a&S POLSKA
www.aspolska.pl

CZASOPISMO RYNKU SECURITY

nr 2/2017
marzec/kwiecień

15 zł (w tym 8% VAT)

TEMAT NUMERU

Ciągłość działania obiektów i instalacji krytycznych dla funkcjonowania państwa jest dziś priorytetem

str. 44

# Bezpieczeństwo infrastruktury krytycznej

TELEWIZJA DOZOROWA

## Światowe trendy 2017

*Deep learning* i *big data*, Internet Rzeczy i *SaaS*... Przedstawiciele globalnych firm przewidują, co nas czeka w tym roku.

str. 16

CYBERBEZPIECZEŃSTWO

## Nowy front w wojnie 2.0

Ochrona przed cyberatakami jest wyzwaniem zarówno dla security managerów, jak i producentów urządzeń security.

str. 82

BEZPIECZEŃSTWO BIZNESU

## Agencje ochrony w XXI wieku

W wyniku głębokich zmian na polskim rynku ochrony komercyjnej tworzą się nowa jakość, standardy i rozwiązania.

str. 92

ISSN 2451-5175

# NR 1 NA ŚWIECIE

innowacyjna firma

jedna z najbardziej wartościowych marek na świecie

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

www.hikvision.com

# **Dla nas najważniejsze jest** bezpieczeństwo Twoich danych video.

**Ryzyko.** Nawet jeden słaby punkt w konfiguracji dozoru może narazić na szwank cały system. Zdolni hakerzy potrafią przeprowadzać ataki typu „man in the middle", przejmując kontrolę nad komunikacją pomiędzy kamerą i systemem zarządzania sygnałem wizyjnym (VMS). Gdy już uzyskają dostęp, mogą rozprowadzać inny sygnał wizyjny, by ukryć niedozwolone działania, lub manipulować obrazem na żywo i wybiórczo usuwać określone szczegóły lub osoby z kadru.

**Kontrola pod każdym kątem.** Nasze czterostopniowe podejście zapewnia kompleksową infrastrukturę nadzoru wizyjnego. Przypisanie klucza uwierzytelniającego do każdego komponentu sieci sprawia, że nasi klienci nam ufają. Chronimy dane przed hakerami, kodując je na poziomie sprzętowym. Nasze rozwiązania korzystają z klucza kryptograficznego bezpiecznie przechowywanego we wbudowanej platformie Trusted Platform Module (TPM). Oferujemy proste narzędzia do zarządzania uprawnieniami dostępu użytkowników, dzięki którym tylko upoważnione osoby mają dostęp do Twoich danych. Zapewniamy także pomoc przy konfigurowaniu infrastruktury klucza publicznego. Innymi słowy — z firmą Bosch możesz czuć się bezpiecznie.

BOSCH

Technologia bliżej nas

# Drodzy Czytelnicy

Pierwszy numer „a&s Polska" i nasza propozycja szerszego spojrzenia na czasopismo branżowe spotkały się z entuzjastycznym wręcz przyjęciem. Cieszą nas ogromnie pozytywne recenzje i opinie.

Tematem przewodnim 2. numeru „a&s Polska" jest **Bezpieczeństwo infrastruktury krytycznej**. Zapewnienie ciągłości działania obiektów i instalacji krytycznych dla funkcjonowania państwa jest tym ważniejsze, że NIK w raporcie pokontrolnym wytknął wiele nieprawidłowości w tym zakresie (s. 44). Dziennikarze i współpracujący z redakcją eksperci pokusili się o analizę tematu pod kątem zarówno wymagań prawnych, jak i stanu faktycznego. O kondycji systemu ochrony IK rozmawialiśmy także z wiceszefem Rządowego Centrum Bezpieczeństwa – polecamy wywiad z Krzysztofem Malesą (s. 46). Temat uzupełnia oferta rozwiązań branży security, będąca odpowiedzią na nowe wyzwania. Polecamy m.in. **przegląd kamer termowizyjnych** oraz promowanych obecnie rozwiązań bispektralnych (s. 39).

