 r.

W raporcie podano, że zapowiedzią zwiększenia tempa rozwoju aplikacji i wprowadzania przez dystrybutorów nowych produktów na rynek był wzrost świadomości i stopnia adaptacji cyfrowych asystentów głosowych, takich jak Amazon Alexa czy Google Assistant.

HIKVISION EUROPE BV
Dirk Storklaan 3, 2132PX – Hoofdorp, Holandia
tel. +48 726 070 411
https://ezviz.eu/pl/

Bezpieczeństwo, wygoda i komfort
System smart home Ezviz

Zmieniające się potrzeby użytkowników na rynku mieszkaniowym i małych firm przyczyniają się do dynamicznego rozwoju sektora *smart home***.** Mieszkańcy dostrzegają zalety wyposażenia domu w inteligentne urządzenia sterowania oświetleniem, roletami czy ogrzewaniem wraz z systemem dozoru wizyjnego i alarmowym. Jednak wartość dla użytkownika stanowi inteligentne współdziałanie tych systemów, a nie niezależne ich funkcjonowanie.

W ten trend doskonale wpisuje się Ezviz – nowa marka biznesowa grupy Hikvision, największego producenta systemów monitoringu wizyjnego na świecie, która powstała na bazie kompetencji i wiedzy eksperckiej Hikvision. Wykorzystując innowacyjne technologie, tworzy rozwiązania umożliwiające wizualną łączność użytkownika z jego domem i pracą. Nowa marka skupia się na trendach na rynku *smart life*, głównym celem rozwiązań Ezviz jest zapewnienie bezpieczeństwa, wygody i komfortu życia użytkowników.

Podstawową grupą produktową w ofercie Ezviz jest linia kamer dozorowych. Są w niej modele o rozdzielczości 720p i 1080p, w wersji transmisji wizji przez sieć Wi-Fi oraz z transmisją przewodową i zasilaniem PoE. Część oferty kamer to modele zaspokajające codzienne potrzeby użytkowników – monitorujące sen dziecka czy osoby wymagającej opieki lub pozwalające użytkownikowi pozostać w kontakcie z bliskimi podczas wyjazdów. Kamery te umożliwiają dwukierunkową komunikację audio wraz z podglądem obrazu z kamery na ekranie smartfonu. Użytkownik może również otrzymać powiadomienie na smartfon o wykrytym przez kamerę ruchu, niezależnie czy znajduje się w sąsiednim pomieszczeniu i monitoruje dziecko, czy jest w podróży i otrzymuje informacje o powrocie dzieci ze szkoły (wystarczy, że smartfon ma połączenie z Internetem). Kamery są wyposażone w porty microSD do rejestracji lokalnej oraz promienniki podczerwieni o kilkumetrowym zasięgu do dozoru w nocy. Bardzo wygodnym rozwiązaniem są modele z podstawą magnetyczną, np. Mini Plus, które w połączeniu z szerokim kątem widzenia 116° (w przypadku Mini Plus) zapewniają użytkownikowi dużą swobodę i elastyczność co do miejsca montażu kamery.

Niektóre modele są również wyposażone w typowe dla telewizji dozorowej funkcje, takie jak WDR i mechaniczny filtr podczerwieni.
Ezviz oferuje także modele bliższe rozwiązaniom profesjonalnym, takie jak kamera *bullet* C3S czy wandaloodporna kamera C4S. Generują one strumień 25 kl./s w rozdzielczości 1920 x 1080, występują w wersji Wi-Fi lub z transmisją przewodową oraz zasilaniem PoE. Promienniki podczerwieni o zasięgu do 30 m, klasa szczelności obudowy IP66 i zakres temperatury pracy od -30°C do 60°C pozwalają na swobodne ich stosowanie na zewnątrz. Ponadto kamera C4S jest wandaloodporna – ma klasę odporności mechanicznej IK10.
Obraz z kamery może być rejestrowany lokalnie na kartach microSD o pojemności maksymalnej do 128 GB lub rejestratorach X3C. Bezprzewodowy rejestrator sieciowy X3C obsługuje do 8 kamer Ezviz przewodowych lub bezprzewodowych. Jest wyposażony w cztery porty Ethernet do podłączenia kamer przewodowych i dwuzakresowe Wi-Fi (2,4 oraz 5 GHz). Rejestrator obsługuje dysk twardy 3,5" o maksymalnej pojemności 6 TB. Zarejestrowane zdarzenia użytkownik może oglądać z poziomu aplikacji na telefonie komórkowym lub komputerze PC.
Koncepcja monitoringu Ezviz zakłada intuicyjność i elastyczność rozwiązań dla użytkownika końcowego. Instalację kamer przeprowadza się w kilku prostych krokach. Wystarczy pobrać aplikację Ezviz mobile na smartfon, założyć konto i po zeskanowaniu kodu QR zakupionej kamery natychmiast uzyskuje się połączenie. Intuicyjna aplikacja na smartfonie umożliwia użytkownikowi łączność z domem czy miejscem pracy z dowolnego miejsca w zasięgu Internetu i obserwację obrazu z aż czterech kamer jednocześnie. W przypadku niepokojącego zdarzenia może on doraźnie zapisać zdjęcie lub film na smartfonie. Aplikacja pozwala też przybliżyć obraz (cyfrowy zoom) oraz sterować kamerami obrotowymi. Modele z dwukierunkowym torem audio umożliwiają użytkownikowi prowadzenie rozmowy.
Z kolei oprogramowanie Ezviz Studio na PC pozwala na obserwację obrazu z maksymalnie 25 kamer, a także umożliwia dostęp do wszystkich zaawansowanych ustawień kamer.
Zwrócono także uwagę na bardzo ważny aspekt zachowania prywatności, dlatego wszystkie modele mają tryb prywatności uruchamiany z aplikacji mobilnej. Powoduje on zatrzymanie rejestracji audio i wideo oraz wyłączenie podglądu na żywo.
Uzupełnieniem oferty Ezviz jest eHub A1 wraz z rodziną czujników. To bezprzewodowy koncentrator obsługujący do 32 czujników. Koncentrator jest typowym urządzeniem DIY przeznaczonym dla konsumentów, a informacje uzyskiwane za jego pomocą mają charakter wyłącznie informacyjny do wykorzystywania w systemie Ezviz. eHub A1 komunikuje się z czujnikami w paśmie 868 MHz, a dalsza komunikacja odbywa się przez sieć Wi-Fi. Dzięki zamontowanym czujnikom PIR, zalania wodą czy stanu otwarcia drzwi użytkownik uzyskuje informacje o zdarzeniu: wykryciu ruchu, wejściu do pomieszczenia czy zalaniu pomieszczenia. Informacja ta jest natychmiast przesyłana na aplikację mobilną, a użytkownik może ją zweryfikować dzięki obrazom z kamer. Aplikacja pozwala też powiązać konkretny czujnik z kamerą, a po zainstalowaniu karty microSD w kamerze powiadomienie o zdarzeniu będzie zawierało również krótki materiał wideo umożliwiający zweryfikowanie zdarzenia, w tym również zapis z prealarmu. Zestaw sensorów z koncentratorem bezprzewodowym A1 stanowi kolejny krok Ezviz w kierunku stworzenia kompleksowego rozwiązania *smart home*.
Ezviz duży nacisk kładzie również na kwestie bezpieczeństwa. Transmisja jest szyfrowana, a w celu zalogowania się do konta z poziomu aplikacji mobilnej należy podać login i hasło. Następnie, aby wyświetlić na danym smartfonie lub PC po raz pierwszy obraz z danej kamery, należy dodatkowo podać kod weryfikacyjny kamery.
Rozwiązania dla *smart home* to dzisiaj jeden z najszybciej rozwijających się rynków, wokół którego skoncentrowało się wielu globalnych producentów. Nowo powstała marka Ezviz nie ogranicza się wyłącznie do obszaru dozoru wizyjnego i bezpieczeństwa. Już niebawem będzie oferowała elementy automatyki: sterowania oświetleniem i urządzeniami elektrycznymi oraz wideodomofony, które pozwolą zbudować wszechstronny ekosystem.
Rozwój rynku *smart home* nie pozostanie bez wpływu na branżę zabezpieczeń w segmentach SMB/SOHO/Residential. To z pewnością nowe wyzwania, ale też otwarcie na nowe możliwości rozwoju zarówno firm instalacyjnych, jak i dystrybutorów systemów zabezpieczeń. Decyzja o wejściu na rynek sprzedaży czy instalacji nie jest łatwa, wymaga rozwoju kompetencji w nowych obszarach i poznania funkcjonowania nowego rynku, jednak może przynieść wymierne korzyści. *Smart home* to instalacje niskonapięciowe, w dużej mierze oparte na Wi-Fi, toteż firmy instalacyjne z branży zabezpieczeń z pewnością skorzystają z nowych możliwości.

Kierunki rozwoju kontroli dostępu

Ten rok okazał się dla branży kontroli dostępu pomyślny. Wyniki sprzedaży w wielu regionach poprawiły się, a popyt na rynkach wertykalnych utrzymał tendencję wzrostową. **Wśród dominujących trendów znalazły się uwierzytelnianie mobilne, usługi w chmurze oraz integracja i konwergencja w ramach IoT, umożliwiające klientom zabezpieczenie mienia i usprawnienie działalności.**

William Pao,
a&s International

Ubiegły rok okazał się korzystny dla kontroli dostępu (KD), która inne działy zabezpieczeń technicznych zostawiła w tyle. Według agencji analitycznej Memoori w 2016 r. rynek KD odnotował 10-procentowy wzrost w porównaniu do 4,2% w telewizji dozorowej i 3,6% w systemach sygnalizacji włamania i napadu – to był drugi rok z rzędu z najwyższym tempem wzrostu.

Analitycy IHS Markit podają nieco bardziej zachowawcze dane, utrzymując, że rynek kontroli dostępu wzrósł w zeszłym roku o 6,1% (o 1% mniej niż prognozowano). *Dynamikę spowolniły takie kraje, jak Brazylia, Rosja, kraje Ameryki Łacińskiej, z wyjątkiem Meksyku, a także Chiny ze wzrostem jedynie na poziomie 8,5%* – wyjaśnia Blake Kozak, główny analityk IHS Markit. – *Perspektywy są jednak obiecujące. Dobra koniunktura ekonomiczna i wzrost inwestycji w innowacyjne technologie kontroli dostępu doprowadziły do istotnego rozwoju w tym obszarze.*

Prognozy wskazują, że do roku 2020 rynek kontroli dostępu znajdzie się przed rynkiem systemów sygnalizacji włamania i telewizji dozorowej.

Analizując poszczególne regiony, widać wzrost obrotów w skali globalnej. *Przez pierwsze trzy kwartały 2016 r. najsilniejszy rozwój rynku obserwowano w regionie Azji i Pacyfiku, na drugim miejscu znalazł się region obu Ameryk* – podsumowuje Brad Aikin, szef działu elektroniki dla sektora komercyjnego w Allegion (Irlandia).

W Stanach Zjednoczonych do ogólnego wzrostu w największym stopniu przyczyniły się regiony mocno zaludnione, takie jak stany północno-wschodnie oraz Kalifornia i Teksas – wyjaśnia Larry Reed, prezes amerykańskiej firmy ZKAccess.

Region Europy i Bliskiego Wschodu radził sobie równie dobrze. *Poza granicami USA intensywny popyt na technologię zabezpieczeń biometrycznych obserwowaliśmy przede wszystkim na Bliskim Wschodzie. Z podobną sytuacją mieliśmy do czynienia w krajach Azji i Ameryki Łacińskiej, które z reguły przyswajają nowe technologie szybciej niż Ameryka Północna i Europa* – podkreśla Larry Reed.

Bliski Wschód, Polska, Afryka, Indie i Wietnam to rynki, które w 2016 r. pod względem tempa wzrostu wysunęły się na prowadzenie – zauważa B. Kozak. – *Prognoza dla takich państw jak Stany Zjednoczone i Wielka Brytania, których rynki zabezpieczeń są już dojrzałe, przewiduje w roku 2017 wzrost przekraczający 7%. Perspektywy dla Francji i Niemiec również są bardzo dobre – mówią o wzroście przekraczającym 5%.*

Obawa o bezpieczeństwo pozostaje siłą napędową rozwoju obszaru kontroli dostępu. *Mimo że media potrafią te zjawiska wyolbrzymiać, to trzeba przyznać, że naruszenia bezpieczeństwa oraz przemoc są w dzisiejszym społeczeństwie wciąż obecne. Populacja się zwiększa, rozwija się Internet, z czym wiąże się coraz większa wrażliwość na ataki skierowane przeciwko mieniu i ludziom* – mówi L. Reed. – *Służby ochrony mają pełną świadomość, że muszą inwestować w niezbędne środki zabezpieczeń.*

Największy wzrost zastosowań systemów kontroli dostępu zanotowano w sektorach najbardziej narażonych na zagrożenia i naruszanie bezpieczeństwa, takich jak edukacja i opieka zdrowotna. *Wzrost powyżej 9% w 2016 r. odnotowały rynki edukacji, mieszkaniowy i energetyczny. To był także rok wzrostów (8% w 2016 r.) na rynku ochrony zdrowia* – podsumowuje B. Kozak.

Szczególnie widoczna jest troska o bezpieczeństwo uczniów, pacjentów i pracowników w szkołach i szpitalach. Zagrożenie stanowią nieupoważnione osoby wchodzące na teren placówki, a także pracownicy bez uprawnień, usiłujący dostać się do stref o ograniczonym dostępie, np. do pracowni komputerowych, pomieszczeń księgowych i archiwów, czy obszarów niebezpiecznych, takich jak składowiska odpadów radioaktywnych lub biochemicznych – wyjaśnia L. Reed.

Wg agencji analitycznej Memoori, w 2016 r. rynek kontroli dostępu odnotował 10-procentowy wzrost w porównaniu do 4,2% w telewizji dozorowej i 3,6% w systemach sygnalizacji włamania i napadu.

Trendy technologiczne

Technologie kontroli dostępu – oprócz ochrony mienia i ludzi – znalazły zastosowania w różnych sektorach biznesu, pomagając użytkownikom poprawiać wydajność pracy. Oto dominujące trendy w obszarze kontroli dostępu:

Uwierzytelnianie mobilne

W 2016 r. popyt na technologię uwierzytelnień mobilnych niezmiennie przyspieszał, o czym według B. Kozaka świadczy 4,5 miliona zamówień w skali globalnej. Jednak to w roku 2017 technologia ta naprawdę rozwija skrzydła. *W tym roku jest spodziewany dalszy szybki rozwój, a rozwiązania uwierzytelniające dla urządzeń mobilnych osiągną 200-procentowy wzrost i globalną sprzedaż na poziomie 13,5 mln wysłanych zamówień* – prognozuje B. Kozak.

Pracownikom technologia ta umożliwia logowanie się do zasobów fizycznych lub logicznych za pomocą urządzeń mobilnych, do których mają stały dostęp. Dla przedsiębiorstw uwierzytelnianie mobilne oznacza niższe koszty, bezprzewodowe procesy świadczenia usług oraz oszczędności na kartach i identyfikatorach dostępu. *Zdaniem IHS uwierzytelnianie mobilne cieszy się popularnością ze względu na wszechstronność i ponadczasowość oferowanych rozwiązań. Oferuje zdalne świadczenie usług oraz zintegrowaną infrastrukturę zabezpieczeń w ramach rynków wertykalnych, np. w sektorze motoryzacyjnym, mieszkaniowym czy ochrony zdrowia* – kontynuuje B. Kozak.

Larry Reed z firmy ZKAccess natomiast zwraca uwagę na kilka wad uwierzytelniania mobilnego i proponuje rozwiązania biometryczne jako bardziej praktyczne. *Uwierzytelnianie mobilne działa dopiero po spełnieniu wielu warunków. Bateria musi być naładowana, nadajnik radiowy musi działać, konieczny jest dostęp do Internetu, a użytkownik nie może zapomnieć o zabraniu ze sobą telefonu. Bardziej praktyczną alternatywą dla tradycyjnych zamków, kluczy czy kart jest uwierzytelnianie biometryczne, ponieważ swoich danych biometrycznych nie można zgubić. Nie można ich ukraść, nie potrzebują też zasilania* – konkluduje L. Reed.

Kontrola dostępu jako usługa

Rozwiązanie ACaaS (*Access Control as a Service* – kontrola dostępu jako usługa) także zyskało na znaczeniu i ten trend się

utrzymuje. Agencja Research and Markets w raporcie za rok 2016 prognozuje średni skumulowany roczny wskaźnik wzrostu (CAGR) dla rozwiązań ACaaS w latach 2016-2020 na 24,6%.

Dzięki usłudze ACaaS użytkownik nie musi ponosić kosztu zakupu sprzętu, uzyskując możliwość bezpiecznego dostępu do danych firmy z dowolnej lokalizacji. Może go jednak zniechęcać konieczność uiszczania usługodawcom miesięcznych opłat. Przed podjęciem decyzji o wyborze modelu ACaaS użytkownicy powinni rozważyć wszelkie „za" i „przeciw".

Usługi w chmurze to świetne źródło stałych miesięcznych przychodów dla dystrybutorów i instalatorów. Zapewniają stały dopływ finansów i są pomocne w szacowaniu wartości usługodawcy, gdy ten chciałby sprzedać swoją firmę lub spodziewa się przejęcia. Jeżeli użytkownik końcowy zgadza się na bezterminowe uiszczanie opłat za usługę w chmurze, takie rozwiązanie może mieć wartość zarówno dla dystrybutora, jak i dla klienta – przekonuje L. Reed. – *Wciąż większość użytkowników nie jest przekonana do przechowywania poufnych danych firmowych w chmurze obcej organizacji, ale nie ma nic przeciwko zarządzaniu własnym systemem kontroli dostępu na firmowych komputerach obsługiwanych przez swoich pracowników na terenie firmy. Usługi w chmurze mają więc zarówno zalety, jak i wady w zależności od celów firmy i źródła finansowania, którym może być budżet kapitałowy lub operacyjny. Jeżeli w budżecie kapitałowym brakuje środków na zakup sprzętu, wówczas jedyną opcją nabycia systemu kontroli dostępu może być usługa w chmurze.*

Integracja

W ostatnim czasie większą popularnością cieszy się integracja systemów KD z innymi systemami. *To najważniejszy element rozwoju kontroli dostępu w minionym roku* – akcentuje Mitchell Kane, prezes Vanderbilt Industries. – *Organizacje, chcąc zmaksymalizować inwestycje kapitałowe, powinny poszukiwać otwartych platform umożliwiających współpracę systemu KD z innymi systemami zabezpieczeń, takimi jak telewizja dozorowa, systemy przeciwpożarowe i alarmowe czy analiza obrazów wideo. Oczekuje się, że systemy kontroli dostępu będą zdolne do integracji i wspomagania innych systemów zabezpieczeń oraz usług w danym środowisku, takich jak parkingi, oświetlenie czy telekomunikacja* – dodaje Brad Aikin.

Ze względu na rosnące zapotrzebowanie coraz więcej firm oferuje rozwiązania zintegrowane, proponując użytkownikom więcej opcji. Niezwykle istotny jest interfejs użytkownika, który pozwoli w prosty sposób zarządzać wszystkimi systemami: antywłamaniowym, telewizji dozorowej, kontroli dostępu, zarządzania ruchem gości i monitorowania czasu pracy – podkreśla L. Reed z firmy ZKAccess. – *O takiej integracji systemów różnych producentów często się mówi, natomiast jest ona jeszcze rzadkością, głównie z powodu kosztów lub nieuświadamianych potrzeb jej implementacji. Dlatego dostawcy systemów zabezpieczeń tworzą własne platformy umożliwiające wszystkie te zastosowania.*

Rzut oka na rok 2017

Siła rozpędu, jakiego ostatnio nabrała branża kontroli dostępu, nie osłabł w tym roku ani na rynkach dojrzałych, ani na wschodzących. *Rynki wschodzące utrzymują dotychczasowy trend wzrostowy, zwłaszcza w sprzedaży zamków elektronicznych. Wzrost sprzedaży zamków elektronicznych wyniesie globalnie około 9 procent, do czego najbardziej przyczynią się kraje Europy Wschodniej i Afryki z szacowanym wzrostem rzędu 17% w 2017 r.* – twierdzi B. Kozak.

Trendy rozwojowe będą się wiązać z rozszerzeniem zastosowań kontroli dostępu. *Dostawcy i integratorzy rozwiązań KD w 2017 r. umocnią swoją pozycję w dziedzinach technologii informatycznych i cyberbezpieczeństwa dzięki coraz bardziej kompleksowym wdrożeniom systemów technicznej i logicznej kontroli dostępu, a także stosowaniu rozwiązań end-to-end* – kontynuuje B. Kozak. – *IHS stoi na stanowisku, że w ciągu najbliższych miesięcy wzrośnie zainteresowanie systemami biometrycznymi, usługami w chmurze i uwierzytelnianiem mobilnym, a wiele obowiązujących w Europie ograniczeń dot. rozwiązań biometrii i w chmurze zostanie zmodyfikowanych.*

Klienci nadal będą wybierać te technologie, które zwiększają zwrot z inwestycji, bezpieczeństwo i wygodę, w tym aplikacje mobilne i rozwiązania biometryczne. W ciągu najbliższych kilku lat preferowaną technologią identyfikacji użytkownika stanie się rozpoznawanie twarzy – prognozuje L. Reed.