Należy w tym kontekście wspomnieć o **cyberzagrożeniach**. Mówi się, że w „wojnie przyszłości" atak cybernetyczny poprzedzi lub zastąpi atak militarny. Z problemem cyberataków musi sobie radzić także branża security, by zapewnić urządzeniom i systemom pełne *nomen omen* bezpieczeństwo przed sieciowymi włamaniami i zakłóceniami.

Polecamy ciekawe opracowanie dotyczące **trendów na rynku telewizji dozorowej** (s. 16). Przedstawiciele światowych firm security opowiadają o *big data* i IoT, *deep learning* i SaaS.

Piszemy też o wkładzie polskiej nauki w przyszłość branży – Politechnika Gdańska uczestniczyła w projekcie dotyczącym kontekstowego rozumienia pozyskiwanego obrazu. Prace zaowocowały trzema patentami (s. 22). Polecamy także lekturę **porad dla integratorów** systemów zabezpieczeń (s. 26), w których przedstawiciele światowych producentów security podzielili się swoimi spostrzeżeniami, wskazali najczęściej popełniane błędy i podpowiedzieli rozwiązania.

Pochlebne recenzje zbiera również dział **Bezpieczeństwo biznesu**. Ten temat dotychczas mało dostrzegany w prasie branżowej, na naszych łamach znalazł stałe miejsce. Cykl o kierunkach rozwoju agencji ochrony w Polsce (s. 92) niejako wyprzedził głośne ostatnio wydarzenie branżowe – przejęcie Konsalnetu przez China Security & Fire. Ta największa transakcja na tym rynku na pewno nie pozostanie bez echa.

Kontynuacją tematów omawianych w czasopiśmie są **śniadania ekspertów „a&s Polska"**, odbywające się po każdym wydaniu numeru. To pierwsze tego typu spotkania przedstawicieli branży security i osób odpowiedzialnych za bezpieczeństwo w firmach i instytucjach. Sądząc po opiniach uczestników i nawiązanych cennych kontaktach, premierowe śniadanie było strzałem w dziesiątkę (relacja na s. 8). Możliwość poznania się i rozmowy w nieformalnej atmosferze cieszyły się ogromnym zainteresowaniem. Zapraszamy na kolejne, poświęcone tematowi przewodniemu tego wydania (więcej na s. 81).

Przed nami także największe przedsięwzięcie i jednocześnie pierwsza taka konferencja w Polsce – **Warsaw Security Summit** odbędzie się w Warszawie 9 czerwca. Stanie się okazją do poznania światowych trendów i wyzwań stojących przed rynkiem security. Partnerami wydarzenia są branżowi liderzy, firmy wyznaczające kierunki rozwoju. Uczestnictwo jest bezpłatne – zachęcamy do rejestracji online na **www.WarsawSecuritySummit.eu**. Do zobaczenia!

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

**Korekta**
Jolanta Kucharska

**Projekt graficzny**
Sylwester Dmowski

**Prenumerata**
www.aspolska.pl/prenumerata

# W numerze...

TEMAT NUMERU

RAPORT STR. 44

## Bezpieczeństwo infrastruktury krytycznej

WYWIAD STR. 46

## Zawsze jest pole do doskonalenia

**Krzysztof Malesa**
zastępca dyrektora Rządowego Centrum Bezpieczeństwa

WAŻNY TEMAT STR. 82

## Bezpieczeństwo cybernetyczne systemów sterowania przemysłowego



# PIERWSZE ŚNIADANIE EKSPERTÓW

**O bezpieczeństwie w transporcie i logistyce rozmawiali uczestnicy pierwszego śniadania ekspertów „a&s Polska”.** Spotkanie odbyło się 3 marca w warszawskim hotelu Westin.

Dyskusję przy wspólnym stole prowadzili przedstawiciele producentów i dystrybutorów firm z rynku security oraz specjaliści i security managerowie firm i instytucji z rynku transportu i logistyki. Pierwsze tego typu spotkanie w branży zabezpieczeń spotkało się z entuzjastycznym przyjęciem uczestników, o czym może świadczyć frekwencja na śniadaniu (ponad 40 osób) oraz liczne pytania o kolejne spotkania w tej konwencji.

**Następne śniadanie ekspertów, które odbędzie się 12 maja,** zostanie poświęcone tematowi tego wydania „a&s Polska”, czyli bezpieczeństwu infrastruktury krytycznej i obiektów przemysłowych. Więcej na s. 81. Zapraszamy!

Obejrzyj film ze spotkania na:
**www.aspolska.pl/pierwsze-sniadanie-ekspertow-as-polska**

*To nie będzie nigdy temat zamknięty. Świat zewnętrzny będzie nam dostarczał nowych zadań, ale i rozwiązania techniczne będą dawały nowe możliwości.*

**Michał Domaradzki**
pełnomocnik prezydent Warszawy ds. bezpieczeństwa transportu publicznego

**Grzegorz Ćwiek**
prezes Schrack Seconet Polska

*Fantastyczne spotkanie w nowej formule, bardzo cieszę się, że nareszcie mogliśmy – jako dostawcy rozwiązań – spotkać się z użytkownikami i osobami odpowiedzialnymi za bezpieczeństwo obiektów transportu i logistyki. Powinniście to kontynuować!*

*Dobrze, że takie eventy mają miejsce również w branży security. To możliwość spotkania osób ze wszystkich właściwie punktów tego rynku.*

**Jacek Grzechowiak**
dyrektor ds. korporacyjnych, Securitas Polska

*Wrażenia jak najbardziej pozytywne. Bardzo się cieszę, że mogłem uczestniczyć w tym spotkaniu z ludźmi, którzy korzystają z systemów, które my oferujemy.*

**Piotr Świder**
Key Account Manager, Hikvision Poland

**Piotr Kozak**
security manager, DHL Express

*Wszyscy mamy wspólne cele i wspólne wnioski po tej konferencji.*

**Harald Dingemans**
prezes Linc Polsks

*Wszystko idzie w kierunku, w którym powinno. Czekam na kolejne takie spotkania.*

**Mateusz Zapotoczny**
Technical Manager, Dahua Technology Poland

*To jest droga właściwa, którą powinniśmy iść. Myślę, że tego typu spotkania zaowocują współpracą dostawców, producentów, integratorów oraz inwestorów i klientów końcowych. Jak najbardziej warto!*

**Kamil Wachowicz**
pełnomocnik zarządu Impel SA

*Warto rozmawiać o szeroko rozumianym bezpieczeństwie, wymienić się doświadczeniami i porozmawiać o przyszłości – w którym kierunku zmierza bezpieczeństwo.*

**Jan Grusznic**
Sales Engineer, Axis Communications

*Wymiana informacji w zakresie nie tylko samej branży, ale i wśród użytkowników końcowych uważam za bardzo istotne dla nas, ale też dla drugiej strony.*

**Piotr Sędziak**
Operations Director, ABC Data

*Największe wyzwania wiążą się z potencjalnymi ograniczeniami w przepływie towarów, spowodowane przez to, co się dzieje w Europie, zagrożeniem terrorystycznym.*

*Nowa forma spotkania klientów z producentami daje ogromną szansę spotkania się w towarzyskiej atmosferze, porozmawiania o tym, co dzieje się na rynku.*

**Sławomir Szlufik,**
Country Manager, Hanwha Techwin Europe

*Bardzo podobało mi się to spotkanie. Mogliśmy wymienić doświadczenia i poznać oczekiwania ludzi, którzy odpowiadają za kompleksowe zabezpieczenie dużych obiektów logistycznych i transportowych. Warto tu być!*