W najbliższym roku wzrośnie zainteresowanie systemami biometrycznymi, usługami w chmurze i uwierzytelnianiem mobilnym, a wiele obowiązujących w Europie ograniczeń dot. rozwiązań w chmurze i biometrii zostanie zmodyfikowanych.

Perspektywy rozwoju

Ubiegły rok okazał się dla branży kontroli dostępu świetny. Użytkownicy otrzymali do dyspozycji nowe technologie oraz modele biznesowe (np. rozbudowa własnej infrastruktury lub hosting w chmurze). Dystrybutorzy wprowadzają na rynek zintegrowane platformy pozwalające zaspokoić oczekiwania użytkowników co do integracji systemów kontroli dostępu z innymi systemami. Ponadto bardziej oczywista konwergencja kontroli dostępu i *big data* umożliwiają jeszcze głębsze zrozumienie środowiska. Wszystkie te czynniki miały wpływ na zeszłoroczny boom w branży kontroli dostępu i w przyszłości nadal będą napędzać jej wzrost.

IoT ORAZ BIG DATA

Skoro systemy kontroli dostępu migrują do sieci, dane generowane przez komunikujące się urządzenia mogą pomóc użytkownikom poznać preferencje personelu i klientów. Dane zbierane przez moduły kontroli dostępu można wykorzystać do określenia sposobu rozliczania kontrahentów, wskazania przemieszczania się pracowników w obiekcie oraz zapewnienia bezpieczeństwa pracy zdalnej.

Blake Kozak, główny analityk w IHS Markit, utrzymuje, że integrując swoje oprogramowanie biznesowe z oprogramowaniem kontroli dostępu, będzie można np. dokładnie monitorować, jak długo kontrahenci przebywają w budynku. *Np dla zarządzających budynkami urządzenia kontroli dostępu mogą stać się narzędziem pozwalającym lepiej poznać wykorzystywanie biura czy sal konferencyjnych* – mówi B. Kozak. *Może to pomóc w usprawnieniu organizacji budynku, aby była bardziej efektywna pod względem czasu pracy pracowników czy zużycia energii. Urządzenia kontroli dostępu są też w stanie wykryć anomalie w zachowaniu osób przebywających w obiekcie. Dane tego typu mogą posłużyć do zapobiegania różnego rodzaju zagrożeniom.*

Analityk IHS zauważa, że użytkownicy wciąż nie są świadomi wartości, jaką daje konwergencja systemu KD i Internetu Rzeczy (IoT). *Mimo gromadzenia danych przez urządzenia kontroli dostępu większość użytkowników wciąż musi nauczyć się te dane wykorzystywać* – przyznaje B. Kozak. – *Potrzebna jest osoba, producent czy usługodawca, która będzie potrafiła zebrać dane uzyskane przez system KD, zarządzać nimi i wyciągać wnioski, przekształcając je w ten sposób w narzędzie analityczne.*

W erze Internetu Rzeczy kwestią kluczową staje się cyberbezpieczeństwo. Na dystrybutorów i użytkowników systemów kontroli dostępu jest wywierana presja stosowania najlepszych sposobów zabezpieczeń. *Luki bezpieczeństwa urządzeń pracujących w sieci nadal będą miały wpływ na wdrażanie IoT. Dlatego należy wymagać i egzekwować zarówno określonych parametrów zabezpieczeń, jak i przestrzegania zasad bezpieczeństwa w świecie wszechobecnych urządzeń mobilnych, które coraz częściej są wykorzystywane np. jako wirtualne karty dostępu* – podkreśla Mitchell Kane, prezes Vanderbilt Industries.

Producenci rozwiązań kontroli dostępu starają się przewidzieć możliwe luki zabezpieczeń i poszukują sposobów na minimalizowanie ryzyka, które jest nieuniknione podczas komunikacji przez sieć. Ponieważ analiza przesyłanych danych może pomóc użytkownikom przewidywać przypadki narażenia bezpieczeństwa urządzeń pracujących w sieci, kluczowe będzie wprowadzenie nadrzędnych przepisów dotyczących bezpieczeństwa.

SALTO Systems Sp. z o.o. Oddział w Polsce
ul. 17 Stycznia 45 A, Warszawa
tel. +48 609 017 777
info.pl@saltosystems.com | **www.saltosystems.com**

Światowe trendy w kontroli dostępu

Inteligentne budynki, chmura, technologie mobilne oraz Internet Rzeczy (IoT) to tylko niektóre kierunki rozwoju w świecie kontroli dostępu. Aby zapewnić sukces firmie, a tym samym jej wzrost, producenci rozwiązań kontroli dostępu muszą nadążać za innowacjami i zmieniającym się otoczeniem.
Marcus Handels, dyrektor ds. marketingu i sprzedaży firmy SALTO Systems, ocenia zmiany mające znaczący wpływ na sektor kontroli dostępu.

Co jest wyznacznikiem inteligentnych budynków?
W tej branży wiele mówi się ostatnio o popularności inteligentnych budynków. W firmie SALTO, która rozpoczęła działalność w 2001 r., zawsze projektowaliśmy, opracowywaliśmy i produkowaliśmy rozwiązania, które dzięki całkowitemu wyeliminowaniu mechanicznego klucza pozwalają tworzyć inteligentne budynki oraz nimi zarządzać. System kontroli dostępu, czasem postrzegany jako fragment całego obiektu, w rzeczywistości jest ogniwem systemu zarządzania instalacjami budynkowymi. Kluczowe są tu elektroniczna kontrola każdych drzwi, a także współpraca z innymi zintegrowanymi systemami, takimi jak CCTV, system alarmowy, sygnalizacji pożarowej itp., zapewniająca skuteczne i oszczędne zarządzanie wszystkimi elementami (*online, offline i wireless*) poprzez jeden pakiet oprogramowania. W firmie SALTO opracowaliśmy gamę urządzeń kontroli dostępu, które zapewniają bezpieczeństwo dzięki zaawansowanej technologii i obecności wewnątrz budynku. Instalując wysokiej jakości elektroniczne systemy kontroli dostępu w całej infrastrukturze budynkowej, właściciele mogą chronić ludzi, majątek i obiekt, zapewniając przy tym komfort i światowy poziom bezpieczeństwa. Chodzi o to, by już dziś, stosując innowacyjne pomysły i zaawansowaną technologię, tworzyć nowoczesne budynki jutra bez klucza mechanicznego.

Technologia Cloud jest coraz powszechniejsza na rynku kontroli dostępu. Jakie są jej zalety?
Sukces chmury i jej rosnące wykorzystanie w projektach na całym świecie przynosi korzyści wynikające ze zmiany sposobu myślenia w naszym sektorze. Wielu użytkowników dostrzega ogromne zalety oferowane przez rozwiązania w chmurze, zwłaszcza gdy zastosuje się odpowiednie zabezpieczenia. Dostrzegliśmy wcześnie jej potencjał, byliśmy jednym z pierwszych producentów, który wprowadził na rynek zaawansowane technologicznie elektroniczne rozwiązania kontroli dostępu oparte na chmurze. Nasz produkt SALTO KS *Keys as a Service* jest doskonałym narzędziem, ponieważ opiera się na wykorzystaniu urządzeń mobilnych zamiast kart dostępu, jest elastyczny i zorientowany na przyszłość. Kontrola dostępu realizowana w chmurze, o potwierdzonej niezawodności i stabilności, ma znacznie lepszą funkcjonalność i wydajność dzięki elastycznemu systemowi zarządzania. Nie wymaga instalacji oprogramowania ani złożonej infrastruktury IT, wystarczy urządzenie IQ z połączeniem internetowym, aby usługi kontroli dostępu stały się dla firm prostym i bezpiecznym rozwiązaniem do zarządzania kluczami, użytkownikami i drzwiami nawet w różnych lokalizacjach.

Co z integracją z innymi aplikacjami w chmurze oprócz kontroli dostępu?
W SALTO partnerzy integracyjni są starannie dobierani. Dbamy o to, aby współpracować tylko z partnerami i systemami korzystającymi z tych samych wysokich standardów bezpieczeństwa. Firma SALTO KS z powodzeniem zintegrowała liczne produkty na rynku, oferując kompleksowe rozwiązanie zabezpieczające w ramach powiązanych usług. Przykładem jest partnerstwo między SALTO a firmą Camera Manager, należącą kiedyś do Panasonica, a teraz wchodzącą w skład sieci EagleEye. To pierwszy przykład integracji pomiędzy najnowocześniejszą firmą CCTV w chmurze a systemem kontroli dostępu opartym na chmurze SALTO KS. Dzięki *KS connect* oraz naszym API oferujemy interfejs pozwalający w przyszłości na większą integrację z rosnącą liczbą usług oferowanych w chmurze.

Technologia mobilna rozwija się na rynku kontroli dostępu. Czy to już widoczny trend?
Oczywiście. Widzimy ekspansywny wzrost w tej dziedzinie, a przejście od danych uwierzytelniających na karcie dostępu do danych identyfikacyjnych w telefonie komórkowym było dla nas krokiem naturalnym. Firmowe dane SALTO związane z technologią karty są kompatybilne z danymi dostępu mobilnego. Umieszczenie danych w telefonie komórkowym ma dużą zaletę, ponieważ użytkownicy mogą je zmieniać szybko, w dowolnym miejscu i dwukierunkowo. Technologia mobilna *JustIn* firmy SALTO ułatwia wprowadzanie smartfonów jako integralnej części systemów kontroli dostępu. Użytkownicy zyskują wygodę i wydajność z zachowaniem bezpieczeństwa, a dostęp mobilny jest tym, czego młodsze pokolenie oczekuje jako standard, akceptując komunikację mobilną jako najnowocześniejszą technologię, która towarzyszy coraz większej liczbie usług i aplikacji mobilnych.

Jakie zalety dla użytkowników wynikają ze stosowania mobilnego dostępu?
Mobilny dostęp staje się nieunikniony, coraz więcej klientów docenia jego zalety. Produkty SALTO są kompatybilne z komunikacją *Bluetooth Low Energy* (BLE), a nowa wersja naszego *Justin Mobile* łączy funkcje BLE i NFC (*Near-Field Communication*) w jednej aplikacji. Dla użytkownika oznacza to, że potrzebuje tylko tej jednej aplikacji, a w zależności od tego, jakim telefonem komórkowym się posługuje, aktywuje element BLE lub NFC otwierający drzwi przez przyłożenie swojego smartfonu do czytnika BLE lub Mifare, elektronicznego okucia lub elektronicznej wkładki. Bezpieczna zaszyfrowana komunikacja mobilna jest kompatybilna z iOS poprzez BLE oraz z systemem Android przez BLE i NFC. Użytkownicy uzyskują prawo dostępu natychmiast i zdalnie, nie jest wymagana żadna infrastruktura ani zestawy bezprzewodowe. Konieczny jest jedynie zasięg 3G w smartfonie, który automatycznie wykrywa, czy drzwi są wyposażone w interfejs Bluetooth lub NFC, a następnie używa swojej bezpiecznej szyfrowanej komunikacji do otwarcia drzwi, nawet jeśli użytkownik ma wiele praw dostępu w jednej aplikacji, do kilku drzwi w różnych systemach SALTO.

Czy kontrola dostępu w Internecie Rzeczy ma przyszłość?
Tak, Internet Rzeczy (IoT) jest dla nas ekscytującą szansą. Świat staje się coraz bardziej połączony w sieci. Rola kontroli dostępu w IoT wzrośnie wraz z rozpowszechnieniem urządzeń IoT, a budynki staną się inteligentniejsze i bardziej połączone. Proliferacja urządzeń połączonych z Internetem będzie zmieniać sposób, w jaki żyjemy, pracujemy i odpoczywamy, a to w nadchodzących latach doprowadzi do przyspieszonego wdrożenia inteligentnych, połączonych rozwiązań kontroli dostępu.

Czy systemy kontroli dostępu będą odgrywać rolę w rozwoju inteligentnego domu?
W SALTO już dawno wiedzieliśmy, że zamki elektroniczne z czasem zastąpią klucze mechaniczne. Obserwowaliśmy to na wielu rynkach biznesowych w ostatniej dekadzie. Teraz nadszedł czas, by skupić naszą uwagę na rynku mieszkaniowym, ostatniej granicy, za którą istnieje masowa obecność kluczy mechanicznych. Wykupiliśmy znaczne udziały w spółce Poly-Control, producenta Danalock, dodając specjalistyczną wiedzę na temat elektronicznego zamykania wejść w budynkach mieszkalnych do naszej wiedzy z zakresu kontroli dostępu. Produkt Danalock w wersji 3. przyspiesza rozwój bezkluczowych rozwiązań IoT w sektorze budynków mieszkalnych w skali globalnej. Telefon jest kluczem do inteligentnego domu i łączności IoT oferowanej przez produkty Danalock, które pozwolą nam szybko wejść na ten rynek.

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

Integracja systemu KD z instalacjami SSWiN SATEL

Coraz więcej obiektów przemysłowych, przedsiębiorstw, budynków instytucji państwowych czy firm prywatnych jest wyposażanych w systemy mające dbać o bezpieczeństwo pracowników, osób przebywających tam czasowo, np. podróżnych na lotnisku czy klientów w biurze handlowym, a także mienia znajdującego się w chronionym obiekcie. **Najczęściej stosowanymi rozwiązaniami są instalacje kontroli dostępu oraz systemy sygnalizacji włamania i napadu. Czy możliwe jest efektywne, a zarazem intuicyjne zarządzanie dwoma systemami jednocześnie?**

Nowością na rynku zabezpieczeń jest możliwość integracji systemów SATEL: kontroli dostępu ACCO NET z instalacjami sygnalizacji włamania i napadu bazującymi na centralach serii INTEGRA oraz INTEGRA Plus. Nowe rozwiązanie jest przeznaczone dla instytucji, firm i przedsiębiorstw, także wielooddziałowych, w których wymagane jest zastosowanie zaawansowanej kontroli dostępu oraz najwyższych standardów bezpieczeństwa.

Organizacja integracji

Aby integracja była możliwa, do centrali INTEGRA lub INTEGRA Plus należy podłączyć moduł komunikacyjny ETHM-1 Plus, z którym komunikuje się serwer ACCO Server przez TCP/IP z wykorzystaniem szyfrowanego protokołu GUARDX. W ten sposób centrale INTEGRA są wirtualnie „wiązane" z centralami kontroli dostępu ACCO-NT. ACCO NET jest systemem skalowalnym – oznacza to, że może być rozbudowywany o dowolną liczbę central ACCO-NT. W związku z tym, że do każdej z nich można „podłączyć" nawet osiem central alarmowych, możliwości stają się wręcz nieograniczone. W ramach opcji oferowanych przez centralę ACCO-NT udostępniana jest jedna bezpłatna integracja z centralą z rodziny INTEGRA. Zintegrowanie kolejnych siedmiu wymaga wykupienia odpowiednich licencji.

Każda centrala kontroli dostępu może obsłużyć maksymalnie 255 kontrolerów, co pozwala na utworzenie do 255 przejść (stref), podczas gdy pojedyncza centrala INTEGRA umożliwia obsługę do 32 stref. Dzięki temu w ramach integracji osiem central INTEGRA łącznie pokryje maksymalną liczbę stref jednej centrali kontroli dostępu ACCO-NT.

Konfiguracja integracji odbywa się z poziomu komputera z zainstalowanym programem ACCO Soft. Wymagany jest jedynie dostęp do Internetu. Dzięki takiemu rozwiązaniu zarządzanie całym systemem jest dostępne z dowolnego miejsca na świecie.

Zalety płynące z integracji

Jedną z głównych idei i jednocześnie podstawową zaletą integracji jest możliwość efektywnego i wygodnego sterowania dwoma systemami jednocześnie. I tak np. przykładając kartę zbliżeniową do czytnika CZ-EMM działającego w ramach ACCO NET, można uzyskać dostęp (otworzyć drzwi) do danego pomieszczenia, jednocześnie wyłączając czuwanie w zintegrowanej strefie systemu INTEGRA. Analogicznie uzbrajając system alarmowy z manipulatora, można zablokować dostęp do zintegrowanej strefy ACCO NET. W efekcie uzbrojenie systemu alarmowego na danym piętrze w biurowcu spowoduje automatyczne zaryglowanie wszystkich drzwi znajdujących się w obrębie strefy tego piętra, nadzorowanych przez system kontroli dostępu.

Co się stanie, gdy zostanie wywołany alarm? Przy alarmie włamaniowym w strefie INTEGRA nastąpi automatyczne zablokowanie zdefiniowanych wcześniej przejść – czyli gdy nastąpi nieautoryzowane wejście, wywołany alarm może spowodować zablokowanie drzwi w okolicznych korytarzach, odcinając intruzowi drogę ucieczki. Natomiast w przypadku alarmu pożarowego w strefie INTEGRA wybrane przejścia w obiekcie mogą zostać otwarte, dzięki czemu wszystkie osoby będą mogły się bezpiecznie ewakuować.

Dodatkową zaletą integracji jest zwiększenie liczby użytkowników, którzy mogą załączać i wyłączać czuwanie wybranej strefy centrali INTEGRA. Gdy system alarmowy działa autonomicznie, może być obsługiwany maksymalnie przez 240 użytkowników. W przypadku integracji wszyscy użytkownicy obsługiwani przez daną centralę ACCO-NT (a może ich być nawet 8000) mogą uzyskać możliwość tzw. przełączania. Oznacza to, że osoby posiadające odpowiednie uprawnienia przypisane w ACCO Web poprzez długie przytrzymanie karty zbliżeniowej przy czytniku będą mogły uzbroić i rozbroić zintegrowaną strefę systemu alarmowego. Dzięki temu możliwe jest jeszcze większe, niż w przypadku systemu kontroli dostępu, zróżnicowanie uprawnień. Przykładowo, pracownicy oddziału firmy X mogą jedynie mieć prawo wejścia do swojego biura, ale ich kierownik może również uzbroić i rozbroić system alarmowy, dyrektor regionalny natomiast może mieć dodatkowo dostęp oraz możliwość sterowania czuwaniem systemów alarmowych we wszystkich obiektach tego przedsiębiorstwa.

> Podstawową zaletą integracji jest możliwość efektywnego i wygodnego sterowania dwoma systemami jednocześnie.

„Przełączaniem" i innymi uprawnieniami użytkowników ACCO NET można wygodnie zarządzać za pomocą aplikacji internetowej ACCO Web, także z urządzeń mobilnych. Istotnym udogodnieniem jest możliwość predefiniowania szablonów użytkowników. Taka funkcjonalność idealnie sprawdzi się np. gdy przyjmujemy do pracy nową osobę i chcemy nadać jej standardowe uprawnienia pracownika biurowego, dodatkowo określając, do których obiektów w całej firmie ma mieć dostęp. Skrócony jest także czas szkolenia nowo zatrudnionej osoby, ponieważ zamiast nauki obsługi dwóch systemów wystarczy wskazanie, jak posługiwać się kartą w ramach ACCO NET.

ACCO Web umożliwia także zdalne zarządzanie przejściami oraz stanem zintegrowanych stref systemów INTEGRA. W jakich sytuacjach może być to przydatne? Otóż blokując zdalnie daną strefę (przejście), można włączyć czuwanie systemu alarmowego. Analogicznie w przypadku przywrócenia kontroli strefy (przejścia) czuwanie może zostać wyłączone. Jednocześnie aplikacja umożliwia podgląd stanu stref oraz wejść i wyjść zintegrowanych central alarmowych, udostępniając obsłudze wgląd w to, co dzieje się w systemie.

Wspólna historia zdarzeń obu systemów to kolejna zaleta najnowszego rozwiązania firmy Satel. Dzięki tej funkcjonalności bezpośrednio w ACCO Web można przeglądać archiwum zawierające informacje dotyczące tego, co działo się w ramach systemu kontroli dostępu, a także mieć wgląd w dane na temat czuwania i alarmów systemów INTEGRA.

Co ważne, z zalet integracji będą mogli korzystać nie tylko użytkownicy nowych instalacji, także istniejące systemy ACCO NET oraz INTEGRA będą mogły zostać poddane integracji. Wystarczy aktualizacja oprogramowania central kontroli dostępu ACCO-NT, kontrolerów przejść oraz central alarmowych (wraz z modułem komunikacyjnym ETHM-1 Plus), aby miały one najnowszą wersję oprogramowania.