**Jacek Wójcik**
Optex Security

## Interkomy IP firmy 2N TELEKOMUNIKACE a.s.

### ARPOL
**info@arpol.pl | www.arpol.pl**

Asortyment oferowanych przez firmę **ARPOL** urządzeń do systemów zabezpieczeń został poszerzony o rodzinę znanych na świecie interkomów **2N® Helios IP**. Składa się ona z sześciu modeli. Dwa o luksusowym wyglądzie i zaawansowanych funkcjonalnościach: 2N® Helios IP Vario i modułowy 2N® Helios IP Verso są przeznaczone do zastosowań w rezydencjach i biurach o wysokim standardzie. Dwa modele do zadań specjalnych, o wysokiej odporności na uszkodzenia mechaniczne (IK10) i warunki atmosferyczne (IP69K), to interkomy 2N® Helios IP Force i alarmowy 2N® Helios IP Safety. Ich przykładowe wdrożenia: zakłady przemysłowe, punkty alarmowe przy autostradach i w przestrzeni miejskiej. Dwa prostsze modele: 2N® Helios IP Base i 2N® Helios IP Uni są głównie wykorzystywane w budownictwie jednorodzinnym. W skład rodziny 2N® Helios IP wchodzą też dwa urządzenia w wersji OEM (2N® Audio Kit i 2N® Video Kit), umożliwiające konwersję istniejącej instalacji domofonowej do nowoczesnego systemu z wykorzystaniem infrastruktury IP.
W interkomach IP zastosowano najnowsze osiągnięcia techniki w dziedzinie bezpieczeństwa i łączności, tj. kamery HD z obsługą ONVIF i zestawianie połączeń audio-wideo poprzez protokół SIP. Umożliwia to wykorzystanie m.in. smartfonów jako terminali odbiorczych w systemach interkomowych. Firma ARPOL, oficjalny dystrybutor urządzeń marki 2N TELEKOMUNIKACE a.s., zapewnia pełne wsparcie przed- i posprzedażowe, szkolenia handlowe i techniczne, serwis gwarancyjny i pogwarancyjny.

## Kopułkowa kamera IP AXIS Q6155-E PTZ

### Axis Communications
**www.axis.com/pl**

Idealne natychmiastowe ustawianie ostrości stanowi wyzwanie w przypadku kamer PTZ, szczególnie przy słabym oświetleniu. Kopułkowa kamera sieciowa PTZ AXIS Q6155-E wykorzystuje zaawansowaną technologię laserową w celu dokładnego ustawienia ostrości, nawet w ciemnościach. Jest idealnym rozwiązaniem do dozoru miejskiego, monitorowania infrastruktury krytycznej oraz innych zastosowań wymagających natychmiastowego ustawiania ostrości przy obserwacji poruszających się obiektów i szybko zmieniających się scen. Technologia laserowa w kamerze AXIS Q6155-E PTZ sprawia, że to najszybciej ustawiająca ostrość kamera PTZ na rynku. Zdecydowanie wyróżnia się w trudnych warunkach pracy, takich jak słabe oświetlenie, niski kontrast lub światła punktowe. Całkowicie bezpieczny promień lasera mierzy odległość pomiędzy kamerą a obiektem w ułamku sekundy, automatycznie zapewniając idealnie ostry obraz.
Kamera Q6155-E została wyposażona w technologię Lightfinder, która potrafi „szukać" światła w ciemności, aby dostarczyć kolorowy obraz wysokiej jakości o niskim poziomie szumów i dużej szczegółowości. Dzięki technologii Sharpdome dostarcza ostre obrazy bez zakłóceń z obszarów zarówno ponad linią horyzontu, jak i poniżej niej. Funkcja Speed Dry pozwala uzyskać czytelne, ostre obrazy podczas deszczu. Z kolei technologia Zipstream firmy Axis zmniejsza znacząco zapotrzebowanie na przepustowość i pamięć przy zachowaniu wysokiej jakości obrazów.

## Kamery hybrydowe Dahua

### Dahua Technology
**www.dahuasecurity.com/pl**

W obserwacji rozległych, słabo oświetlonych obszarów i detekcji intruza kamery termowizyjne sprawdzają się dużo lepiej niż klasyczne kamery optyczne. Mają jednak pewne ograniczenia – stały kąt widzenia, w związku z czym już w fazie projektu należy założyć, jaki wycinek całego obszaru będzie obserwowany.
Rozwiązaniem problemu jest nowa linia kamer hybrydowych na głowicy uchylno-obrotowej TPC-PT8620 Dahua Technology. Zostały one wyposażone w dwa moduły: optyczny i termowizyny. Oba znacznie różnią się od podobnych rozwiązań bispektralnych dostępnych na rynku. Niechłodzony przetwornik VOx w module termowizyjnym ma zoom optyczny z szybkim ustawieniem ostrości, który pozwala na efektywną detekcję poruszających się obiektów, nawet z odległości 12 km, i rejestrację obrazu w rozdzielczości 1280 x 1024. Wykryty obiekt może następnie zostać zidentyfikowany dzięki modułowi optycznemu full HD z przetwornikiem STARLIGHT, który wyposażono w potężny obiektyw 12,5…775 mm (62x zoom optyczny). Tak duża ogniskowa umożliwia identyfikację tablic rejestracyjnych z odległości nawet 2 km! Całości dopełnia laserowy promiennik podczerwieni o zasięgu 1 km, a wbudowany dalmierz pozwala precyzyjnie określić odległość obiektów oddalonych nawet o 5000 m z dokładnością do 2 m.
Kamera jest kompatybilna z ONVIF, posiada interfejsy analogowy i CVI, może być więc zintegrowana z dowolnym istniejącym systemem i okablowaniem.

# Innowacje MOBOTIX

Więcej niż standard. Spełnienie Twoich oczekiwań.

MX6

Nowa platforma Mx6
ze wsparciem H.264\ONVIF
Rewolucyjny krok MOBOTIX

Detekcja ruchu w 3D
Nowy standard w każdej kamerze


Bezpieczna technologia
Dzięki niej kamery MOBOTIX
są tak niezawodne

Łatwiejsza integracja
Większe możliwości


Linc Polska Sp. z o.o.
Zaprasza:

MOBOTIX Innovation
**Roadshow 2017**

## Nowa kamera kopułkowa Hikvision


### Hikvision
**www.hikvision.com**

**Hikvision DS-2CD4D26FWD-IZ** to najnowszy model kamery kopułowej o wysokiej czułości serii Darkfighter Lite 2MP. Kamera została wyposażona w wysokiej klasy przetwornik CMOS 1/1,8" ze skanowaniem progresywnym oraz zmiennoogniskowy obiektyw motozoom 2,8…12 mm. Dzięki wysokiej czułości (0,002 lx) zapewnia wysokiej jakości kolorowy obraz nawet w trudnych warunkach oświetleniowych.
W tym atrakcyjnym cenowo modelu zostały zaimplementowane zaawansowane funkcje analizy obrazu i inne funkcjonalności udoskonalające jej pracę, takie jak WDR (poprawa dynamiki obrazu), zasilanie PoE, *defog* (korekcja mgły), 3D DNR (cyfrowa redukcja szumów). W trybie nocnym, przy słabym oświetleniu, kamera Darkfighter zapewnia czysty obraz bez odbić IR.
W ciągu dnia, dzięki wykorzystaniu funkcji WDR obraz jest wyraźny zarówno w scenach mocno oświetlonych, jak i o wysokim kontraście oświetlenia. Dzięki funkcji HLC (*High Light Compensation*) jest polecana do obserwacji miejsc z silnymi źródłami światła skierowanymi w stronę kamery. Funkcja HLC automatycznie rozpoznaje i ogranicza natężenie silnego światła, aby obiekty znajdujące się w polu widzenia kamery były lepiej rozpoznawalne.