Integracja ACCO NET z centralami alarmowymi INTEGRA z pewnością ułatwi nadzór oraz obsługę instalacji zabezpieczeń osobom zarządzającym obiektami i ich sieciami. Uzyskane funkcjonalności wpływają jednocześnie na zwiększenie wygody codziennej obsługi z punktu widzenia użytkownika. Podsumowując, integracja to kompleksowe rozwiązanie „łączące" system kontroli dostępu oraz system sygnalizacji włamania i napadu oferowane przez SATEL, które spełnia stawiane przed nim oczekiwania, zaspokajając potrzeby specjalistów z branży security.

Włamania do systemów kontroli dostępu

Solidny system kontroli dostępu jest istotnym elementem każdej organizacji, jednak z różnych powodów często jest on łatwy do sforsowania. Podczas tegorocznych targów ISC West w Las Vegas Valerie Thomas, Executive Security Consultant w firmie Securicon, przybliżyła **sposoby stosowane przez hakerów do przełamywania systemów kontroli dostępu i wskazała, co powinny zrobić firmy, aby uchronić się przed atakami.**

a&s International

Systemy kontroli dostępu stanowią istotny element każdego systemu bezpieczeństwa firmy. Kontrola dostępu – kto, do czego oraz gdzie i kiedy ma dostęp – przyczynia się do zapewnienia bezpieczeństwa, jednocześnie umożliwiając śledzenie i kontrolowanie tego rodzaju aktywności. Niestety firmy często wdrażają systemy bez odpowiedniego przetestowania, w efekcie powstają luki w zabezpieczeniu, co naraża je na ataki.

Valerie Thomas, Executive Security Consultant w firmie Securicon, podaje przykłady podatności systemów kontroli dostępu (KD) w firmach na ataki i podpowiada, jak można tym atakom zapobiegać.

Ignorowanie cyberprzestrzeni

Podczas projektowania i implementacji systemu KD cyberataki często nie są nawet brane pod uwagę. System ten w znacznym stopniu opiera się na IT, natomiast – nad czym ubolewa Valerie Thomas – branża zabezpieczeń cierpi na braki wiedzy i zrozumienia technologii informatycznych. System KD jest zazwyczaj instalowany przez podwykonawcę, który kończy swoją pracę z chwilą ukończenia instalacji, ale nawet podczas realizacji tego zlecenia obszar bezpieczeństwa jest najczęściej pomijany. Systemy te opierają się na technice cyfrowej i rozwiązaniach sieciowych, ale w ich projektowanie, tworzenie i zarządzanie rzadko są angażowani eksperci z dziedziny cyberbezpieczeństwa.

Mamy do czynienia z sytuacją, w której za poszczególne elementy odpowiadają różne osoby, ale zwykle nikt nie patrzy na problem całościowo – wskazuje V. Thomas. Zwraca jednocześnie uwagę, że próba zabezpieczenia przed jednym tylko typem ataku hakerskiego nie zabezpieczy użytkowników końcowych. Skupiając się wyłącznie na najnowszych i najsilniejszych metodach uwierzytelniania i technologii wykonania kart, inne elementy systemu pozostają otwarte i podatne na ataki, a to tylko zwiększa ryzyko. Dlaczego tak się dzieje? Zdaniem V. Thomas w branży brakuje specjalistów, których szeroka wiedza

obejmuje zagadnienia z różnych dziedzin. Bez udziału eksperta od bezpieczeństwa sieci komputerowych, który wesprze tworzenie systemu KD i zadba o zastosowanie odpowiednich środków bezpieczeństwa, powstała sieć wprowadza do systemu słabe punkty, sprawiając, że staje się on łatwym celem hakerów.

Ataki hakerów na systemy KD

Jest wiele sposobów dokonywania ataków na system KD – zarówno wyszukanych, jak i nieskomplikowanych. W rzeczywistości większość z nich nie jest skomplikowana. Specjaliści do spraw bezpieczeństwa powinni więc zrobić wszystko, by współtworzona przez nich sieć była bezpieczna, a system kontroli dostępu chroniący firmę zabezpieczony przed atakami.

Proxmark 3

Jest reklamowany jako przyrząd do badania systemów komunikujących się radiowo (RFID) lub z wykorzystaniem technologii NFC (*Near Field Communication* – technologia bliskiego zasięgu). Nawet pobieżne wyszukiwanie w Internecie przynosi dziesiątki wyników o sposobach klonowania kart RFID za pomocą tego narzędzia. Nie wymaga to ani pogłębionej wiedzy hakerskiej, ani znajomości technologii. Wystarczy, że zestaw nawiąże komunikację z kartą kontroli dostępu. Aby z niego skorzystać, trzeba dysponować źródłem zasilania i anteną – może to więc wzbudzić podejrzenia, dlatego nie jest to najskuteczniejszy sposób wykradania danych kart.

BLEKey

To niewielkie urządzenie, które nawiązuje połączenie z czytnikiem RFID dzięki podłączeniu do ścieżek transmitujących dane w formacie Wiegand. Wystarczy je podłączyć do trzech przewodów; zasilanie pochodzi z czytnika. Po nawiązaniu połączenia BLEKey przechwytuje dane karty, które są przez czytnik odczytywane. Korzystając ze standardu BLE (*Bluetooth Low Energy*), urządzenie można zsynchronizować z aplikacją na telefon i wywołać powtórzenie ostatniej operacji odczytu karty.
Ta metoda ataku obnaża brak szyfrowania protokołu Wiegand, który jest stosowany w czytnikach kontroli dostępu. Aby uniemożliwić hakerom podłączenie BLEKeya, użytkownicy powinni zainstalować w czytniku alarm przeciwsabotażowy, który powiadomi o próbie włamania.

Urządzenia typu REX

(Request to Exit)

V. Thomas podkreśla, że urządzenia REX nie zawsze są „inteligentne", zatem włamanie się do nich może być dość proste. Wiele urządzeń REX wykorzystuje detekcję ruchu zamiast przycisku umożliwiającego wyjście. Choć dzięki temu opuszczenie danego obszaru jest jeszcze mniej skomplikowane, to tak samo łatwe jest obejście tych urządzeń. Aby aktywować detektor ruchu otwierający drzwi, wystarczy wsunąć pod drzwiami jakiś przedmiot, np. wieszak na ubrania czy balon. Urządzenie REX wykryje ruch w pomieszczeniu, a wejście intruza nie zostanie odnotowane. Jeden ze sposobów, w jaki można zapobiec tego typu atakom, to podniesienie wiązki detektora.

Pozyskiwanie kodów kontroli dostępu

Zabezpieczenie sieci, w której działa system KD, stanowi krytyczny element zabezpieczenia tego systemu. Niewystarczająca znajomość zagadnień IT i środowiska komputerowego podczas instalacji często powoduje pozostawienie luk. Hakerom wystarczy włamanie się do kontrolera systemu KD, by odczytać w zasadzie dowolne informacje potrzebne do przejęcia kontroli nad całym systemem. Takie informacje, jak dane obszaru będącego pod nadzorem danego kontrolera, adresy IP innych kontrolerów i serwerów, numery kart i dzienniki logowań czy hasła – wszystko to można zdobyć z jednego systemu KD. V. Thomas zauważa, że wiele kontrolerów obsługuje anonimowy dostęp do FTP-a, co czyni system podatnym na atak (nawet jeśli FTP jest stosowany wyłącznie jako *backup*).

Serwer

Serwerem systemu kontroli dostępu opiekuje się zazwyczaj firmowy dział IT, który traktuje go jako jeden z wielu innych serwerów. V. Thomas podkreśla, że na serwerze DNS serwer systemu KD jest często opisany jako „kontrola dostępu", więc jest łatwy do zidentyfikowania.
W obszarze poza siecią firmową V. Thomas zwraca uwagę na narzędzie Shodan – wyszukiwarkę, która pozwala odnajdywać „dziurawe" serwery. Shodan, zwany też „Google dla urządzeń sieciowych", wyszukuje podłączone do Internetu routery, serwery itd. Strona ta jest najczęściej wykorzystywana przez specjalistów ds. bezpieczeństwa do wykrywania luk w zabezpieczeniu. Korzystają z niej jednak również hakerzy, by uzyskać dostęp do niedostatecznie strzeżonych sieci.

Edukacja i ochrona

Atakom na systemy KD można zapobiec.
Od strony informatycznej jest to w znacznej mierze kwestia konfiguracji. Można dokonać łatwej segmentacji w ramach sieci, a następnie zastosować podstawowe metody kontroli bezpieczeństwa sieciowego, co zamknie drogę takim atakom z wielu różnych źródeł – wyjaśnia V. Thomas.
Ważną sprawą jest edukacja użytkowników konieczna w zapewnieniu systemowi KD odpowiedniej ochrony. Dotyczy to nie tylko specjalistów ds. bezpieczeństwa w firmie, ale także innych pracowników, w tym pracowników ochrony. Często zapomina się o przeszkoleniu personelu ochrony i pozostałych pracowników działów zabezpieczeń technicznych z zakresu ataków kierowanych przeciwko systemom.

Świadomość rodzajów ataków, na które podatny jest system KD, podejmowanie odpowiednich kroków w celu zabezpieczenia systemów od strony sieciowej oraz edukacja użytkowników chronionych organizacji to narzędzia niezbędne do zabezpieczenia systemów przed atakami w przyszłości.

Pomiędzy CYBERNIEOSTROŻNOŚCIĄ a CYBERBEZPIECZEŃSTWEM

W serwisach na całym świecie pojawiła się niedawno informacja o tym, że **tysiące plików zawierających informacje o żołnierzach i tajnych agentach służb specjalnych Stanów Zjednoczonych wyciekły w nieznanych okolicznościach.** Znaleziono je na niezabezpieczonym serwerze.

Michał Czuma

Jak podał serwis IBTimes, „9402 dokumenty opatrzone klauzulą *ściśle tajne* znaleziono na jednym z serwerów Amazona. Kopia danych, do której dostęp miał każdy, została odkryta przez specjalistę od cyberbezpieczeństwa". Na innych serwisach z kolei napisano, że „pliki zawierały poufne dane dotyczące wojskowych oraz pracowników tajnych służb. Wśród ujawnionych informacji znalazły się prywatne adresy, numery telefonów, adresy e-mail i historia zatrudnienia. Niektóre rekordy zawierały numery prawa jazdy lub paszportu, a nawet poziom dostępu do tajnych danych".

Jak zareagowałby każdy z nas, gdyby okazało się, że poufne dane zarówno firmy, jak i jej klientów, e-maile i opinie znalazły się w nieodpowiednim miejscu albo ktoś je opublikował w celu sprzedaży? Ile trzeba by zapłacić, żeby nie przedostały one się do opinii publicznej, i co by się stało, gdyby je sprzedano…

Często uczestniczę w sympozjach i panelach dyskusyjnych dotyczących sposobów radzenia sobie z cyberzagrożeniami. Słowo cyber dodaje się obecnie do wielu określeń. Wszyscy chcą przeciwdziałać cyberprzestępczości, spora grupa ludzi zatrudnia cybereksperów, by zabezpieczali firmy przed cyberatakami, cyberfraudami i hakerami oraz innymi formami cyberprzestępczości. Powstaje niezliczona liczba aplikacji mających na celu ochronę systemów przed „ulotem informacji", cyberpenetracją czy cyberatakami. Ale co jakiś czas każdy zastanawia się nad kilkoma kwestiami: czy jestem bezpieczny w sieci, czy moja firma jest dobrze zabezpieczona przed wrogimi działaniami, czy opłaca się wydawać krocie, bo i tak jakiś haker przełamie kosztowne zabezpieczenia i poniosę straty. Jak więc wygląda bezpieczeństwo systemów i ochrona przed cyberatakami?

Nie istnieje system, dzięki któremu można powiedzieć, że dana firma czy korporacja są skutecznie zabezpieczone przed cyberatakami. Nikt nie jest bezpieczny w 100%.

O poprawnie zainstalowanych zabezpieczeniach na poziomie systemów informatycznych można mówić na podstawie dużych firm. Im mniejsze przedsiębiorstwo, tym bardziej jest bezbronne. Hakerstwo to obecnie doskonale zorganizowany biznes, w coraz większym stopniu oparty na socjotechnice i olbrzymiej ilości informacji, które o życiu prywatnym umieszczamy w social mediach. Dobry haker zaczynał swoje działania, grzebiąc w nocy w śmietniku ofiary będącej jego celem. I do dzisiaj to robi, dlatego dobrze zabezpieczone firmy kupują specjalistyczne maszyny do niszczenia dokumentów, a w piwnicach trzymają specjalny sprzęt do prasowania śmieci. Dobremu hakerowi wystarczy kilka minut, by na swój komputer pobrać podstawowe informacje dotyczące konkretnej osoby.

Nie tak dawno pewnym menedżerem w pewnej korporacji zainteresowała się w sieci atrakcyjna dziewczyna. On był pracownikiem średniego szczebla, ona pracowała – jak twierdziła – niedaleko. Znajomość w sieci trwała w najlepsze, menedżer zapałał gorącym uczuciem do pięknej (jak wyglądała na prezentowanych w portalach społecznościowych zdjęciach) dziewczyny, przeszli więc na korespondencję e-mailową. Pani przesyłała masę fotografii, na wszystkich wyglądała atrakcyjnie, on był przekonany, że już ją gdzieś widział. Zachęcał ją do spotkania w realu, ale ona była zapracowana i przekładała terminy spotkań. W e-mailach zadawała wiele pytań, pan pokazywał, gdzie pracuje i czym się zajmuje. Chwalił się swoimi osiągnięciami. Pani zaproponowała, że odezwie się do niego na Skypie w czasie pracy i wtedy w końcu się zobaczą. Pan z żalem odmówił, informując, że w jego firmie wymogi bezpieczeństwa uniemożliwiają instalowanie wszelkiego, niecertyfikowanego oprogramowania. Jego rozmówczyni nie zraziła się, wprost przeciwnie – nie widziała problemu, ponieważ i ją też obowiązywały „wygórowane wymogi bezpieczeństwa", ale obiecała, że prześle mu link, który „obchodzi wszelkie blokady", i będą mogli zobaczyć się online. W pracy na służbowy e-mail (w firmie menedżera nie można odbierać prywatnej poczty nawet przez przeglądarkę), który wcześniej został zarzucony zdjęciami, plikami z pięknymi filmami i albumami nieznajomej, przyszedł e-mail wysłany z adresu znanej wszystkim firmy, z linkiem do strony z apletem umożliwiającym telekonferencję. Gdy otworzyło się okno z apletem, pan ucieszony włączył mikrofon w swoim komputerze, po drugiej stronie usłyszał głos przemiłej dziewczyny, ale był bardzo niezadowolony z powodu braku wizji. Minęło kilka minut, gdy usłyszał w głosie dziewczyny nutkę irytacji i pytanie, czy otwierając link, zatwierdził certyfikat, o jaki przeglądarka musiała go przecież zapytać. Przypomniał sobie, że gdy otwierał link, aplet zasygnalizował potrzebę instalacji dekodera i certyfikatu, ale będąc po szkoleniu zorganizowanym przez biuro bezpieczeństwa, nacisnął „nie", nie wyrażając zgody na instalację, zresztą jak

POCZĄTEK INTERNETU – KONIEC BEZPIECZEŃSTWA?

Należę do pokolenia, które pamięta narodziny Internetu. Programowania uczono mnie jeszcze w liceum, gdy na lekcjach informatyki pierwsze algorytmy pisaliśmy długopisem w zeszycie. Pierwsze programy pisałem, mając ZX Spectrum, korzystając z egzemplarzy „Bajtka", ucząc się programowania oraz komend pozwalających na opanowanie komputera i napisanie kilku użytecznych skryptów. Podczas pobytu w USA w 1990 r. dowiedziałem się o Internecie, który krok po kroku wciągał mnie w rzeczywistość wirtualną. W Polsce horrendalnie drogi dostęp do Internetu uruchomił w 1991 r. NASK, będący monopolistą na rynku. Trwało to kilka lat. Ale już wtedy, mimo że nie istniały jeszcze strony www, a pierwszy serwer sieci akademickiej Uniwersytetu Warszawskiego dopiero się tworzył, wykorzystując dostęp oferowany mi przez kuzyna, obserwowałem sieć i grzebałem w zasobach i treściach przechowywanych na serwerach. Szybko odkryłem, że siecią najbardziej zainteresowali się przestępcy, dostrzegając tu nowe możliwości do nielegalnych działań. Przyspieszenie zainteresowania Internetem nastąpiło po uruchomieniu przez Telekomunikację Polską powszechnie dostępnego numeru telefonicznego, pozwalającego wszystkim abonentom posiadającym komputer z modemem na połączenie z globalną siecią. Wtedy jeszcze nikt nie myślał o bezpieczeństwie, chociaż były już pierwsze sygnały, iż sieć nie jest bezpieczna i mogą pojawiać się zagrożenia. Pierwszy program antywirusowy był zapowiedzią tego, co czeka w sieci. Jeszcze nie do końca przewidywano rozmiar zagrożeń, ale zaczęto się zastanawiać, czy Internet jest bezpieczny. Dzięki mnożącym się BBS-om (oferującym dostęp do sieci) rozpoczął się proces upowszechnienia się w Polsce Internetu. W tym czasie, pracując przy tajnym projekcie, niechcący przełamałem zabezpieczenia w sieci wewnętrznej mojej instytucji. Zgłosiłem mojemu ówczesnemu szefowi, że system komputerowy jest zawodny, skoro w kilka chwil można wyciągnąć z jego komputera ściśle tajne informacje. Jako dowód przekazałem wydrukowaną na igłowej drukarce OKI listę jego osobistych kontaktów. Był wyraźnie niezadowolony. Był rok 1995 i wtedy postanowiłem opuścić mury tej instytucji. Uzmysłowiłem sobie, że wielu ludziom niewiedza daje większy spokój niż świadomość zagrożeń. By zachować złudny spokój, wystawiają siebie i firmy na wiele zagrożeń. Wtedy wydawało mi się, że to absurd, ale dzisiaj już nie jestem tego pewny.

powtarzał dziewczynie, „nie miał do tego takich uprawnień". Dziewczyna przekonywała go, że też nie miała uprawnień, ale po instalacji bez problemu mogła rozmawiać z mamą, tatą i koleżankami. Szybko dokonał więc rachunku potencjalnych zysków i strat i uznał, że w oczach pięknej dziewczyny nie może wypaść na lamera. Przeprosił ją, po czym się rozłączył, przeładował stronę i zrobił to, o co go poprosiła. Jednej rzeczy nie mógł się domyślić – akceptując niezaufaną aplikację, certyfikat, a wcześniej otwierając zdjęcia, wśród których „część się nie otwierała", za to zawieszała komputer, zainfekował nie tylko swojego laptopa w domu i pracy, ale także do systemu firmy wpuścił *worma* intruza, a ten najpierw umożliwił instalację spreparowanego skryptu, otwierając dostęp do wszystkich tajemnic firmy osobom nieupoważnionym. W ten sposób zdolny haker wszedł do sieci korporacyjnej firmy i tylko dzięki czujności administratorów po tygodniu ślad jego działalności został wykryty. Do dzisiaj nie wiadomo, co zrobił haker, do czego uzyskał dostęp oraz jakie straty poniosła firma. Menedżer musiał pożegnać się z pracą, a poznana w sieci dziewczyna już nie odpowiada na jego e-maile. Co gorsza, ta historia jest prawdziwa.

Najsłabszym elementem najbardziej nawet wyrafinowanych systemów bezpieczeństwa jest człowiek: użytkownik, administrator i nadzorca systemu.