## Kamera nasobna ZEPCAM

### Linc Polska
**www.linc.pl**

Firma ZEPCAM oferuje profesjonalne kamery nasobne oraz mobilne rozwiązania wideo, które tworzą zintegrowaną platformę do strumieniowej transmisji danych na żywo. Urządzenia są wyposażone w nadajnik GPS i umożliwiają strumieniowanie wizji przez sieci 3G, 4G i Wi-Fi np. do centrum zarządzania. Mają małe rozmiary i wagę, dzięki czemu nie krępują ruchu podczas różnego rodzaju działań w terenie. Można je z łatwością umieścić na kasku, odzieży wierzchniej lub samochodzie.
Wszystkie produkty ZEPCAM są łatwe w użytkowaniu oraz niezwykle wytrzymałe na uderzenia i trudne warunki atmosferyczne. Kamery wyposażono w opaskę na rękę służącą do zdalnego sterowania, która ma funkcje „nagrywaj", „zatrzymaj", a także tagowania istotnych zdarzeń. Umieszczony w przewodzie mikrofon umożliwia nagrywanie dźwięku nawet wtedy, gdy kamera jest odłączona.
ZEPCAM to kompleksowe rozwiązanie oferujące zarówno rejestrację obrazu i dźwięku, jak i przesyłanie danych do centrum operacyjnego. Gwarantuje wysoką jakość zapisu, niezawodność, elastyczność oraz prostą i szybką konfigurację. System ten jest przeznaczony dla przedstawicieli agencji ochrony, zespołów ratowniczych, straży pożarnej, wojska oraz policji. Znajduje zastosowanie w sportach ekstremalnych i przemyśle. ZEPCAM to profesjonalny, zintegrowany system mobilnego dozoru wizyjnego, który sprawdzi się w wielu działaniach.

## Nowa bariera podczerwieni OPTEX zasilana hybrydowo

### OPTEX Security
**www.optex.com.pl**

SL-100/200 TNR są barierami podczerwieni zasilanymi hybrydowo, zapewniającymi ochronę na najwyższym poziomie. Znajdują szerokie zastosowanie w miejscach, gdzie dostęp do sieci energetycznej jest utrudniony lub wręcz nieosiągalny. Zarówno nadajnik, jak i odbiornik mogą być bowiem zasilane bateryjnie lub sieciowo. Sprzyja to ograniczeniu kosztów instalacji dzięki lepszemu wykorzystaniu istniejącej infrastruktury.
Konstrukcja obudowy umożliwia łatwą wymianę baterii bez konieczności otwierania osłony przedniej oraz ponownego przeprowadzania żmudnego procesu strojenia bariery. Bariera ma innowacyjną funkcję oszczędzania baterii. Nadajnik informuje odbiornik o stanie słabej baterii sygnałem zakodowanym w wiązce podczerwieni. Informacja z odbiornika jest następnie przekazywana do centrali alarmowej.
Kolejną zaletą bariery jest możliwość zastosowania różnych baterii, od dedykowanych litowych VIZTRO po standardowe baterie CR123A.
Nowa bariera podczerwieni OPTEX została zaprojektowana pod kątem zapewnienia jak największej elastyczności w dostosowaniu do potrzeb użytkownika i wymagań aplikacji.

HIKVISION


# TURBO HD 3.0

Wprowadzenie technologii Turbo HD 3.0 firmy Hikvision jest początkiem nowej ery na rynku CCTV. Technologia zapewnia transmisję rozdzielczości dwukrotnie wyższych niż full HD po kablu koncentrycznym. Trybrydowa kompatybilność zapewnia przełom w ewolucji transmisji analogowej, oferując obsługę wszystkich formatów wideo od kamer analogowych do HDTVI, AHD i IP.