Pracownicy branży bezpieczeństwa, oferujący bardzo dobre rozwiązania dotyczące obszaru cybersecurity, często mają problemy z zachęcaniem potencjalnych klientów do korzystania z rozwiązań i usług w tym zakresie. Prezentując skuteczne rozwiązania osobom odpowiedzialnym za cyberbezpieczeństwo, nierzadko spotykają się albo z brakiem decyzji, albo wręcz z niechęcią. Trzeba więc się zmierzyć z faktami. Nawet najlepsi administratorzy systemów odpowiedzialni za bezpieczeństwo sieci firmowych nie mają pewności, czy sieć, o którą dbają, jest skutecznie zabezpieczona przed atakiem. Pentesterzy testujący bezpieczeństwo systemu powinni przeprowadzać testy penetracyjne przynajmniej raz na pół roku, ponieważ tylko w ten sposób mogą określić stopień bezpieczeństwa badanego systemu. Terminem pentester określa się wysokiej klasy hakera, który penetrując system firmy, wykrywa w niej podatności i luki umożliwiające potencjalny atak. Niestety cena za takie testy jest niemała, a mogą one potrwać nawet kilka tygodni. Wynagrodzenie pentestera wynosi 500 euro za dzień pracy. Po znalezieniu ewentualnych słabych punktów wybrana firma usuwa je, po czym pentester przeprowadza kolejne testy. Jeśli znajdzie kolejne luki, proces jest kontynuowany, aż do całkowitego „załatania" systemu. Czasami trzeba zmienić sposób funkcjonowania całego biznesu, zwyczaje w firmie, wprowadzić procedury, nowe specjalizacje – co zwiększa koszty działalności, a w konsekwencji firmy rezygnują z tych wydatków. Jak bardzo cyberzagrożenia wpływają na koszty funkcjonowania? Wystarczy sobie wyobrazić, jakie niezadowolenie w firmie może spowodować wprowadzenie polityki „czystych biurek", gdy pracownikom zabrania się przynosić do pracy notatniki, a telefony komórkowe trzyma się w specjalnym pomieszczeniu z dala od komputerów, by uniemożliwić kopiowanie z ekranów danych osobowych czy poufnych dokumentów firmy. Jest to nieodzowne, gdy na ekranach komputerów pracownicy mogą przeglądać tajne dokumenty. Kolejne procedury blokujące dostęp do portów, wprowadzające kody dostępu do drukarki, monitorowanie poczty elektronicznej mogą budzić sprzeciw pracowników. Jeśli ponadto ma zostać wprowadzona kontrola dostępu do pomieszczeń, zakaz używania komórek prywatnych w pracy, a wszystko, co robi pracownik, będzie podlegać kontroli, monitorowaniu i analizie służb bezpieczeństwa firmy, może to skłonić właścicieli do zaniechania takich działań. Dlatego wielu ekspertów odwiedzających polskie firmy, oferujących coraz lepsze rozwiązania zwiększające odporność systemów korporacyjnych na cyberataki i cyberzagrożenia, spotyka się z murem niemożności. Nie można uzyskać odpowiedzi, czy dane rozwiązanie ma szansę stać się elementem zabezpieczenia systemu klienta, czy zarząd firmy jest zainteresowany zakupem i czy w ogóle zwiększenie bezpieczeństwa należy do priorytetów. Niestety wielu ludzi mających czuwać nad bezpieczeństwem sieciowym w pewnym momencie się poddaje. Nie chcąc wchodzić w konflikty z szefami, pracownicy sygnalizują jedynie, że system wymaga zakupów, testów, upgrade'u oprogramowania, gdyż spada poziom zabezpieczeń przed starymi i nowymi formami ataków. Zdarza się, że tylko informują decydentów o nowym zagrożeniu i potrzebie sfinansowania zabezpieczeń, zdając sobie sprawę z tego, że ich siła przebicia jest niewielka.

> To, że nie da się w pełni zabezpieczyć przed zagrożeniami, nie może powodować, że w ogóle rezygnuje się z rozwiązań zabezpieczających zasoby.

Stan bezpieczeństwa systemów informatycznych jest mierzony wysokością nakładów firmy na bezpieczeństwo.

Wiele firm ubezpieczeniowych oferowało ubezpieczenie na wypadek cyberataków. Okazało się, że ten rodzaj ubezpieczeń nie cieszy się zbytnim zainteresowaniem. Produkt oferowany obecnie przez siedem towarzystw sprzedaje się bardzo słabo, takie ubezpieczenie kupiła tylko jedna polska firma i był nią duży bank. W dużych firmach, szczególnie finansowych, infrastruktura informatyczna bardzo często jest poddawana atakom. Z każdym atakiem wydatki na bezpieczeństwo się zwiększają. Czyżby więc chodziło o to, że rodzimi przedsiębiorcy wychodzą z założenia, że jeśli nikt ich nie atakuje, a procedury bezpieczeństwa działają, to oznacza, że są bezpieczni i nic więcej nie muszą robić? Testy przeprowadzane w Polsce pokazują, że dobrze chronione są duże firmy, szczególnie z branży finansowej i bankowej, natomiast im mniejsza firma, tym gorzej. Przedsiębiorcy i menedżerowie stojący na czele średnich firm często nie zdają sobie sprawy ze skali zagrożeń.

Kwestią jest nie to, czy firma będzie celem ataku, ale kiedy ten atak nastąpi.

O skali zagrożenia świadczy fakt, że ceny wystawionych na sprzedaż danych sukcesywnie spadają. Wiele lat temu cena

danych osobowych pojedynczych rekordów wykradzionych z polskich firm i instytucji, zawierających dane osobowe i dotyczące kont, numery rachunków bankowych itp. wahała się od 1000 do 1500 zł. Obecnie za pojedynczy rekord tej samej bazy płaci się 10–20 gr. Jeszcze niedawno cena na czarnym rynku za numer karty kredytowej z danymi osobowymi jej posiadacza wynosiła 10 dolarów za rekord, dziś spadła do zaledwie kilku centów. Ta analiza dowodzi, że na czarnym rynku występuje nadpodaż danych, co jest najlepszym wskaźnikiem zagrożenia firm w sieci.

Przeświadczenie, że jeszcze nikt nie zaatakował firmy, jest aprioryczne. Większość firm nie wie, jakie i ile ich poufnych danych jest już dostępnych w Darknecie, a także kiedy i ile razy spenetrowano ich zasoby.

Analizując zasoby danych pozwalających na penetrację firm i wyrządzenie szkód, widać, że tych danych jest w Darknecie bardzo dużo. I chyba tylko nieświadomość wielu zjawisk, które sygnalizują fakt, iż firma została spenetrowana albo jej poufne dane są dostępne w Darknecie sprawia, że zagrożenia są lekceważone. Ważne, aby każde przedsiębiorstwo opracowało procedury bezpieczeństwa i je egzekwowało. Pewne zwyczaje muszą szybko zniknąć, ponieważ stwarzają ogromne ryzyko. To, że nie da się w pełni zabezpieczyć firm przed zagrożeniami, nie może powodować, że w ogóle zrezygnują one z wdrożenia rozwiązań zabezpieczających ich zasoby. **Wkrótce wejdą w życie regulacje, które nakładają na firmy, niezabezpieczające chociażby tylko przechowywanych w swoich systemach danych osobowych i danych wrażliwych, kary sięgające do 4% rocznego ich obrotu. Łatwo więc policzyć, ile będzie kosztowało oszczędzanie na zabezpieczeniu baz danych.**

Sytuacje, w których właściciel firmy lekceważy informacje o możliwym bankructwie nie tylko z powodu braku zabezpieczeń związanych z zagrożeniami fraudami i oszustwami, ale również cyberprzestępczością, występują często. Może nawet dzięki oszczędzaniu na bezpieczeństwie tego typu przedsiębiorstwa osiągają przewagę nad konkurencją, ale muszą sobie zdawać sprawę, że to działanie krótkowzroczne. Ludzi przezornych dziwi ta nonszalancja i brak zdolności przewidywania.

Należy więc podjąć podstawowe działania zwiększające bezpieczeństwo.

1. Ważnym krokiem w odpowiednim zabezpieczeniu firmy przed cyberatakami powinno być zbudowanie wyspecjalizowanej komórki wewnętrznej lub sięgnięcie po zespół zewnętrzny, który zajmie się przygotowaniem firmy na cyberataki i będzie na bieżąco monitorował stan bezpieczeństwa.
2. Ulubioną bronią cyberprzestępców jest manipulacja i socjotechnika. Metodologia przestępców opiera się nie tylko na zaufaniu, ale także na niewiedzy i braku świadomości zagrożenia. Odpowiednio przeszkoleni pracownicy mogą ograniczyć skuteczność ataku hakerów. Nie bez kozery pierwszy atak, jaki wykonują przestępcy, to ustalenie listy pracowników, ich numerów telefonów oraz adresów e-mail, które wykorzystują do testowania świadomości pracowników firmy na potencjalne zagrożenia.
3. Firma musi opracować procedury, które pozwalają na ochronę przedsiębiorstwa przed ewentualnymi zagrożeniami. Pracownicy mają niestety naturalną tendencję do łamania procedur, ale na pewno określenie ich oraz ustanowienie odpowiednich sankcji za łamanie jest lepsze niż ich brak.

Polskie firmy bagatelizują zagrożenia cyberatakami, ale jednocześnie zwiększają wydatki na ochronę przed nimi. Daje się jednak zauważyć tendencję do poszukiwania możliwości wykorzystania luk w systemach firmowych w celu ich penetracji i użycia do szpiegostwa gospodarczego. Dzisiaj prawie każda firma obserwuje konkurencję, jej ofertę i trendy w branży. Jest mnóstwo możliwości robienia tego zgodnie z przepisami, ale łatwo pójść na skróty i przekroczyć pewną granicę, podejmując działania niezgodne z prawem, a wtedy należy mówić już o szpiegostwie. Do zagrożeń cyberprzestępczością dochodzi zagrożenie ze strony nieuczciwej konkurencji. Zaskoczenie i straty z tego wynikające są przyczyną dużych problemów wielu firm. Przedsiębiorca, chcąc pokonać konkurencję nieuczciwymi metodami, szuka możliwości włamania się na serwer biznesowego rywala, by poznać jego strategie, plany i tajemnice.

Twierdzenie, iż przed cyberprzestępczością nie da się obronić w 100%, nie oznacza, że nie można się przed nią zabezpieczyć. Czy zakup systemu alarmowego do domu jest niepotrzebnym wydatkiem, bo przecież „złodziej ma swoje sposoby”? Nawet najlepiej zabezpieczone przed kradzieżą samochody również są kradzione. Czy w związku z tym nie instalujemy w domach systemów monitoringu, a samochody przestajemy zabezpieczać i parkujemy z kluczykami w stacyjce? Montujemy alarmy, kupujemy ubezpieczenia, parkujemy na parkingach strzeżonych – na bezpieczeństwie nie można oszczędzać. Nie trzeba specjalistycznego oprogramowania, by wejść na fora dyskusyjne konkretnych firm, zagadnąć sfrustrowanego pracownika, który np. został zwolniony z pracy, pała chęcią zemsty i powie wszystko, co chce konkurencja. Firmy nie chwalą się tym, że ich zasoby zostały wykradzione, dane ich klientów i informacje wrażliwe przejęte przez grupy przestępcze lub hakerów. Większość tych spraw jest najpilniej strzeżonymi sekretami zaatakowanych firm. Nie żałują one później pieniędzy na testy penetracyjne, specjalistyczne usługi, wynajęcie wyspecjalizowanych firm doradczych, sięgnięcie po usługi cyberguard i cybersecurity, ponieważ wiedzą, ile kosztuje spokój, byt i los firmy. A ten koszt jest zawsze mniejszy niż straty poniesione z powodu braku podjęcia stosownych działań w odpowiednim czasie. Lepiej być mądrym przed szkodą.

QNAP
3F, No. 22, Zhongxing Rd., Xizhi Dist.
New Taipei City, 221, Taiwan (R.O.C.)
www.qnap.com | gbielawski@qnap.com

INTELIGENTNE ZAGROŻENIA BEZPIECZEŃSTWA DANYCH

Będzie coraz gorzej

Ataki na IoT i chmurę oraz nowa generacja *ransomware* stają się coraz bardziej inteligentne, działają autonomicznie i są coraz trudniejsze do wykrycia.

Z analiz firmy SonicWall wynika, że w ciągu ostatniego roku aktywność złośliwego oprogramowania typu *ransomware* zwiększyła się 167-krotnie – takich ataków odnotowano 638 mln (rok wcześniej zaledwie 3,8 mln). Zagrożenie jest więc realne, coraz częściej dotyka ono również polskie firmy i instytucje. Według danych firmy Check Point w ubiegłym roku ok. 10% wszystkich cyberataków w Polsce to były właśnie przypadki użycia *ransomware*. Zasada działania klasycznej aplikacji tego typu jest standardowa – po zainfekowaniu komputera (do którego aplikacja dociera, podszywając się np. pod dokument, aktualizację czy infekując go z poziomu strony WWW) ransomware błyskawicznie szyfruje wybrane pliki, po czym blokuje użytkownikowi dostęp do nich. Następnie na ekranie pojawia się komunikat, z którego wynika, że dostęp do danych może zostać przywrócony, ale wyłącznie po uiszczeniu odpowiedniej opłaty. To wyjątkowo podły, ale jednocześnie skuteczny mechanizm – przestępcy doskonale zdają sobie sprawę z tego, że w przypadku firmy brak dostępu do krytycznych dla jej funkcjonowania danych może oznaczać przestój i gigantyczne straty finansowe. Dlatego też przedsiębiorcy płacą „okup" – rozwiązując doraźnie problem, ale jednocześnie czyniąc tę operację opłacalną i motywując przestępców do kolejnych ataków.

Czy można zabezpieczyć system firmy przed *ransomware*?

Skuteczne zabezpieczenie przed atakami *ransomware* jest niezwykle trudne. Przestrzeganie podstawowych zasad bezpieczeństwa (aktualizowanie aplikacji i systemu, stosowanie oprogramowania antywirusowego) wprawdzie ogranicza ryzyko, ale go nie eliminuje. Często zdarza się, że nowe programy *ransomware*

NAJGŁOŚNIEJSZE ATAKI *RANSOMWARE* W 2017 R.

- Zaatakowanie luksusowego alpejskiego hotelu sieci Seehotel Jägerwirt – wbrew medialnym doniesieniom nie doszło tam wprawdzie do zablokowania dostępu do pokoi hotelowych, jednak ryzyko było realne, dlatego właściciele hotelu zdecydowali się na zapłacenie okupu.
- Atak na szpital w Ottawie (przestępcy żądali wysokiego okupu, administratorzy szpitalnego systemu zdołali jednak przywrócić dane z *backupu*).
- Zainfekowanie *ransomware* komputerów holenderskiego parlamentu (podejrzewa się, że ów atak mógł być motywowany politycznie – trop prowadził do Turcji).
- Zaszyfrowane przez *ransomware* dane urzędu z województwa lubelskiego. Odpowiedzialny za to program był rozsyłany w e-mailu podszywającym się pod wiadomość od Poczty Polskiej.
- Atak na system IT urzędu odpowiedzialnego za nadzór nad transportem miejskim w San Francisco (spowodował paraliż komunikacyjny, m.in. blokując system sprzedaży biletów).
- Zaszyfrowanie plików pacjentów i personelu w amerykańskim szpitalu Presbyterian Medical Center (za ich odblokowanie przestępcy domagali się 3,4 mln USD).

Specjaliści ds. bezpieczeństwa zwracają uwagę, że niektóre takie programy są tworzone również przez Polaków – świadczą o tym m.in. komentarze w języku polskim w kodzie złośliwego programu WildFire.

skutecznie ukrywają się przed „antywirusami" i korzystają z luk zero-day.

Pewnym rozwiązaniem może być regularne tworzenie backupu, jednak standardowa kopia zapasowa danych nie zawsze skutecznie chroni przed *ransomware*. Jeśli nośnik, na którym będzie zapisywany *backup*, jest stale podłączony do komputera (przez USB/Ethernet/Wi-Fi), to istnieje duże prawdopodobieństwo, że również te dane zostaną zaszyfrowane podczas ataku. Na szczęście jest skuteczna metoda ochrony danych – wdrożenie *backupu* opartego na mechanizmie migawek, czyli przechowującego wiele wersji skopiowanych danych. Dzięki temu w razie ataku *ransomware* użytkownik może przywrócić dane do poprzedniej wersji, neutralizując działanie „szkodnika".

Pełna ochrona danych firmowych dzięki migawkom

Rozwiązaniem 100-procentowo skutecznym, chroniącym użytkownika nie tyle przed samym atakiem *ransomware*, ile przed jego skutkami, jest skorzystanie z systemu *backupu* opartego na mechanizmie migawek, czyli *snapshotów*. Takie narzędzie, dostępne we wszystkich modelach serwerów QNAP NAS, pozwala na regularne, automatyczne wykonywanie kopii wskazanych danych/wolumenów.

Serwer przechowuje kolejne „wersje" *backupu* i w razie incydentu – awarii czy ataku *ransomware* i zablokowania dostępu do danych – administrator może bez problemu przywrócić wcześniejsze wersje. Co ważne, na bieżąco są archiwizowane tylko dane, w których pojawiają się zmiany. Dzięki temu kopie zajmują mniej miejsca, a wszystkie kluczowe informacje zostają zabezpieczone.

Nie ma żadnych przeciwwskazań, by jeden serwer QNAP NAS stał się centralnym systemem *backupu* dla wielu firmowych komputerów – użytkownik może wygodnie skonfigurować go tak, by zapisywał i przechowywał *backup* z wielu źródeł.

Warto podkreślić, że serwer NAS jest w 100% odporny na atak *ransomware*, ponieważ pracuje pod kontrolą bazującego na Linuksie systemu QTS. Ponadto wyposażono go we wbudowany mechanizm antywirusowy, skanujący zapisywane w urządzeniu dane.

Więcej o tym, jak zminimalizować zagrożenie ze strony *ransomware* przy użyciu serwera QNAP NAS, na stronie: **www.qnap.com/solution/ransomware/pl-pl/index.php**

RODO

JAK NADZOROWAĆ PROWADZENIE I OCHRONĘ ZBIORÓW DANYCH OSOBOWYCH

OCHRONA DANYCH OSOBOWYCH CZ. 4

Wprowadzanie zmian wynikających z wdrażania RODO do polskiego porządku prawnego to proces ciągle trwający, poddawany modyfikacjom stosownie do rozwiązań sektorowych i uzupełniany o nowe doświadczenia wynikające ze szczegółowych branżowych analiz.

Marek Blim

Zagadnienia przedstawione w artykule są wierzchołkiem góry lodowej (1/10 jej masy widoczna nad wodą), wskazując główne problemy zmieniających się wymagań ochrony danych osobowych opartych na zasadzie *risk based approach* (podejścia opartego na ryzyku), jakie muszą poznać, zrozumieć i wdrożyć w swoich firmach przedsiębiorcy branży security, zajmujący się projektowaniem zabezpieczeń, ochroną fizyczną i techniczną oraz konserwacją systemów ochronnych i alarmowych.

W kolejnym artykule cyklu adresowanego do przedsiębiorców i specjalistów branży security przedstawiamy zmiany wynikające z treści unijnych dokumentów: rozporządzenia nr 2016/679 oraz dyrektywy nr 2016/680, jakie w swoich działaniach musi uwzględnić kierownik agencji ochrony, szef alarmowego centrum nadzoru czy właściciel firmy instalującej systemy alarmowe,

Po czteroletnich przymiarkach i konsultacjach państwa europejskie w grudniu 2015 r. uzgodniły i po zatwierdzeniu w I kwartale 2016 r. przez trilog zarządczy UE (Parlament Europejski, Rada Europy i Komisja Europejska) 27 kwietnia podpisały dokument EU nr 2016/679, który został opublikowany 4 maja 2016 r. Dokument ten jest nowym rozporządzeniem unijnym, tzw. ogólnym Rozporządzeniem o Ochronie Danych (Osobowych) RODO (GDPR – *General Data Protection Regulation*). RODO wejdzie w życie 25 maja 2018 r., a dotyczy wszystkich przedsiębiorstw oraz instytucji w UE przetwarzających lub gromadzących dane osobowe. Równocześnie wydano nową dyrektywę UE nr 2016/680 związaną z ochroną danych w systemach prawnych i policyjnych.

Jest to największa od 20 lat zmiana ustawodawstwa w zakresie przetwarzania danych. Aby w pełni sprostać jej wymaganiom, przewidziano dwuletni okres *vacatio legis* na przygotowanie wdrożenia.

Jak wykazały badania ankietowe, znaczna liczba firm przetwarzających dane nie jest gotowa do wprowadzenia zmian zapisanych w rozporządzeniu, a nawet o nim nie słyszała.

- Według danych z maja i listopada 2016 r. oraz stycznia 2017[1)] r. w Polsce jest bardzo niska znajomość treści RODO/GDPR, ponieważ:
  - aż 45% firm nigdy nie słyszało o no-

wym rozporządzeniu (RODO/GDPR) albo wie o nim niewiele;
- tylko 24% firm ma świadomość wejścia regulacji w życie oraz zna wszystkie jej istotne szczegóły.

- Trudno mówić o gotowości do sprostania wymaganiom RODO / GDPR, gdyż:
  - 31% przedsiębiorstw nie ma żadnej świadomości o RODO/GDPR;
  - 18% słyszało o regulacji, ale nie wykonało żadnych działań, by przygotować się do nadchodzących zmian;
  - jedynie 15% jest już przygotowane na zmiany.
- Jedynie 52% firm (w skali UE) ma świadomość pozostałych wiążących regulacji, takich jak *Personal & Impact Assessment Data Protection oraz National Interoperability Framework*. W Polsce są to odpowiednio: bezpośrednia odpowiedzialność właściciela zasobu danych osobowych za analizę ryzyk i zabezpieczenie się przed ich skutkami (ocena, czy przetwarzanie „z dużym prawdopodobieństwem może spowodować wysokie ryzyko" – DPIA/BIA), Krajowe Ramy Interoperacyjności (czyli KRI) oraz akty prawne Komisji Nadzoru Finansowego (np. rekomendacja D – edycja z 2013 r.).

Spośród badanych w Polsce firm aż dwie trzecie stwierdziło, że w przypadku ich przedsiębiorstw nowe regulacje z zakresu ochrony danych osobowych znajdą zastosowanie, wskazując przy tym fakt, że wiele z tych regulacji wymaga doprecyzowania, ponieważ rozporządzenie odnosi się równoważnie co do swoich wymagań zarówno do mikroprzedsiębiorstw, jak i wielkich ponadnarodowych korporacji.