## Kluczowe cechy:

- Kompresja H.264+
- Transmisja nawet do 800 m w rozdzielczości Full HD
- Wysoka rozdzielczość – nawet do 5MP
- Zestaw funkcji SMART
- Funkcja Plug&Play

smart

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

www.hikvision.com

## Szybkoobrotowe kamery IP z promiennikiem IR o zasięgu 150 m

**Polvision**
**www.polvision.pl**

Firma Polvision wprowadziła do sprzedaży dwie nowoczesne szybkoobrotowe kamery IP z wbudowanym adaptacyjnym promiennikiem IR o zasięgu 150 m. Model SD2322-IR oferuje wysokiej jakościobraz skompresowany metodą H.264 (ONVIF) w rozdzielczości 2,0 Mpix (1920 x 1080, 30 kl./s). Zastosowany obiektyw 4,7...103 mm umożliwia 22x zoom optyczny. Ma wbudowane dwa wejścia i jedno wyjście alarmowe, wejście i wyjście audio do dwukierunkowej komunikacji dźwiękowej, wyjście analogowe BNC oraz slot na karty. Kamera jest umieszczona w wandaloodpornej obudowie klasy IK10 i IP66, zasilanej 24 VAC/VDC (maks. 53 W z wł. grzałką). Model SD3732-IR ma te same funkcje, ale oferuje obraz z kompresją H.265 (ONVIF) o wyższej rozdzielczości 3,0 Mpix (2048 x 1536, 30 kl./s), przy 33-krotnym zoomie optycznym (4,5…148,5 mm), co pozwala na uzyskanie obrazu bardzo szerokiej sceny o zaskakująco wysokim poziomie szczegółowości. Na uwagę zasługuje również szeroki zakres temperatury pracy: od -40 do 70°C oraz gama uchwytów i adapterów do montażu w dowolnej lokalizacji. W komplecie z kamerami jest dostarczane wysoko zaawansowane oprogramowanie VMS dla serwerów i stacji monitorowania, umożliwiające automatyczne śledzenie obiektów.
Ceny detaliczne kamer wynoszą odpowiednio: 4573 zł i 6056 zł.
Urządzenia są objęte ROZSZERZONĄ 36-miesięczną gwarancją firmy Polvision.

## Ekonomiczne minikopułki IP 4 Mpix z kompresją H.265

**Polvision**
**www.polvision.pl**

Ekonomiczna seria kamer minikopułkowych o rozdzielczości 4 Mpix z kompresją H.265 (ONVIF) to kolejna nowość wprowadzona na rynek przez firmę Polvision. Kamery są wyposażone w obiektywy 2,8 mm (kąt widzenia 100 stopni w poziomie) oraz w promienniki podczerwieni o zasięgu 30 m.
Seria składa się z trzech następujących modeli: kamera zewnętrzna typu *eyeball* EBD4700, zewnętrzna wandaloodporna EDR4700 oraz plastikowa EFD4700 do zastosowań wewnętrznych.
Kamery mają wymiary odpowiednio: Ø126 x 94, Ø114 x 63, Ø100 x 60 mm. Model EBD4700 ma ponadto regulację trójosiową (3-axis) i jest odporny na bardzo niską temperaturę nawet do -35°C.
Wszystkie modele zostały wyposażone w superczułe przetworniki i układy WDR PRO 120dB. Oferują wysokiej jakości obraz w kompresji H.265 o rozdzielczości 4 Mpix (20 kl./s) lub 3 Mpix (30 kl./s). Są zasilane w standardzie 12 VDC lub PoE (maks. pobór 6 W).
W komplecie z kamerami jest dostarczane wysoko zaawansowane oprogramowanie VMS do serwerów i wielomonitorowych stacji operatorskich.
Ceny detaliczne tej serii kamer wynoszą 600–700 zł.
Urządzenia są objęte ROZSZERZONĄ 36-miesięczną gwarancją firmy Polvision.

## System przyzywowy VISO-OPT PLUS

**Schrack Seconet Polska**
**www.schrack-seconet.pl**

Schrack Seconet Polska wprowadził na rynek cztery systemy przyzywowe, zapewniające różną funkcjonalność w zależności od obiektów i grup użytkowników. Najprostszy z nich, VISO-OPT PLUS PLUS, spełnia wymagania norm europejskich, w tym VDE 0834 (część 1).
Ze względu na budowę oraz parametry techniczne system znajduje zastosowanie głównie w:
- toaletach dla osób niepełnosprawnych w budynkach publicznych, takich jak biurowce, galerie handlowe, dworce, stadiony, lotniska itp.,
- pomieszczeniach i łazienkach hotelowych przystosowanych dla osób niepełnosprawnych,
- domach opieki społecznej,
- szpitalach itp.