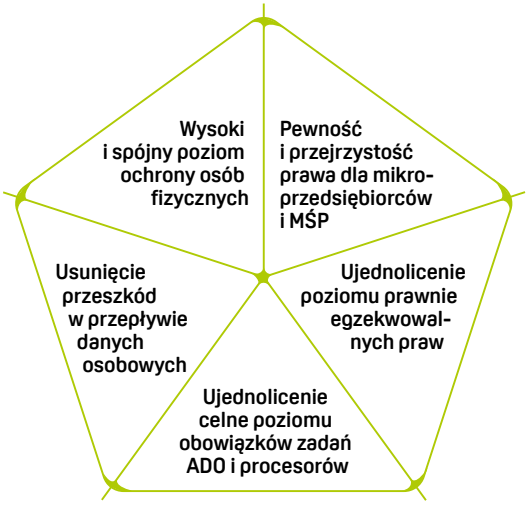
Wprowadzane zmiany:

zamiast GIODO/ABI będzie PUODO/IOD (ang. DPA/DPO)

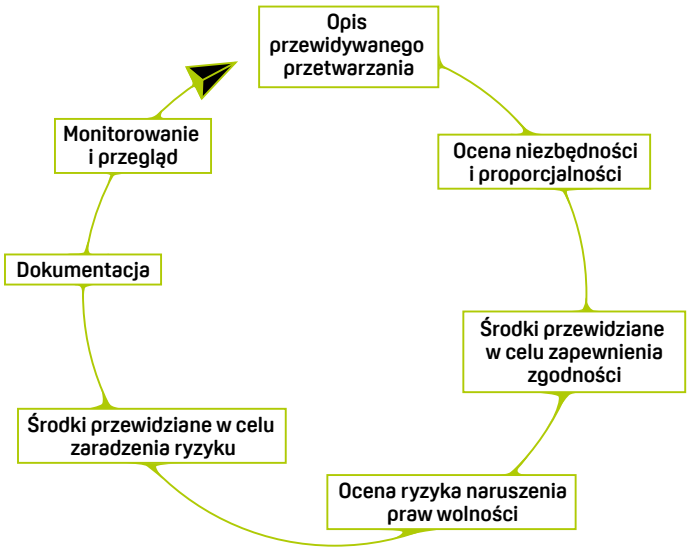
Zmiany zachodzące w społeczeństwie informacyjnym (tzw. trzecia fala[2]) rozwoju społecznego) spowodowały znaczącą rozbieżność między prawami krajowymi, opracowanymi na podstawie dyrektywy nr 95/46/WE Parlamentu Europejskiego i Rady WE (zawiera definicje podstawowych terminów odnoszących się do dzie-

Zagadnienia przedstawione w artykule są wierzchołkiem góry lodowej, jakie muszą poznać, zrozumieć i wdrożyć przedsiębiorcy branży security, zajmujący się projektowaniem zabezpieczeń, ochroną fizyczną i techniczną oraz konserwacją systemów ochronnych i alarmowych.

[1] www.rp.pl; www.instytutodo.pl; http://gdpr.pl
[2] A. Toffler, *Trzecia fala*, wyd. 2., Poznań, Wyd. Kurpisz
[3] W Polsce była to ustawa z 27 sierpnia 1997 r. o ochronie danych osobowych – wielokrotnie nowelizowana (tj. z 2002 r., z 2008 r., z 2015), obecnie obowiązuje jej tekst jednolity (Dz.U. z 2016 r., poz. 922).
[4] Rozporządzenie MSWiA o warunkach technicznych przetwarzania danych osobowych (Dz.U. z 2004 r., nr 100, poz. 1024).
[5] EOG/EEA – Europejski Obszar Gospodarczy/ European Economic Area – obejmuje państwa Unii Europejskiej i Europejskiego Stowarzyszenia Wolnego Handlu (EFTA), z wyjątkiem Szwajcarii. EOG opiera się na czterech fundamentalnych wolnościach: swobodzie przepływu ludzi, kapitału, towarów i usług.
[6] „Imprimatur" prawa międzynarodowego nad prawem krajowym (bezwzględnie obowiązujące przepisy prawa <=> mandatory/imperative provisions/regulations of law).
[7] www.rp.pl
[8] DPIA – *Data Protection Impact Assessment*, oszacowanie wpływu zdarzeń na ochronę danych
[9] Wytyczne Grupy Roboczej, art. 29 ds. ochrony danych przyjęte 4 kwietnia 2017 r.



Rys. 1. **Zestawienie celów RODO/GDPR**
(opracowanie własne autora)



Rys. 2. **Ogólny proces iteracyjny przeprowadzania DPIA**
(źródło: 17/EN, WP 248)[9)]

dziny danych osobowych, ustala zasady zbierania, gromadzenia, przechowywania i udostępniania danych osobowych) a rzeczywistymi potrzebami zintegrowanego w ramach strefy Schengen rynku europejskiego. Dyrektywa określiła zasady i warunki zgodności przetwarzania danych osobowych z prawem oraz prawa osób, których dane dotyczą, nakazując zarazem ich wdrożenie w prawie krajowym oraz wprowadzanie stosownych aktualizacji[3)]. Rozwiązania krajowe uzupełnione dodatkowymi rozporządzeniami wykonawczymi[4)] nie sprawdzały się w sytuacjach konfliktowych w trakcie realizacji umów transgranicznych, zwłaszcza w przypadku państw o odmiennym układzie odniesienia prawnego (*common law ≠ codex law*).

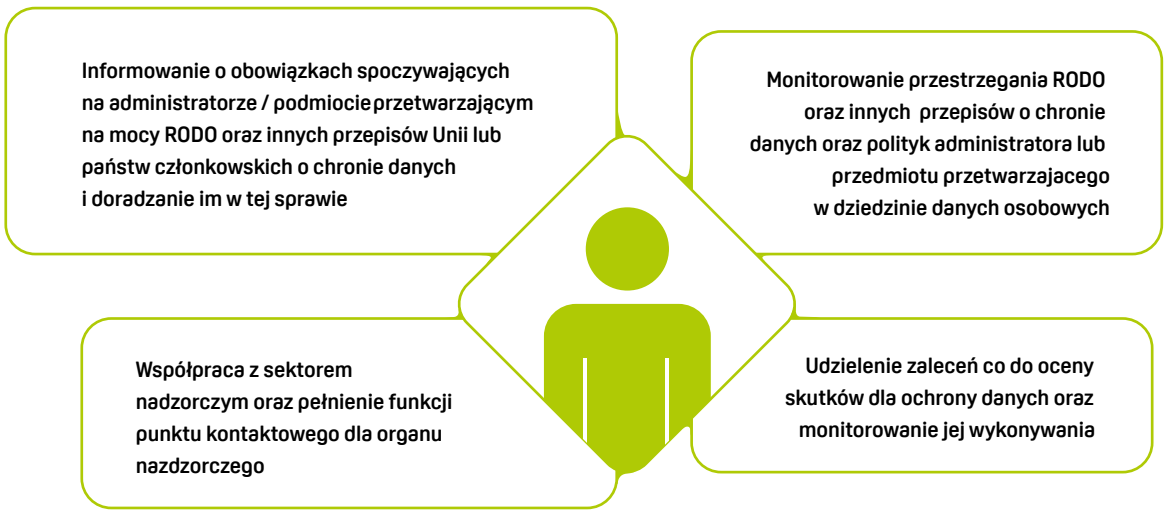
Rozwijający się handel w ramach EOG/EEA[5)] stworzył nową rzeczywistość. Na jednolitym rynku UE (tzw. rynku wewnętrznym) możliwy jest swobodny przepływ ludzi, towarów, usług i pieniędzy w całej UE, niczym w obrębie jednego państwa. Podstawową rolę w usuwaniu barier w handlu odgrywa wzajemne uznawanie. Obywatele UE mogą studiować, mieszkać, robić zakupy, pracować i przechodzić na emeryturę w dowolnym kraju UE, a także korzystać z produktów i usług pochodzących z całej Europy. Z takim podejściem wiąże się konieczność jednolitego unormowania prawa dotyczącego ochrony danych osobowych dla każdego obywatela UE, stąd zmiany w RODO względem dotychczasowej dyrektywy i uniwersalny obowiązek jego stosowania (*peer see*)[6)]. Potrzeba zmian jest oczywista. *Kiedy przyjmowano dyrektywę 95/46/WE, założyciel Facebooka Mark Zuckerberg miał trzynaście lat, Google dopiero został założony, a cloud computing raczkował. Rozporządzenie uchwalone w 2016 r. jest o wiele bardziej dostosowane do obecnego, zdigitalizowanego świata* – mówi radca prawny Izabela Kowalczuk-Pakuła, kierująca praktyką ochrony danych osobowych i prywatności w kancelarii Bird & Bird[7)].

Cele rozporządzenia tworzą spójny pięcioelementowy blok działań (*rys. 1*) oparty na nowym ujęciu znanych już pojęć z zakresu przetwarzania. To enumeratywny (zamknięty) katalog uprawnień w stosunku do danych osobowych obejmujący gromadzenie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie/modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie, dopasowywanie, rozpowszechnianie, ograniczanie, usuwanie/niszczenie. Wprowadzonym nowym definicjom (rozdz. I, art. 4, pkt 1–26) mają towarzyszyć transparentna polityka i procedury postępowania z posiadanymi zbiorami danych osobowych.

Nowe ujęcie pojęcia „zbiór danych osobowych" (art. 4, pkt 6) oznacza każdy uporządkowany zestaw danych o charakterze osobowym, dostępnych wg określonych kryteriów, niezależnie od tego, czy jest scentralizowany, czy rozproszony funkcjonalnie lub geograficznie. Właściciel tego zasobu jest zarazem właścicielem wszystkich rodzajów ryzyka, związanych z zasobem oraz jego administratorem (ADO – administrator danych osobowych) odpowiedzialnym za postępowanie z tymi rodzajami ryzyka, a dobór środków zabezpieczenia danych pozostaje w jego gestii (technologiczna neutralność), przy czym jest wymagany ujednolicony poziom obowiązków ADO i jego procesorów/podprocesorów.

Zmiany w stosunku do aktualnie obowiązującego w Polsce prawa dotyczą głównie organów nadzoru nad bezpieczeństwem samych danych osobowych, a także metod i sposobów ich przetwarzania (w tym skutecznego zapobiegania rodzajom ryzyka o dużym prawdo-

[10)] Dr Joanna Tomaszewska, konferencja RODO, 25 maja 2017r., ambasada Wlk. Brytanii w Warszawie.
[11)] www.giodo.gov.pl/pl/p/opinie-i-wytyczne-grupy-roboczej-art-29.
[12)] Tamże.



Rys. 3. **Zadania Inspektora Ochrony Danych wg RODO/DPO-GDPR**
(źródło: materiały SSW)

podobieństwie wystąpienia), zwłaszcza w świetle art. 35 mówiącego o wysokim ryzyku naruszenia „praw lub wolności osób fizycznych". W dotychczasowych rozstrzygnięciach dotyczących zadań i funkcji ABI oraz GIODO elementy oceny ryzyka miały charakter jednostkowy – w RODO jest to działanie kompleksowe pozwalające na elastyczne przeprowadzenie w minimalnym zakresie DPIA[8)] (art. 35 ust. 7 oraz motywy 84 i 90 w preambule rozporządzenia), obejmujące zestaw czynności przedstawiony na *rys. 2.*

Praktyczne przeprowadzenie tego procesu wymaga znacznie większej wiedzy i uprawnień niż te, które są przypisane administratorowi bezpieczeństwa informacji (ABI), stąd w RODO szerokie uprawnienia przypisane niezależnemu Inspektorowi Ochrony Danych (IOD/DPO) oraz konieczność zmiany zakresu uprawnień i nazwy dotychczasowemu GIODO (w projekcie ustawy MC jest to Prezes Urzędu Ochrony Danych Osobowych pełniący funkcję krajowego organu nadzoru – DPA).

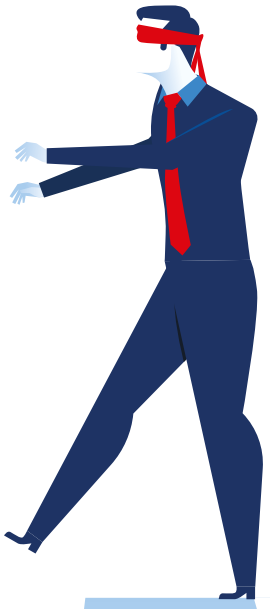
Powołany IOD/DPO zgodnie z art. 37–39 RODO/GDPR realizuje zadania przedstawione na *rys. 3.*

Szerszą odpowiedź na pytania, kim będzie Inspektor Ochrony Danych (IOD/DPO), jaka jest jego niezależność, zadania oraz zakres odpowiedzialności można znaleźć w ostatniej wersji dokumentu grupy roboczej art. 29 ds. ochrony danych osobowych nr 16/EN, WP 243 rew.01 [11)] z 5 kwietnia 2017 r.

Rola nadzoru – organów krajowych i europejskich

Rozporządzenie nakłada na Administratora Danych Osobowych i podmiot przetwarzający szereg obowiązków w zakresie zapewnienia bezpieczeństwa danych osobowych (rozdz. IV, art. 24), które odpowiednio podlegają monitorowaniu ze strony Inspektora Ochrony Danych Osobowych IOD/DPO (art. 37) – osobie powoływanej w celu wspierania ADO w działaniach ochronnych i będącej zarazem punktem kontaktowym organu nadzorczego (art. 31) [krajowego – DPA (art. 51) oraz za jego pośrednictwem organu europejskiego, Europejskiej Radzie Ochrony Danych] szczególnie w przypadkach wymagających zachowania mechanizmu spójności stosowania zasad RODO (art. 63).

Istotne znaczenie ma także ustalenie organu nadzorczego w przypadku działań transgranicznych związanych z przetwarzaniem/przekazywaniem danych osobowych, co zostało opisane w dokumencie grupy roboczej w art. 29 ds. ochrony danych osobowych nr 16/EN, WP 244 rew. 01 [12)] z 5 kwietnia 2017 r. „Wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego".



Z czym – wg RODO – musi się liczyć przedsiębiorca branży security

Administratorem danych osobowych (ADO) jest obligatoryjnie właściciel zasobu/zbioru/zbiorów danych osobowych. Może nim być osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który to samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art. 4, pkt 7. RODO) lub nakazuje/zleca ich przetwarzanie w swoim imieniu innej osobie fizycznej lub prawnej, organowi publicznemu, jednostce lub „podmiotowi przetwarzającemu" (patrz: art. 4, pkt 8. RODO).

Przedsiębiorca branży security jest ADO względem danych osobowych swoich pracowników oraz współpracowników i kontrahentów w realizowanych wspólnie pracach i projektach, natomiast staje się „podmiotem przetwarzającym" w momencie dostępu do danych osobowych zapisanych we wszelkich systemach security (SKD, TSN/VSS, ESKK, SSWiN, bazy: SMA/LCN/ACO) w momencie ich konserwacji, modernizacji lub naprawy. Nie została obecnie określona jednoznacznie potrzeba (jako przypisów w umowie na wykonanie ww. prac) zobowiązań wynikających bezpośrednio z art. 28 RODO, dotyczących powierzenia przetwarzania danych osobowych (identyfikacja osoby, jej wizerunku, danych dostępowych itd.).

Przedsiębiorca branży security, działając jako procesor na dostępnych mu zbiorach, pomaga ADO zapewnić zgodność z obowiązkami określonymi w art. 30–34 RODO i poddaje się obowiązkowi rejestrowania swoich działań w celu ewentualnego udostępnienia ich na potrzeby kontroli zgodności z wymaganiami RODO.

Przedsiębiorca zajmujący się projektowaniem zabezpieczeń, ochroną fizyczną i techniczną oraz konserwacją systemów ochronnych/alarmowych wykorzystujących biometrię (SKD, VSS) powinien szczegółowo przeanalizować to, że art. 4 ust. 14 RODO/GDPR definiuje „dane biometryczne" jako dane osobowe (takie jak wizerunek twarzy lub dane daktyloskopijne), które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby. Oznacza to m.in. że dane biometryczne użytkowników systemów SKD lub ESKK będą musiały być szczególnie chronione jako wrażliwe/poufne dane osobowe od 25 maja 2018 r., zgodnie z wymaganiami rozdz. II, art. 9 RODO/GDPR, a sposób ich zabezpieczenia powinien być opracowany już na etapie projektowania tych systemów – zgodnie z art. 25 ust. 2 (przy uwzględnieniu uwag zawartych w motywie 78 preambuły).

> Od 25 maja 2018 r. dane biometryczne użytkowników systemów SKD lub ESKK będą musiały być szczególnie chronione jako wrażliwe/poufne dane osobowe, a sposób ich zabezpieczenia powinien być opracowany już na etapie projektowania tych systemów.

Stosowanie reguły wdrażania mechanizmów zwiększających ochronę prywatności nakłada określone zobowiązania związane z przetwarzaniem danych osobowych w systemach security. Działania obejmują tzw. *privacy by design* – na etapie projektowania poszczególnych systemów, kiedy to informujemy zleceniodawcę – administratora danych osobowych (ADO) o sposobie przetwarzania danych w systemach, a także *privacy by default* – jako domyślne ustawienie i akceptowanie zabezpieczeń zgromadzonych w systemie security danych osobowych dostępnych dla konserwatora/modyfikatora w trakcie wykonywania prac serwisowych i modernizacyjnych systemu.

Skutki prawne i finansowe RODO/GDPR

Złamanie przepisów RODO/GDPR będzie wiązało się z odpowiedzialnością prawną, w tym z ogromnymi karami – nawet 4% rocznego obrotu o maksymalnej kwocie 20 mln euro. Dotyczy to odpowiednio także małych i średnich przedsiębiorstw. Regulacja obejmuje przede wszystkim firmy i organizacje, które zatrudniają więcej niż 250 pracowników i przechowują dane ponad 5000 osób. Tego typu przedsiębiorstwa, w myśl nowego prawa, będą musiały zatrudnić specjalistę na stanowisku inspektor ochrony danych – IOD/DPO (*Data Protection Officer*), który będzie odpowiadać za całokształt polityki ochrony i przetwarzania danych osobowych. Jego zadania, uprawnienia i obowiązki znacznie wykraczają poza funkcje spełniane przez dotychczasowych administratorów bezpieczeństwa informacji w ochronie danych osobowych.

Jednocześnie zostają zachowane wolności i zasady ujęte w Karcie praw podstawowych (z obowiązku stosowania rozporządzenia są wyłączone organizacje, które przetwarzają dane związane z wyznawaną religią, orientacją seksualną, przebytymi chorobami oraz karalnością). Oznacza to, że np. związki wyznaniowe lub organizacje mniejszości seksualnych nie będą musiały dostosowywać swoich struktur do nowego prawa.

BIO

dr inż. Marek Blim
Europejski menedżer systemu zarządzania jakością EOQ, certyfikowany audytor systemów jakości i zarządzania bezpieczeństwem informacji, ekspert systemowy ISO 9000 INTERCERT/TüV Rheinland Polska. Rzeczoznawca systemów technicznej ochrony osób i mienia oraz zarządzania bezpieczeństwem. Projektant systemów ochrony. Czynny zawodowo konsultant-rzeczoznawca-audytor.

JAK ZLIKWIDOWAĆ STANOWISKO PEŁNOMOCNIKA DS. OCHRONY INFORMACJI NIEJAWNYCH W PODMIOCIE PRAWA HANDLOWEGO

PORADNIK

Likwidacja Pionu Ochrony Informacji Niejawnych lub tylko stanowiska Pełnomocnika Zarządu ds. Ochrony Informacji Niejawnych [POIN] – samodzielnego stanowiska pracy – nie jest możliwa (w sensie prawnym i faktycznym) z dnia na dzień, co niekiedy próbują czynić zarządcy niektórych jednostek organizacyjnych, zwłaszcza podmiotów prawa handlowego, gdy zostaną cofnięte im przez ABW świadectwa bezpieczeństwa przemysłowego lub świadectwa te utracą ważność, w związku z upływem czasu i braku woli zarządców podmiotu, by wszcząć kolejne postępowanie bezpieczeństwa przemysłowego.

Marek Ryszkowski

W jednej ze spółek prawa handlowego, która posiadała dwa świadectwa bezpieczeństwa przemysłowego III stopnia – krajowe na poziomie klauzuli tajności TAJNE i międzynarodowe na poziomie klauzuli tajności NATO SECRET – zlikwidowano samodzielne stanowisko pełnomocnika ds. ochrony informacji niejawnych. ABW cofnęła je jeszcze przed upływem połowy siedmioletniego okresu ich ważności. W okresie ważności ww. świadectw spółka ta nie wykonywała żadnej umowy (samodzielnie lub w składzie konsorcjum), do której wykonywania byłoby potrzebne świadectwo bezpieczeństwa przemysłowego. W cofnięciu przez ABW ww. świadectw nie było „winy pełnomocnika", np. znamion naruszenia przez niego prawa ochrony informacji niejawnych lub zaniechania przez niego obligatoryjnego działania w zakresie ochrony informacji niejawnych. Zarząd spółki podjął decyzję, że nie będzie ubiegał się w przyszłości o ponowne uzyskanie jakichkolwiek świadectw bezpieczeństwa przemysłowego. Zatem samodzielne stanowisko pracy pełnomocnika zarządu ds. ochrony informacji niejawnych w spółce nie będzie potrzebne. Podjęto więc również decyzję o likwidacji tego stanowiska pracy. Pełnomocnik, zatrudniony na ww. stanowisku, poinformował zarząd spółki, że w trakcie wykonywania przedsięwzięć likwidacyjnych należy przestrzegać odnośnych (które wymienił w informacji) przepisów prawa ochrony informacji niejawnych, prawa ochrony danych osobowych, prawa o narodowym zasobie archiwalnym i archiwach oraz prawa pracy.

W spółce zatrudniano kierownika jednostki organizacyjnej i pełnomocnika zarządu ds. ochrony informacji niejawnych, a także pracowników z ważnymi poświadczeniami bezpieczeństwa na poziomie klauzul tajności Tajne i NATO SECRET oraz aktualnymi zaświadczeniami o odbyciu szkoleń z zasad ochrony informacji niejawnych o ww. klauzulach tajności – są to warunki *sine qua non* uzyskania krajowego i międzynarodowego świadectwa bezpieczeństwa przemysłowego wymagane przepisami prawa OIN. Nie zorganizowała pionu ochrony informacji niejawnych, ponieważ w przypadku świadectw bezpieczeństwa przemysłowego III stopnia nie wymaga tego prawo ochrony informacji niejawnych.

Pełnomocnik zarządu ds. ochrony informacji niejawnych był etatowym pracownikiem spółki, zatrudnionym w wymiarze ¼ etatu i nie miał powierzonych innych obowiązków, np. administratora bezpieczeństwa informacji (ABI) lub osoby odpowiedzialnej za ochronę fizyczną spółki, co często ma miejsce w podmiotach

Istnieje katalog niezbędnych dokumentów poświadczających prawomocność i zgodność z prawem przedsięwzięć likwidacyjnych samodzielnego stanowiska pracy POIN.

prawa handlowego. Otrzymał on w siedzibie spółki stanowisko pracy biurowej, wyposażone w meble biurowe, komputer i sprzęt biurowy, a także szafę stalową do przechowywania imiennych akt postępowań sprawdzających oraz innych dokumentów, np. korespondencji z ABW, KRS, urzędami stanu cywilnego itp. Miał też zezwolenie na wykonywanie niektórych, ściśle określonych czynności pełnomocnika w systemie telepracy. Akta zwykłych postępowań sprawdzających, chociaż nie są opatrywane klauzulami tajności, powinny być przechowywane jak dokumenty o klauzuli tajności ZASTRZEŻONE, zatem do ich przechowywania, a także innych dokumentów pełnomocnika, służyła ww. szafa stalowa. Kluczami do zwykłego zamka mechanicznego i kodami do zamka mechanicznego o zmiennym nastawieniu szafy dysponowali jedynie pełnomocnik (użytku bieżącego) i kierownik jednostki organizacyjnej (zapasowe, w zalakowanej kopercie). Ten drugi na wypadek konieczności komisyjnego otwarcia szafy, np. pod nieobecność pełnomocnika.

Postępowanie przy likwidacji samodzielnego stanowiska pracy POIN powinno uwzględniać okoliczności:

- likwidacja stanowiska w podmiocie prawa handlowego oznacza zmianę jego struktury organizacyjnej, zatem powinna być dokonana na podstawie uchwały zarządu, uchwały rady nadzorczej (jeżeli istnieje) lub uchwały zgromadzenia udziałowców bądź akcjonariuszy;
- przedsięwzięcia związane z likwidacją powinna wykonać komisja likwidacyjna, w której skład nie powinien wchodzić pełnomocnik, zatrudniony na likwidowanym stanowisku; powinien on być zobowiązany do ścisłej współpracy z komisją likwidacyjną, głównie jako jej doradca i wykonawca niektórych przedsięwzięć likwidacyjnych;
- komisja likwidacyjna powinna być powołana zarządzeniem prezesa zarządu podmiotu; na czele komisji powinien stać kierownik jednostki organizacyjnej – KJO (w rozumieniu prawa OIN), jeżeli nie jest nim prezes zarządu podmiotu, albo inny członek zarządu, jeżeli prezes zarządu podmiotu jest jednocześnie KJO;
- członkowie komisji likwidacyjnej powinni posiadać ważne poświadczenia bezpieczeństwa i aktualne zaświadczenia o odbyciu szkolenia z zasad ochrony informacji niejawnych;
- zarządzenie powołujące komisję likwidacyjną powinno zawierać m.in. uprawnienia przewodniczącego komisji i obowiązki komisji; obowiązki wobec komisji pełnomocnika i jego samodzielne obowiązki likwidacyjne; określenie dnia wejścia w życie zarządzenia i oznaczenie czasu przeznaczonego na likwidację stanowiska pełnomocnika (od – do); określenie terminu rozwiązania stosunku pracy z pełnomocnikiem.

WZÓR NR 1

Zarządzenie nr…../20….

z dnia dd mm rr

Prezesa Zarządu …… Sp. z o.o.

w sprawie likwidacji samodzielnego stanowiska pracy pełnomocnika zarządu ds. ochrony informacji niejawnych.

W związku z cofnięciem przez Agencję Bezpieczeństwa Wewnętrznego posiadanych przez przedsiębiorstwo …… Sp. z o.o., zwane dalej „Spółką", świadectw bezpieczeństwa przemysłowego III stopnia na poziomie krajowej klauzuli tajności TAJNE i międzynarodowej klauzuli tajności NATO SECRET, na podstawie uchwały nr …. Zarządu Spółki z dnia dd mm rr w sprawie ……...

z a r z ą d z a m:

§1

1. Likwidację stanowiska Pełnomocnika Zarządu Spółki ds. Ochrony Informacji Niejawnych – samodzielnego stanowiska pracy i rozwiązanie stosunku pracy z zatrudnionym na tym stanowisku pracownikiem Spółki, zwanym dalej „Pełnomocnikiem", na zasadach i w trybie określonym niniejszym zarządzeniem.

2. Likwidację ww. stanowiska przeprowadzi Komisja Likwidacyjna, dalej „Komisja", w składzie:

Przewodniczący – imię i nazwisko, imię ojca i PESEL, członek zarządu Spółki, posiadający ważne poświadczenie bezpieczeństwa i aktualne zaświadczenie o odbyciu szkolenia z zasad ochrony informacji niejawnych;

Członek – wyznaczony przez Przewodniczącego Komisji pracownik Spółki, posiadający takie uprawnienia dostępu do informacji niejawnych, jak Przewodniczący.

3. Przewodniczący Komisji, z udziałem Pełnomocnika, opracują i przedstawią do akceptacji harmonogram wykonania przedsięwzięć, o których mowa w ust. 1.

4. Likwidacja ww. stanowiska będzie uznana za dokonaną po wykonaniu wszystkich przedsięwzięć, ujętych w ww. harmonogramie, i przedstawieniu protokołu likwidacji, podpisanego przez Przewodniczącego Komisji i Pełnomocnika.

5. Rozwiązanie stosunku pracy z Pełnomocnikiem może być dokonane z końcem miesiąca kalendarzowego, w którym zaakceptowany zostanie protokół likwidacji ww. stanowiska.

§ 2

Przewodniczący Komisji:

1) odpowiada za terminową realizację przedsięwzięć ujętych w ww. harmonogramie;

2) ma prawo uzupełnić skład Komisji o kolejnego pracownika Spółki, spełniającego wymagania, o których mowa w ust.1 i 2 §1;

3) może zażądać współpracy przy realizacji ww. harmonogramu od każdego pracownika Spółki.

4) Komisja ujmie w harmonogramie swego działania także przedsięwzięcie polegające na przeglądzie i selekcji dokumentacji likwidowanego stanowiska pracy, z wyłączeniem imiennych Akt Zwykłych Postępowań Sprawdzających, celem wydzielenia spośród nich dokumentacji niemającej wartości archiwalnej i dokonania komisyjnego jej zniszczenia.

§ 3

Pełnomocnik jest zobowiązany do ścisłej współpracy z ww. Komisją, nie może być jednak włączony w jej skład. Pełnomocnik odpowiada w szczególności za:

1. Opracowanie jako jednostki archiwalne, oznaczone kategorią archiwalną B20, wytworzonych przez okres swojej działalności w Spółce imiennych Akt Zwykłych Postępowań Sprawdzających i sporządzenie przesyłki, celem przekazania ich do Archiwum Wydzielonego Agencji Bezpieczeństwa Wewnętrznego.

2. Przygotowanie przesyłki z imiennymi Aktami Zwykłych Postępowań Sprawdzających, wytworzonymi i opracowanymi jako jednostki archiwalne przez osoby pełniące w przeszłości funkcję pełnomocników Zarządu Spółki ds. Ochrony Informacji Niejawnych, celem przekazania ich do Archiwum Wydzielonego Agencji Bezpieczeństwa Wewnętrznego.

3. Współpracę z ww. Komisją w okresie realizacji przez nią przedsięwzięć ujętych w ww. harmonogramie, w szczególności podczas dokonywania przez Komisję przeglądu i selekcji dokumentów likwidowanego stanowiska pracy na archiwalne i niemające wartości archiwalnej oraz sporządzenia protokołu zniszczenia dokumentów niezaliczonych do archiwalnych, a także nadzór nad fizycznym procesem ich ostatecznego zniszczenia. Protokół zniszczenia, o którym mowa wyżej, po podpisaniu go przez członków Komisji, podlega przedstawieniu mi do akceptacji. Ostateczne, fizyczne zniszczenie wyszczególnionych w nim dokumentów likwidowanego stanowiska pracy może nastąpić dopiero po zaakceptowaniu protokołu zniszczenia i zezwoleniu na ostateczne, fizyczne zniszczenie wyszczególnionych w nim dokumentów.

§ 4

1. Zarządzenie wchodzi w życie po siedmiu dniach roboczych, od dnia jego podpisania.

2. Komisja przedstawi mi do akceptacji ww. harmonogram po upływie siedmiu dni roboczych od dnia wejścia w życie niniejszego zarządzenia.

3. Zarządzenie podlega ogłoszeniu w sieci LAN Spółki, niezwłocznie po jego podpisaniu. Szefowie komórek organizacyjnych Spółki mają obowiązek sprawdzenia, czy podlegli im pracownicy zapoznali się z jego treścią.

Prezes Zarządu

……...

(pieczęć imienna i podpis)

WZÓR NR 2

…….. HARMONOGRAM

(pieczęć imienna i podpis PZ lub KJO[1])

przedsięwzięć likwidacyjnych stanowiska pracy Pełnomocnika Zarządu ds. Ochrony Informacji Niejawnych [POIN] w ……Sp. z o.o.[Spółka].

Lp.	Nazwa przedsięwzięcia	Termin realizacji	Odpowiedzialny za realizację	Uwagi i zalecenia
1	2	3	4	5
1	Opracowanie i przedstawienie do akceptacji harmonogramu [H]	X[2]+7 dni roboczych [DR]	Przewodniczący Komisji Likwidacyjnej [PKL]	H podpisują PKL i POIN
2	Opracowanie jako jednostki archiwalne imiennych AZPS[3] założonych przez POIN	1 DR na jedne AZPS	POIN	Wykonuje to jednoosobowo POIN
3	Sporządzenie przesyłki [P] z AZPS założonych przez POIN i odrębnej przesyłki z AZPS, założonych przez poprzednika(ów) POIN	1 DR na każdą P	POIN	Uwaga – jak wyżej
4	Sporządzenie wykazu mienia i innego wyposażenia stanowiska pracy POIN, podlegającego zwrotowi Spółce przez POIN	1-2 DR	POIN	Wykaz podlega akceptacji przez PZ lub KJO
5	Analiza i ocena dokumentacji stanowiska pracy POIN i dokonanie podziału na dokumenty archiwalne i niearchiwalne	3-5 DR	PKL+POIN	W analizie i ocenie może brać więcej członków KL[4]
6	Sporządzenie protokołu zniszczenia dokumentów niearchiwalnych i przedstawienie go do akceptacji PZ	1-2 DR	PKL+POIN	Zniszczenie komisyjne tych dokumentów nadzoruje POIN
7	Sporządzenie wykazu dokumentów likwidowanego stanowiska pracy pozostających w aktach Spółki	1 DR	PKL+POIN	Dokumenty te, tylko jawne, przekazać „za podpisem" do KED[5] w Spółce
8	Przekazanie do Archiwum Wydzielonego ABW przesyłek, o których mowa w pkt 3 harmonogramu	1 DR	POIN	Dokonuje osobiście POIN, PKL zapewnia transport
9	Przekazanie wskazanemu pracownikowi Spółki mienia i wyposażenia, ujętego w Wykazie, o którym mowa w pkt 4 harmonogramu	1-2 DR	POIN i wskazany przez PZ, KJO lub PKL pra-cownik Spółki	Przekazania do-konać „za podpisem" na Wykazie …
10	Sporządzenie Protokołu likwidacji stanowiska pracy POIN w Spółce i przedłożenie go do akceptacji PZ	1-3 DR	PKL+POIN	Protokół podpisują wszyscy członkowie KL i POIN
11	Akceptacja ww. Protokołu przez PZ	1 DR (X+30-45 DR)	PZ+PKL+POIN	Protokół do akceptacji przedstawić wraz z załącznikami.
12	Sporządzenie dokumentacji rozwiązania stosunku pracy z POIN	1-2 DR	Kierownik komórki pracowniczej Spółki	Niezwłocznie po wykonaniu zadania pod lp.11
13	Rozwiązanie stosunku pracy z POIN	1 DR	PZ	Termin określa §1 ust. 5 zarządzenia (wzór nr 1)

Podpisy:

Pełnomocnik …….

Przewodniczący Komisji Likwidacyjnej ……..

[1] PZ – Prezes Zarządu. Harmonogram może też akceptować KJO (jeżeli nie jest nim PZ), a w treści zarządzenia przewidziano taką możliwość.
[2] Dzień wejścia w życie Zarządzenia w sprawie likwidacji stanowiska pracy POIN.
[3] AZPS – Akta Zwykłych Postępowań Sprawdzających.
[4] KL – Komisja Likwidacyjna.
[5] KED – komórka ewidencjonująca dokumenty.

Zatem niezbędnymi dokumentami poświadczającymi prawomocność i zgodność z prawem przedsięwzięć likwidacyjnych ww. stanowiska pracy powinny być:

1. uchwała zarządu (rady nadzorczej lub zgromadzenia udziałowców/akcjonariuszy) podmiotu o likwidacji samodzielnego stanowiska pracy pełnomocnika zarządu ds. ochrony informacji niejawnych;
2. zarządzenie powołujące komisję likwidacyjną ww. stanowiska;
3. harmonogram przedsięwzięć likwidacyjnych wraz z dokumentami poświadczającymi sposób i terminowość ich wykonania;
4. protokół komisyjnego zniszczenia dokumentów likwidowanego stanowiska, ocenionych przez komisję jako niemające wartości archiwalnej;

WZÓR NR 3

AKCEPTUJĘ
i zezwalam na zniszczenie
……..
(pieczęć imienna i podpis PZ)

PROTOKÓŁ nr …./20….
zniszczenia dokumentów likwidowanego samodzielnego stanowiska pracy
Pełnomocnika Zarządu ds. Ochrony Informacji Niejawnych.

Lp.	Nazwa nośnika (dokumentu)	Klauzula tajności i nr ewidencyjny	Liczba stron (arkuszy)	Adnotacja o zniszczeniu nośnika (dokumentu) w UE[6]
1	2	3	4	5
1	Dokument – wykaz pracowników Spółki posiadających ważne poświadczenia bezpieczeństwa	ZASTRZEŻONE Nr ewid. Z-1/2010	10 str. A4 wydruku komputerow.	Adnotacji o zniszczeniu w UE dokonał POIN
2	Nośnik – dysk twardy 250 GB z zapisem elektronicznym dokumentów POIN + karta zapisu nośnika [KZN]	ZASTRZEŻONE nr ewid. Z-1/2011	KZN-6 str. form. A6, Dysk - zapisane 35 GB	Dysk przekazano administratorowi LAN Spółki celem skasowania zapisów i zniszczenia metodą chemiczną.
n	……	……	……	……

Razem pozycji n.

Wyselekcjonowania nośników (dokumentów) do zniszczenia i ich ostatecznego zniszczenia dokonała Komisja, wyznaczona przez Prezesa Zarządu Spółki Zarządzeniem nr …. z dnia dd mm rr w sprawie likwidacji samodzielnego stanowiska pracy Pełnomocnika Zarządu ds. Ochrony Informacji Niejawnych w składzie:

1. Przewodniczący – imię i nazwisko, imię ojca, nr PESEL.
2. Członek – dane jw.

Podpisy:
1. Przewodniczącego:……
2. Członka:……..

Zniszczenia nośników i dokumentów dokonano w mojej obecności:

1. Dokumentów – przez pocięcie w maszynie do cięcia papieru.
2. Nośników komputerowych – przez rozpuszczenie w mieszaninie związków chemicznych, po uprzednim skasowaniu zapisów metodami elektronicznymi, dokonanym w mojej obecności.
3. Proces niszczenia nośników i dokumentów zarejestrowano metodami fotograficznymi. Nośnik z ww. zapisem stanowi załącznik do niniejszego protokołu.
4. Protokół ten, wraz z załącznikiem, powinien być dołączony do protokołu likwidacji samodzielnego stanowiska pracy Pełnomocnika Zarządu ds. Ochrony Informacji Niejawnych.

Pełnomocnik

……..
(pieczęć imienna i podpis)

[6] UE – urządzenie ewidencyjne, w którym ujęto zniszczony nośnik. Rubryki nie wypełnia się, jeżeli zniszczony nośnik (dokument) nie był opatrz klauzulą tajności i/lub nie miał numeru ewidencyjnego, świadczącego o wpisaniu do urządzenia ewidencyjnego, np. dziennika korespondencji.

5. dokument (dokumenty) potwierdzający (potwierdzające) przekazanie do Archiwum Wydzielonego ABW wytworzonych i przechowywanych przez pełnomocnika zarządu ds. ochrony informacji niejawnych podmiotu imiennych AKT Zwykłych Postępowań Sprawdzających przeprowadzonych wobec pracowników podmiotu;
6. protokół komisji z jej działań związanych z likwidacją ww. stanowiska;
7. dokumentacja rozwiązania z pełnomocnikiem stosunku pracy.

Do modelowych wzorów omawianych w artykule dokumentów należą: • zarządzenia w sprawie likwidacji samodzielnego stanowiska pracy pełnomocnika zarządu ds. ochrony informacji niejawnych • harmonogramu przedsięwzięć likwidacyjnych samodzielnego stanowiska pracy pełnomocnika zarządu ds. ochrony informacji niejawnych • protokołu komisyjnego zniszczenia dokumentów niemających

WZÓR NR 4

AKCEPTUJĘ

……..……

(pieczęć imienna,
data i podpis PZ)

Kategoria archiwalna B10

PROTOKÓŁ[7]

likwidacji samodzielnego stanowiska pracy Pełnomocnika Zarządu …… Sp. z o.o. ds. Ochrony Informacji Niejawnych.

W dniach od dd mm rr do dd mm rr Komisja w składzie:

1. Przewodniczący: imię i nazwisko, imię ojca, nr PESEL
2. Członek: imię i nazwisko, imię ojca, nr PESEL

powołana Zarządzeniem Prezesa Zarządu …. Sp. z o.o. nr …… z dnia dd mm rr, w sprawie …….. wykonała, przy udziale Pełnomocnika, czynności likwidacyjne ww. stanowiska, wyszczególnione w harmonogramie, stanowiącym załącznik do niniejszego protokołu, który przedłożono do akceptacji Prezesowi Zarządu …… Sp. z o.o. w dniu dd mm rr. Data przedłożenia do zaakceptowania tego protokołu jest datą likwidacji ww. stanowiska.

Komisja i Pełnomocnik nie wnoszą zastrzeżeń do treści niniejszego protokołu i dołączonych do niego załączników[8].

Podpisy:

Pełnomocnika:

……..

Członków Komisji:

1. ……

2.……

Załączniki:

1. Harmonogram czynności likwidacyjnych samodzielnego stanowiska pracy Pełnomocnika Zarządu ….. Sp. z o.o. ds. Ochrony Informacji Niejawnych.
2. Dokumenty poświadczające przekazanie przez Pełnomocnika Zarządu ….. Sp. z o.o. ds. Ochrony Informacji Niejawnych przesyłek z Aktami Zwykłych Postępowań Sprawdzających do Archiwum Wydzielonego Agencji bezpieczeństwa Wewnętrznego, za pośrednictwem Biura Podawczego ABW na ul. Rakowieckiej 2A w Warszawie.
3. Protokół zniszczenia dokumentów niearchiwalnych z dokumentacji likwidowanego stanowiska pracy.
4. Wykaz dokumentów archiwalnych z likwidowanego stanowiska pracy przekazanych do komórki ewidencjonującej dokumenty w ……. Sp. z o.o. (tylko dokumenty nieklasyfikowane).
5. Wykaz wyposażenia i innych elementów mienia ….. Sp. z o.o. przekazanych przez Pełnomocnika pracownikowi wskazanemu przez Prezesa Zarządu/Członka Zarządu.

[7] Kopię protokołu, wraz z załącznikami 1, 2 i 5 przekazuje się Pełnomocnikowi Ochrony Informacji Niejawnych.

[8] Jeżeli któraś ze stron wnosi zastrzeżenia, podpisuje protokół i formułuje zastrzeżenia pisemnie (w formie wydruku komputerowego), podpisuje go i dołącza do protokołu.

wartości archiwalnej likwidowanego stanowiska pracy i protokołu komisji z wykonania przedsięwzięć likwidacyjnych. Wzory tych dokumentów odzwierciedlają szczególne warunki prawno-organizacyjne przedsiębiorstwa, w którym likwidowano samodzielne stanowisko pracy POIN. Nie mogą być one wprost i bez istotnych zmian, uzależnionych od sytuacji prawnej i organizacyjnej innych przedsiębiorstw, w których są lub mogą być likwidowane piony ochrony informacji niejawnych lub samodzielne stanowiska pracy POIN, w sytuacji posiadania przez te przedsiębiorstwa innych rodzajów świadectw bezpieczeństwa przemysłowego.

Doradzając podmiotom prawa handlowego w sytuacjach podobnych do opisanych, która w tym przypadku nie była najbardziej skomplikowana, autor spotykał się kilkakrotnie z następującymi pytaniami:

- Po co ta biurokracja?
- Czy nie można zniszczyć komisyjnie całej dokumentacji likwidowanej komórki organizacyjnej albo likwidowanego stanowiska pracy?
- Dlaczego nie da się *lege artis* dokonać czynności likwidacyjnych w ciągu kilku dni roboczych?
- Czy pełnomocnik nie może wziąć świadectwa pracy, należnej odprawy i ewentualnie wynagrodzenia za niewykorzystany urlop wypoczynkowy i pozostawić prezesowi zarządu i/lub kierownikowi jednostki organizacyjnej kłopotu z wykonaniem dalszych czynności prawno-organizacyjnych?

Odpowiedź jest krótka: NIE.

Wyczerpujące odpowiedzi na te i inne pytania związane z likwidacją pionu ochrony informacji niejawnych lub stanowiska pracy POIN wymagają przedstawienia brzmienia konkretnych przepisów prawa ochrony informacji niejawnych, przepisów prawa ochrony danych osobowych, przepisów prawa o narodowym zasobie archiwalnym i archiwach oraz przepisów prawa pracy, a także wynikających z tych przepisów obowiązków pełnomocnika, prezesa zarządu i/lub kierownika jednostki organizacyjnej oraz zagrożeń karnych, służbowych i/lub dyscyplinarnych, grożących sprawcom niewykonania tych przepisów lub ich niedbałego wykonania. Tematyka będzie kontynuowana na łamach „a&s Polska”.

BIO

Marek Ryszkowski
Dr inż., ekspert KSOIN, autor licznych artykułów i kilku książek z zakresu prawa ochrony informacji niejawnych, były pełnomocnik ochrony informacji niejawnych w kilku podmiotach prawa handlowego.

Kwalifikacje projektantów systemów sygnalizacji pożarowej

Zgodnie z zapowiedzią przedstawioną w nr. 4/2017 „a&s Polska" Stowarzyszenie NOWACERT organizuje seminarium poświęcone opisom kwalifikacji rynkowych projektantów systemów sygnalizacji pożarowej. Zostaną zaprezentowane projekty opisów kwalifikacji, jakie opracowało Stowarzyszenie NOWACERT we współpracy z Instytutem Badań Edukacyjnych (IBE), odbędzie się też dyskusja nt. treści tych opisów w gronie specjalistów. Po uzgodnieniu ostatecznej wersji opisy zostaną zgłoszone do Zintegrowanego Rejestru Kwalifikacji. Jeżeli przejdą „cierniową drogę" we właściwym ministerstwie, zostaną opublikowane w Monitorze Polskim jako obwieszczenie o włączeniu kwalifikacji rynkowej do Zintegrowanego Systemu Kwalifikacji. Tak zdefiniowane kwalifikacje rynkowe będą mogły być wykorzystywane przez jednostki certyfikujące do walidacji i certyfikacji specjalistów. Projekt ma charakter środowiskowy. Obwieszczenie ministra nie będzie zawierało żadnej informacji o autorze opisu kwalifikacji. Walidację i certyfikację będzie mogła prowadzić dowolna jednostka certyfikująca, która zdobędzie uprawnienia w tym zakresie.

Opisy kwalifikacji będą dostępne zarówno dla firm szkoleniowych, jak i dla pracodawców. Pozwoli to dobrze określić podstawowy zakres szkoleń, a także umiejętności posiadacza certyfikatu poświadczającego posiadanie odpowiednich kwalifikacji. Projekty opisów kwalifikacji powinny zostać wypracowane przez branżę, przedyskutowane w gronie praktyków – projektantów systemów sygnalizacji pożarowej, kierowników pracowni projektowych, menedżerów firm usługowych działających w branży ochrony przeciwpożarowej, szkoleniowców itd. Stowarzyszenie NOWACERT, we współpracy z IBE, opracowuje także opisy innych kwalifikacji z zakresu ochrony przeciwpożarowej. Zapraszamy do współpracy.

Seminarium odbędzie się 14 listopada w Warszawie. Udział jest bezpłatny, ale ze względu na ograniczoną liczbę miejsc, wyłącznie z zaproszeniami. Zgłoszenia należy przesyłać do 10 października na: *biuro@nowacert.org* **Formularz zgłoszeniowy jest dostępny na:** *www.nowacert.org*

Bezpieczne wykrywanie zagrożeń w otoczeniu budynku dzięki Pyronix

Nowa zewnętrzna czujka XDL12TT-AM firmy Pyronix niezawodnie wykrywa intruza w promieniu 12 m.

Czujka wykorzystuje dwa niezależne czujniki PIR i jeden czujnik mikrofalowy oraz logikę wykrywania na podstawie trzech sygnałów *Tri-Signal Detection Logic*. Wszystkie trzy czujniki muszą zostać aktywowane jednocześnie, aby czujka wygenerowała alarm. Zwiększa to odporność czujki na zakłócenia i ogranicza fałszywe alarmy.
Czujka jest odporna na zwierzęta. Górny czujnik PIR wykrywa intruzów w kierunku „na zewnątrz i w górę", a dolny „na zewnątrz i w dół". Ich strefy wykrywania nie nakładają się na siebie. Nawet duży pies lub kot, który wejdzie w płaszczyznę objętą zasięgiem dolnego czujnika PIR, nie jest wystarczająco wysoki, aby wejść również w górną płaszczyznę PIR. Nie zostanie więc wygenerowany alarm.

Wpływ otoczenia
W urządzeniu zastosowano funkcję analizy przeciwdziałającej efektom ruchu roślin. Obudowa czujki z grubego poliwęglanu pokrytego filtrem UV ma IP55.

Próby manipulacji
Czujka jest zabezpieczona przed manipulacjami. Zastosowano funkcje *antymasking* i *antyblocking*. Opatentowana technologia *antymaskingu* stopnia 3 chroni przed próbami zamaskowania każdego z czujników takimi materiałami jak tektura, taśma klejąca, farba w sprayu, lakier czy folia aluminiowa. Technologia *antyblockingu* stopnia 4 uniemożliwia uzbrojenie systemu, jeśli coś zasłania pole widzenia któregoś z czujników. Aby więc uzbroić system, trzeba najpierw usunąć przeszkodę.

Duży ruch na drogach
XDL12TT-AM może mieć charakterystykę wolumetryczną lub kurtynową. Można zamaskować wybraną soczewkę, aby ograniczyć obszar objęty zasięgiem. Przydaje się to szczególnie w miejscach, w których chroniony obiekt znajduje się w pobliżu drogi lub chodnika. Można też tak zamontować czujkę, aby uzyskać dowolny kąt widzenia i obrys zasięgu. Czujka może działać w jednym z trzech pasm częstotliwości, co zapobiega interferencjom z inną czujką zainstalowaną w pobliżu. Stosując stały wspornik montażowy z dwiema czujkami ustawionymi tyłem do siebie, można uzyskać obszar zasięgu w zakresie 180° w promieniu 24 m.

Łatwa instalacja
Zastosowano *buzzer* testu przejścia, regulowany kąt PIR i zakres mikrofal, kontrolki stanu LED, nawiercone otwory na kable z możliwością wyboru rezystorów końca linii.

VX Shield : niezawodna detekcja i nowoczesny wygląd

Oferta urządzeń OPTEX została wzbogacona o nową serię czujek Shield. Produkty z tej linii opracowano z myślą o jak najlepszym dopasowaniu do potrzeb klientów.

Czujki VX Shield stanowią unikalne połączenie najbardziej zaawansowanych technologii (znanych już z serii VXi) z nowoczesnym wyglądem. W serii VXS zastosowano ponadto kilka rozwiązań ułatwiających montaż i konfigurację:

- zamknięcie obrotowe (90º),
- wbudowaną poziomicę, która pozwala łatwo ocenić, czy czujka zamontowana jest równolegle do podłoża,
- elastyczne modelowanie obszaru detekcji.

Funkcja antymaskingu jest dostępna we wszystkich czterech modelach czujek serii VX Shield.

Model	Metoda detekcji	Zasilanie
VXS-AM	PIR	przewodowe
VXS-RAM	PIR	bateryjne
VXS-DAM	PIR+MW	przewodowe
VXS-DRAM	PIR+MW	bateryjne

Więcej informacji na www.optex.com.pl

System PAVIRO firmy Bosch: rozszerzone funkcje i możliwość stosowania w większych instalacjach

System nagłośnieniowy i dźwiękowy system ostrzegawczy PAVIRO firmy Bosch oferuje teraz nowe rozwiązania sprzętowe i programowe, które rozszerzają jego funkcjonalność i umożliwiają stosowanie systemu w większych instalacjach dzięki najnowocześniejszej technologii IP.

Dzięki wykorzystaniu technologii IP system PAVIRO oferuje najwyższą jakość odtwarzania dźwięku i minimalne czasy opóźnień. Możliwość wykorzystania sieci istniejących w infrastrukturze budynku oznacza także szybszą instalację i niższe koszty wdrożenia.
Za pośrednictwem protokołu IP system PAVIRO można zintegrować z innymi urządzeniami, takimi jak komputery czy laptopy, co umożliwia efektywną zdalną kontrolę, diagnozę i konserwację systemu przez Internet.

fot. Bosch

Funkcjonalność sieciową i komunikację PAVIRO zawdzięcza nowemu modułowi interfejsu sieci Dante (OM-1) firmy Bosch. Umożliwia on stworzenie 16-kanałowej sieci audio Dante pomiędzy poszczególnymi kontrolerami, co oznacza poprawę zasięgu. Ponadto architektura sieci IP umożliwia użytkownikom tworzenie topologii z wieloma kontrolerami do obsługi większych terenów za pośrednictwem maksymalnie czterech zdecentralizowanych kontrolerów. Kolejną zaletą jest mniejsza ilość kabli.
W najszerszej konfiguracji system PAVIRO może obsługiwać do 984 stref, zapewniając sumaryczną moc wzmacniaczy 164 000 W. Jest zatem odpowiednim rozwiązaniem do większych instalacji o dużej liczbie wymaganych stref i głośników.

Może być także stosowany w istniejących instalacjach, gdy infrastruktura budynku wymaga zmian i rozszerzenia systemu o kolejne pomieszczenia. Konfiguracja sieci zapewnia kanały redundantne, co podnosi bezpieczeństwo obiektu, nawet gdy kontroler straci połączenie z siecią.
System PAVIRO został wyposażony w monitoring stref głośników i 30-minutową pamięć *flash*, która umożliwia nagranie komunikatów ewakuacyjnych.
PAVIRO ma certyfikat EN 54 firmy Bosch, co pozwala architektom, planistom i projektantom spełnić wymagania określone w dokumentacji wielu przetargów.
System PAVIRO jest idealnym wyborem dla mniejszych i średnich biur, średniej wielkości hoteli, fabryk, szkół i domów towarowych.

Axis: nowa wersja Zipstream dla kamer 360° i 4K

Axis Communications przedstawił podczas IFSEC 2017 nową wersję techniki kompresji Zipstream, która jest w stanie sprostać wymaganiom dotyczącym transferu i przechowywania danych przez kamery panoramiczne o kącie widzenia 360° oraz urządzenia generujące obraz w rozdzielczości 4K. Firma wprowadziła do swojej oferty również dwie nowe kamery kopułkowe zapewniające obraz w wysokiej rozdzielczości w zakresie 360°.

Wymagania klientów stawiane systemom dozoru wizyjnego mogą wydawać się sprzeczne: z jednej strony to stałe pragnienie poprawy jakości, rozdzielczości i zasięgu widzenia kamer, z drugiej zaś rosnąca potrzeba kontroli kosztów w zakresie wykorzystania łączy oraz przechowywania danych.
Axis Communications odpowiada na te potrzeby, systematycznie ulepszając swoją sztandarową technologię kompresji strumienia wizji Zipstream. *Przechowywanie danych i przepustowość łącza to istotne elementy całkowitych kosztów systemu dozoru. Zipstream pozwala zminimalizować wymagania bez utraty szczegółów rejestrowanego obrazu* – mówi Jan T. Gruszczynic, Sales Engineer/Technical Trainer w Axis Communications. – *Cieszymy się, że teraz Zipstream działa także z kamerami panoramicznymi i Ultra-HD.*
Firma zaprezentowała dwie nowe kopułkowe kamery sieciowe AXIS M3047-P oraz AXIS M3048-P, które wykorzystują ulepszoną technologię Zipstream, dzięki czemu są w stanie zapewnić obraz w zakresie 360° w przystępnej cenie.
Atrakcyjna, mniejsza niż w poprzednich wersjach konstrukcja sprawia, że nowe kamery są płaskie i nie mają dodatkowej kopuły nad soczewką. Dzięki temu są nie tylko bardziej dyskretne, ale także wyeliminowano ryzyko pojawienia się refleksów w kopule. Jako wyposażenie dodatkowe dla obu modeli są dostępne obudowy odporne na uszkodzenia oraz wersje w kolorze czarnym.
Kamery obsługują zarówno wewnętrzny, jak i zewnętrzny *dewarping* (funkcje korekcji perspektywy obrazu panoramicznego w celu usunięcia zniekształceń). Płynną obróbkę obrazu w pełnym obszarze 360° ułatwiają aplikacja *AXIS Camera Station*, a także inne systemy do zarządzania wizją zarówno podczas podglądu na żywo, jak i na nagranych materiałach.
W modelu AXIS M3047-P zastosowano przetwornik obrazu o rozdzielczości 6 Mpix, w AXIS M3048-P o rozdzielczości 12 Mpix. Oba urządzenia zapewniają pełnoekranowy obraz o doskonałej jakości, korekcję ostrości oraz wysoką czułość.
Połączenie nowych kopuł 360° z najnowszą wersją technologii Zipstream to opłacalne rozwiązanie dla klientów – zapewnia kompleksowo pokrycie monitorowanego obszaru, jednocześnie gwarantując o szczegółowość panoramicznego obrazu podczas przesyłania i przechowywania danych – dodaje Jakub Kozak, Sales Manager - Poland, Ukraine, Baltics w Axis Communications.

Nagroda dla Dahua NVR5224-24P-4KS2

ePoE NVR NVR5224-24P-4KS2 firmy Dahua zdobył nagrodę *2017 Security Best New Product Award* **za spektakularną transmisję na odległość 800 metrów!**

Konkurs *2017 Security Best New Products* sponsorowany przez Sony to święto najbardziej innowacyjnych produktów, które trafiły na rynek australijski w ciągu ostatnich 12 miesięcy. Produkty zostały ocenione za oryginalność, wpływ innowacji i mierzalne korzyści przez wymagających sędziów ds. bezpieczeństwa. Nowy ePoE NVR firmy Dahua wyróżniał się spośród zgłoszonych ponad 50 produktów.

Zdobycie nagrody *2017 Security Best New Product Award* to duże uznanie, a także rekomendacja światowych ekspertów.
Dahua NVR5224-24P-4KS2 to 24-kanałowy NVR zdolny do przesyłania danych na odległość do 800 m między kamerą a NVR-em. To ogromny wzrost odległości w porównaniu z dystansem ograniczonym do 100 m w tradycyjnych sieciach IP.

Dahua, kontynuując działalność w kierunku „innowacji, jakości i usług", będzie dostarczać klientom produkty i usługi najwyższej klasy.

EZVIZ, czyli *easy vision* Nowa linia biznesowa grupy Hikvision

***Smart home* to obecnie jeden z najdynamiczniej rozwijających się rynków. Systemy *smart home* adresowane głównie na rynek mieszkań, domów i małych biur będą miały wpływ na dalszy rozwój branży security (podobnie jak przenikanie się branż IT i zabezpieczeń). Zadecydują o tym zmieniające się potrzeby użytkowników rynków małego i średniego biznesu (SMB), SOHO i mieszkaniowego. W trend ten doskonale wpisuje się Ezviz – nowa linia biznesowa Grupy Hikvision.**

W ofercie Ezviz dominują kamery dozorowe przeznaczone na rynki SMB, SOHO i mieszkaniowy. Firma nie poprzestaje jednak na ofercie urządzeń telewizji dozorowej, wzbogacając ją o bezprzewodowy system czujek ruchu, zalania i kontaktronów z eHubem A1 obsługującym do 32 czujników. Współpracując z kamerami, system umożliwia wizyjną weryfikację zdarzenia z poziomu aplikacji *Ezviz mobile* na ekranie smartfonu.
Docelowo system Ezviz pozwoli również na sterowanie oświetleniem i innymi urządzeniami elektrycznymi, a także wideodomofonami, które w przyszłości stworzą wszechstronny ekosystem Ezviz.

Koncepcja systemu Ezviz opiera się na intuicyjności i elastyczności rozwiązań przeznaczonych dla użytkownika końcowego. Dlatego wszystkie urządzenia Ezviz można obsługiwać za pomocą aplikacji mobilnej Ezviz na smartfon, a instalacja czy dodanie kamery lub innego urządzenia przebiega w kilku prostych krokach.
Intuicyjna aplikacja na smartfonie pozwala użytkownikowi łączyć się ze swoim domem czy miejscem pracy z dowolnego miejsca będącego w zasięgu Internetu. Ezviz pozwala spełnić codzienne potrzeby użytkownika, począwszy od monitorowania snu dziecka, przez możliwość pozostania w kontakcie z bliskimi podczas wyjazdów, na podstawowym dozorze wizyjnym firmy czy domu skończywszy.
Obraz z kamer może być rejestrowany lokalnie na karcie microSD w kamerze lub na rejestratorze sieciowym.
Rosnący popyt na rozwiązania sektora *smart home* otwiera też nowe możliwości rozwoju dla firm instalacyjnych i dystrybutorów systemów zabezpieczeń. Zainteresowanych zachęcamy do bezpośredniego kontaktu przez stronę www.ezviz.eu/pl lub z dystrybutorami: Promitel, ABC Data i Security Office.

Doroczne spotkanie Axis Partners' Day

Nowe produkty, ambitne plany na kolejny rok i podsumowanie programu partnerskiego Axis 2017 – tak wyglądała tegoroczna edycja Axis Partners' Day. Firma już po raz drugi zaprosiła gości do warszawskiego domu handlowego VITKAC.
Konferencja była okazją do podsumowania dotychczasowych projektów i przedstawienia strategicznych celów firmy na nadchodzący rok. Spotkali się na niej zarówno partnerzy, jak i dystrybutorzy Axis. Wręczono nagrody dla członków Programu Partnerskiego Axis.
Tytułem Najlepszego Partnera Roku 2017 i pamiątkową statuetką nagrodzono firmę **mvb** ze Szczecina. Za najlepszy Debiut Roku 2017 uznano **ServiceLine**, a nagrodę za Najbardziej Dynamiczny Wzrost otrzymała firma **IB Systems**. Dodatkowo wyróżnienie za najciekawszy zrealizowany projekt przyznano firmie **Elstech** za implementację jednego z pierwszych w Polsce systemów kontroli dostępu.
Zaprezentowano także plany strategiczne firmy na najbliższy rok, ze szczególnym uwzględnieniem współpracy w ramach dynamicznie rozwijanej sieci partnerskiej.
Podczas Axis Partners' Day 2017 omówiono sposób szacowania całościowych kosztów systemu zabezpieczeń na podstawie modelu całkowitego kosztu posiadania (*Total Cost of Ownership – TCO*), który pozwala uwzględnić wszystkie koszty związane z systemem dozoru wizyjnego w całym okresie jego eksploatacji.
Gościem spotkania był Grzegorz Domagała, ekspert w zakresie doskonalenia procesów sprzedaży B2B, który przedstawił założenia działania wg metody *ConsumerCentric Selling*.
Dużo uwagi poświęcono także kwestiom cyberbezpieczeństwa sieciowych urządzeń i systemów dozoru wizyjnego, kluczowego w kontekście rosnącego zagrożenia ze strony cyberprzestępców.
Zgromadzeni goście mieli okazję zapoznać się z najciekawszymi nowościami z portfolio Axis, takimi jak kamery wykorzystujące technologię radarową, a także z zapowiedziami zbliżających się premier rynkowych.
Eksperci zaprezentowali także koncepcję kompleksowych rozwiązań dla poszczególnych segmentów rynku, które umożliwią najlepsze wykorzystanie parametrów i technologii dostępnych w urządzeniach Axis.

Nowe technologie wsparciem dla biznesu Konferencja firm CBC i VCN

O szczegółach systemu do rozpoznawania numerów tablic rejestracyjnych VnetLPR, unikatowych funkcjach gwarantujących wysoką jakość obrazu w kamerach GenSTAR i technologiach wspierających biznes można było usłyszeć na konferencji zorganizowanej przez warszawską firmę CBC Poland i poznańską VCN.

Spotkanie, w którym uczestniczyło ponad 100 projektantów i instalatorów oraz użytkowników końcowych, odbyło się w Centrum Konferencyjnym PIAP w Warszawie. Mieli oni okazję poznać możliwości systemu VnetLPR opracowanego przez firmę VCN oraz zapoznać się z jego działaniem na konkretnych przykładach.
Zaprezentowano też kryteria doboru kamer, z którymi systemy rozpoznawania numerów tablic rejestracyjnych mogą współpracować, oraz inne zaawansowane technologie związane z usprawnianiem procesów biznesowych, m.in. *People Counting* – narzędzie służące do zliczania i monitorowania zachowań klientów oraz *VideoParagon* do wizyjnego dozoru transakcji kasowych.
Firma CBC zaprezentowała ofertę swoich dwóch marek: Computar oraz Ganz. Na specjalnie przygotowanych stoiskach można było zapoznać się z możliwościami GANZ Control – oprogramowania klasy Enterprise.

Targi Baltexpo

XIX Międzynarodowe Targi Morskie BALTEXPO były otwarte dla zwiedzających od 11 do 13 września.
Inwestycje infrastrukturalne związane z gospodarką morską i żeglugą śródlądową było przedmiotem cyklu debat. Zainteresowaniem cieszyły się debaty nt. rozwoju portów i żeglugi śródlądowej oraz programu „Batory" – budowy promów w polskich stoczniach. Trzeciego dnia targów odbyła się konferencjach dot. bezpieczeństwa, edukacji oraz ochrony środowiska morskiego.
Ofertę i osiągnięcia przedstawiło 300 firm, instytucji i organizacji z 19 krajów.
W specjalnej strefie innowacji można się było zapoznać z prototypowymi rozwiązaniami technicznymi.

Jesienna edycja Smart City Forum

VI edycja Smart City Forum odbyła się 20-21 września w warszawskim hotelu Sheraton. Nasza redakcja była oficjalnym partnerem medialnym wydarzenia.

Podczas konferencji przedstawiciele biznesu i administracji debatowali nad wieloma płaszczyznami transformacji miast, które stają się coraz bardziej inteligentne. Spotkanie pełne niezwykle ciekawych dyskusji i dużej dawki wiedzy merytorycznej przyciągnęło ponad 400 uczestników.

Jesienną edycję konferencji Smart City Forum uroczyście otworzył wiceprezydent Wrocławia Maciej Bluj. Następnie niezwykle barwną i inspirującą prezentacją podzielił się gość honorowy, Renato de Castro, ekspert *smart city* z Rio de Janeiro.

Przemiana w funkcjonowaniu miast dotyka wielu aspektów życia. Podczas siedmiu bloków tematycznych eksperci poruszyli wiele aspektów dot. inteligentnych miast. Rozpoczęto od przedstawienia wizji i planów związanych z inteligentnym zarządzaniem zasobami infrastruktury. Następnie dyskutowano o współdzieleniu tychże zasobów, m.in. w kontekście *car sharingu* czy *ride sharingu*. W kolejnym bloku prelegenci zastanawiali się, jak usprawnić procesy mobilnych płatności za usługi miejskie, aby były szybkie i bezpieczne. Dyskutowano także o założeniach i perspektywach bezpieczeństwa publicznego. Uczestnicy dowiedzieli się również, jak z perspektywy miast stosowana będzie sieć 5G i jaki jest realny termin jej wprowadzenia w Polsce. Eksperci rozmawiali także m.in. o szansach i wyzwaniach związanych z elektromobilnością oraz o inteligentnej sieci energetycznej.

Smart City Forum jest cykliczną konferencją, która stanowi platformę wymiany opinii i doświadczeń dotyczących rozwoju inteligentnych miast w Polsce. Organizatorem wydarzenia jest MMC Polska.

Targi SICUREZZA 2017: większe, ciekawsze, bardziej międzynarodowe

Trzy hale wystawiennicze, ponad 450 wystawców, bogaty program ponad 100 szkoleń i warsztatów – kolejna edycja targów SICUREZZA odbędzie się w dniach 15 – 17 listopada w Mediolanie. Czasopismo „a&s Polska" jest oficjalnym patronem medialnym targów.

Sicurezza 35 lat buduje swoją pozycję na światowym rynku security, przekształcając się z tradycyjnej imprezy targowej w globalne wydarzenie napędzające dyskusję o przyszłości branży i umożliwiające zdobycie wartościowych kontaktów.

Wymiar biznesowy

Rynek security we Włoszech rozwija się dynamicznie – całkowite obroty w tym sektorze wzrosły do 2,2 mld euro w roku 2016. Rynkiem włoskim coraz bardziej interesują się rynki światowe – na najbliższych targach Sicurezza swoje produkty zaprezentuje o 26% więcej wystawców zagranicznych niż w poprzedniej edycji. W tym roku co szósty wystawca będzie spoza Włoch. Z myślą o nich organizator uruchomił platformę *My Matching,* która umożliwia zaplanowanie spotkania wystawcy z potencjalnym klientem jeszcze przed rozpoczęciem imprezy.

Wymiar edukacyjny

Inżynierowie i instalatorzy systemów zabezpieczeń mają stały kontakt z firmami, menedżerami projektów i użytkownikami końcowymi. Instalator musi wobec tego przyjmować rolę „konsultanta", pośrednika między klientem a producentem. Powinien więc umieć przedstawić paletę możliwych rozwiązań i doradzić najlepsze. Dlatego jest ważne, by klient miał do niego zaufanie, które można zbudować jedynie na solidnej wiedzy i kompetencjach.

Rozbudowany program szkoleniowy podczas targów obejmuje ponad 100 spotkań w ciągu trzech dni, koncentrujących się na najważniejszych i najbardziej aktualnych tematach branży. Będzie więc mowa m.in. o regulacjach dotyczących prywatności i ich wpływie na pracę specjalistów, ochronie i zarządzaniu danymi, inteligentnym mieście, przeciwdziałaniu terroryzmowi, nowych normach dotyczących kwalifikacji zawodowych, rozwiązaniach Internetu Rzeczy w zastosowaniu security, wykorzystaniu sztucznej inteligencji w zabezpieczeniach czy o roli zabezpieczeń w projektowaniu budynków.

Podczas targów będą także zorganizowane specjalne strefy dedykowane najważniejszym trendom w branży security. Powstanie wioska poświęcona technologiom informatycznym oraz najbardziej innowacyjnym rozwiązaniom, szczególnie w zakresie cyberbezpieczeństwa systemów dozoru wizyjnego i Internetu Rzeczy. Ponadto największe włoskie i międzynarodowe firmy oraz szkoły sterowania UAV będą prezentować pracę dronów w specjalnie przygotowanej strefie ekspozycyjnej. Będzie można zapoznać się z modelami wykorzystywanymi do interwencji ratowniczych przez organy ścigania, policję, firmy ochroniarskie, straż pożarną czy Włoski Czerwony Krzyż w obszarach dotkniętych klęskami żywiołowymi.

Odrębna strefa powstanie dla rozwiązań systemów zabezpieczeń w handlu – tu planowane są dyskusje przedstawicieli sektora *retail* z producentami technologii security na temat dostosowania rozwiązań do potrzeb odbiorców.

Imprezy towarzyszące

Targom SICUREZZA będą towarzyszyły dwie imprezy: Smart Building Expo oraz ITASSICURA. Pierwsza z nich będzie okazją do przedstawienia koncepcji inteligentnego budynku i zapewni obszerny przegląd oferty z zakresu m.in. okablowania, Internetu Rzeczy, standardów integracji, systemów audio-wideo oraz *digital signage*. Impreza zajmie część hali nr 3 i będzie otwarta dla wszystkich odwiedzających targi SICUREZZA.

Równolegle odbędzie się dwudniowe wydarzenie dla specjalistów z branży ubezpieczeniowej. Sektor ten, który coraz częściej i bliżej współpracuje z branżą zabezpieczeń, przeżywa obecnie okres transformacji, wpływając na branżę security. Celem ITASSICURA jest zatem umożliwienie ubezpieczycielom spotkania z rynkiem security i nawiązania bliższych kontaktów.

Informacje organizacyjne

Bilet na targi SICUREZZA można zarezerwować i kupić online. Pozwoli to na ominięcie kolejek do wejścia i skorzystanie ze specjalnej Fast Line. Bilety kupione online są także tańsze – zamiast 15 euro kosztują 8 euro. Istnieje także możliwość rezerwacji biletu online i jego zakupu na miejscu – w tym przypadku cena wynosi 10 euro.

Dla wystawców i odwiedzających targi SICUREZZA pracuje także MiCodmc, oficjalna agencja podróży Fiera Milano, która pomoże w zorganizowaniu pobytu w Mediolanie.

JEDNO SŁOWO, WIELE ROZWIĄZAŃ

sferica.net

SiCUREZZA

INTERNATIONAL SECURITY & FIRE EXHIBITION

TAM, GDZIE PRODUKTY I STRATEGIE TWORZĄ ROZWIĄZANIA

Fiera Milano, Rho

W DNIACH 15-17 LISTOPADA 2017 ROKU

www.sicurezza.it

WRAZ Z

SMART BUILDING EXPO

ZAREJESTRUJ SIĘ NA STRONIE INTERNETOWEJ
WWW.SICUREZZA.IT OSZCZĘDZAJ CZAS I PIENIĄDZE!

MIĘDZYNARODOWA SIEĆ

BRASEG
BRAZILIAN TRADE SHOW FOR OCCUPATIONAL SAFETY AND HEALTH, AND FIRE PROTECTION
www.braseg.tmp.br

EXPOSEC
www.exposec.com.br

FISP
INTERNATIONAL FAIR OF SAFETY AND PROTECTION
www.fispvirtual.com.br

POD PATRONATEM

Ministero della Difesa

Città metropolitana di Milano

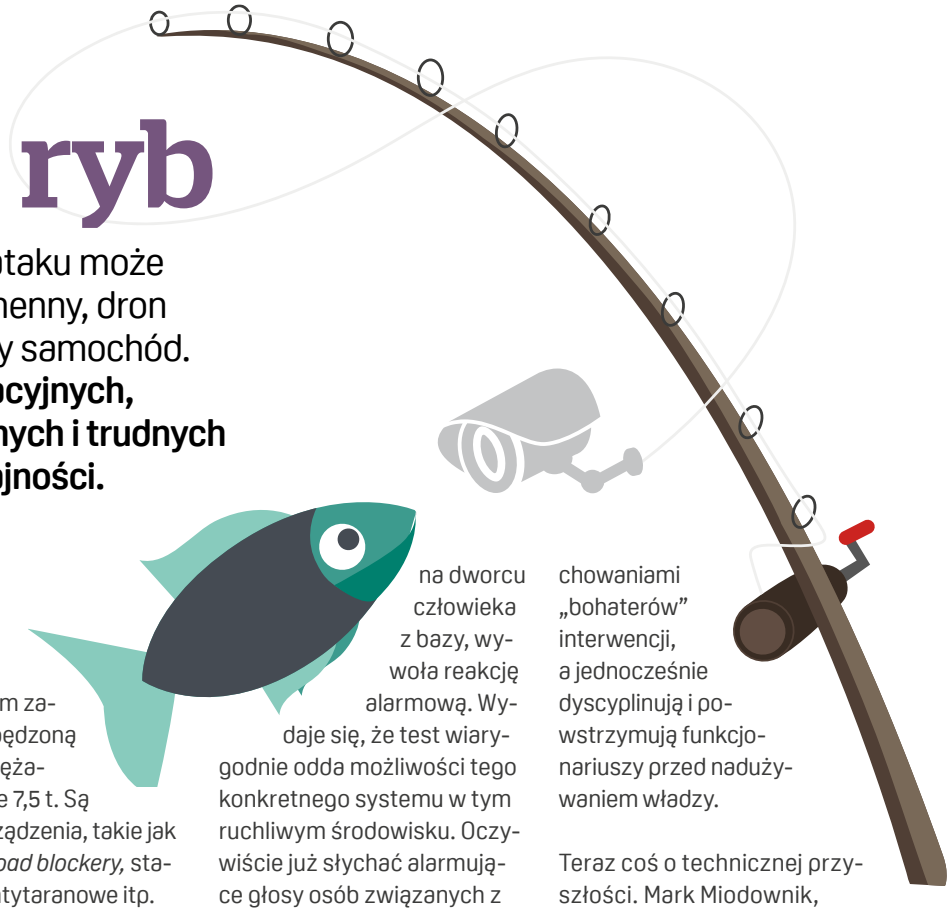
CAMERA DI COMMERCIO MILANO

ZORGANIZOWANA PRZEZ

FIERA MILANO

Sztuka łowienia ryb

Terrorysta ma coraz łatwiej. Do ataku może mu wystarczyć młotek, nóż kuchenny, dron za kilkaset złotych lub skradziony samochód. **Nie potrzebuje struktur organizacyjnych, logistyki i szkoleń – czasochłonnych i trudnych z punktu widzenia utrzymania tajności.**



Może nawet pod wpływem emocji uderzyć na tzw. wariata. Jak coś takiego przewidzieć? Trudno, bo nie ma zgody na tworzenie powszechnego systemu inwigilacji, a podglądać cudzych myśli, jeśli nie uzewnętrzniają ich jakieś działania, jeszcze nie umiemy. To zresztą straszna wizja *science fiction*: masowy, prewencyjny *skanning* głów obywateli, poza ich świadomością.

Jacek Wojciechowicz, były wiceprezydent stolicy, a obecnie prezes Instytutu Rozwoju Warszawy, zwrócił uwagę na poważną lukę w ochronie na popularnym Trakcie Królewskim. Sposób zabezpieczenia tej części miasta nie jest adekwatny do współczesnych zagrożeń. Stosowane są nieliczne barierki drewniane. Ogrodzenia metalowe ustawiane raźnie i doraźnie przez policję z okazji demonstracji „religijnych" nie zatrzymają nawet cięższej osobówki. Ratusz obiecał, że przyjrzy się propozycji, tłumacząc się mętnie tym, że zwiększono liczbę patroli pieszych (skutecznych w zderzeniu z ciężarówką?). Podpowiadam, nowoczesne zabezpieczenia mechaniczne to nie są specjalnie drogie inwestycje i nie psują wyglądu historycznej części miasta. Zapora drogowa typu wysuwany słup antyterrorystyczny zakotwiczony na głębokości ok. 2 m zatrzymuje rozpędzoną do 80 km/h ciężarówkę o masie 7,5 t. Są także inne urządzenia, takie jak zapory typu *road blockery,* stałe pachołki antytaranowe itp.

Wędkarski spławik był pra-ideą alarmu czujnika – zauważył rybę albo… nie. Firmy telewizyjne od dawna pracują nad systemami do automatycznej identyfikacji poszukiwanych osób w przestrzeniach publicznych. Ale choćby nie wiem jakie cuda w marketingowych *reality show* obiecywały, te naprawdę skuteczne istnieją tylko w amerykańskich filmach sensacyjnych. Rzadko słychać o prawdziwych pracach w tej dziedzinie. Zauważyłem więc z ciekawością, że niedawno zaczął się półroczny eksperyment na berlińskim dworcu Südkreuz. Przy wejściach i wyjściach zainstalowano kilka kamer systemu automatycznej identyfikacji. Do bazy danych „poszukiwanych osób" dobrowolnie zgłosiło się 300 chętnych. Wpisano w pamięć biometryczne zdjęcia ich twarzy oraz dane osobowe. Gdy system zauważy na dworcu człowieka z bazy, wywoła reakcję alarmową. Wydaje się, że test wiarygodnie odda możliwości tego konkretnego systemu w tym ruchliwym środowisku. Oczywiście już słychać alarmujące głosy osób związanych z ochroną danych i prywatności, że ta technologia stworzy możliwość nadużyć i poddania ludzi nieuzasadnionej kontroli. Czy są bezzasadne?

Prasa doniosła, że policja ogłosi przetarg na zakup mobilnych kamerek (na razie kilkuset), które mają nosić na mundurach policjanci z prewencji i drogówki. Trwają prace nad przetargową SIWZ oraz pilotaż sprzętu różnych firm w kilku komendach. Kamerki nasobne nie są żadną nowością, nawet w Polsce. Używają ich niektóre straże miejskie – słyszałem o Tarnowie. Jeszcze kilka lat temu były to techniczne „zabawki", teraz rejestrują i archiwizują ciągły obraz wysokiej jakości. Są przydatne, i to obustronnie – powstrzymują przed agresywnymi zachowaniami „bohaterów" interwencji, a jednocześnie dyscyplinują i powstrzymują funkcjonariuszy przed nadużywaniem władzy.

Teraz coś o technicznej przyszłości. Mark Miodownik, materiałoznawca i dyrektor Institute of Making w University College London, ocenił („Polityka" nr 32/2017), że wyzwaniem rozwojowym będzie umiejętność łączenia struktur o różnej skali w jeden duży przedmiot. Czymś takim jest już smartfon integrujący elektronikę w nanoskali z zaprojektowanym w makroskali ekranem dotykowym. Jesteśmy też coraz bliżej spełnienia wizji przedmiotów całkowicie przeniknietych obwodami elektronicznymi na podobieństwo układu nerwowego. Pewnego dnia budynki będą mogły generować energię, kierować ją w odpowiednie miejsca czy nawet samodzielnie wykrywać uszkodzenia i je naprawiać. Dlaczego nie miałyby mieć w strukturze zabezpieczeń technicznych?

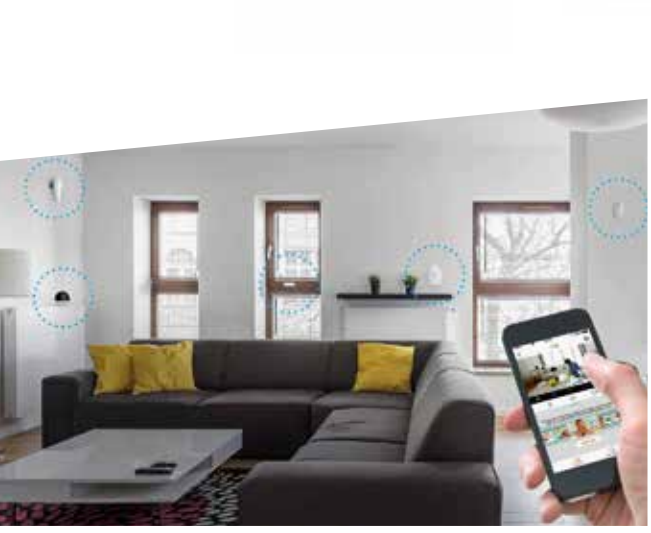
BIO

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

ezviz
Video Security For Your Smart Life

Ezviz - Bezpieczeństwo na wyciągnięcie ręki.

Dzięki Ezviz profesjonalni instalatorzy systemów zabezpieczeń mogą zmienić każdy dom lub firmę w inteligentny budynek i jednocześnie bezpieczne miejsce.



App Your Life

ODKRYJ NASZE PRODUKTY NA WWW.EZVIZ.EU/PL

Bringing Ultra HD & Color Surveillance to Darkness

Kamery 4K z przetwornikiem Starlight

- Przetwornik STARVIS 4/3” o rozdzielczości 8 Mpx
- Generowanie obrazu w czasie rzeczywistym, w jakości 4K przy 30 kl./s.
- Kompresja obrazu Smart H.265+ w czasie rzeczywistym przy przepustowości 1 Mb/s
- 120dB WDR dla zachowania jasności obrazu w całym kadrze

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