W przypadku wystąpienia zagrożenia życia lub zdrowia umożliwia zaalarmowanie personelu. Może również przekazać informację o uszkodzeniu do np. systemów bezpieczeństwa SMS (*Security Management System*).
VISO-OPT PLUS ma budowę modułową, jest wyposażony w liczne przyciski i lampki sygnalizacyjne.
W Polsce obowiązują akty prawne wymagające stosowania systemów przyzywowych.

Schrack Seconet oferuje cykl szkoleń projektowych w zakresie systemów przyzywowych i komunikacji. Zainteresowanych VISO-OPT PLUS, a także innymi systemami, firma prosi o kontakt.

POLON-ALFA NAJNOWSZA TECHNOLOGIA. NAJWYŻSZA JAKOŚĆ

Systemy sygnalizacji pożarowej:

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

Uniwersalne centrale sterujące **UCS 6000**

JUŻ **60 LAT**
PRODUKUJEMY
BEZPIECZEŃSTWO

Polon-Alfa Spółka z ograniczoną odpowiedzialnością Sp. k.
85-861 Bydgoszcz, ul. Glinki 155, www.polon-alfa.pl

## TELEWIZJA DOZOROWA

# Światowe trendy 2017

W ubiegłym roku rynek urządzeń telewizji dozorowej zanotował mniejszy wzrost obrotów spowodowany głównie przez chińskich dostawców dążących do obniżania cen i zwiększania udziałów w rynku. **W odpowiedzi dostawcy zachodni o ugruntowanej pozycji zaczęli inwestować w technologie i rozwiązania wykraczające poza konwencjonalne zastosowania security, oferując użytkownikom inne „wartości".**

**William Pao,**
a&s International

Z badań przeprowadzonych przez firmę analityczną Memoori wynika, że w 2016 r. rynek urządzeń telewizji dozorowej wzrósł tylko o 4,2% w porównaniu do 10% na rynku urządzeń kontroli dostępu. Już drugi rok z rzędu tempo wzrostu rynku CCTV jest mniejsze i obecnie nie przekracza połowy wartości wskaźnika CAGR (średni roczny wzrost) z poprzednich trzech lat. Mimo to wolumen sprzedaży zwiększył się, ponieważ główni konkurenci z Chin drastycznie obniżyli ceny produktów dla odbiorców na całym świecie. Mając zaplecze w postaci ochrony rynku krajowego i wsparcie finansowe rządu chińskiego, weszli na rynek Ameryki Północnej i częściowo do Europy, gdzie szybko zwiększają swoje udziały. Wszystko wskazuje na to, że ta strategia przynosi korzyści. Taką opinię potwierdza większość dostawców. Podkreślają oni, że spowolnienie wzrostu jest związane raczej z obniżką cen, a nie ze spadkiem popytu.

*W roku 2016 odnotowaliśmy rekordowy wzrost i dynamikę. Kontrakty z nowymi klientami stanowiły 67% obrotów* – mówi Brandon Reich, dyrektor ds. rozwiązań telewizji dozorowej w amerykańskiej firmie Pivot3, mającej oddziały na całym świecie.

*Niewykluczone że spowolnienie w obszarze telewizji dozorowej można przypisać pojawieniu się tanich produktów z Chin. Branża i firmy na całym świecie oczekują jednak dalszej integracji unikatowych technologii, które wykorzystują nowe typy danych, nie tylko obrazy wideo w celu uzyskania „prawdziwego oglądu sytuacyjnego"* – zdradza Steve Birkmeier, wiceprezes ds. rozwoju sprzedaży i biznesu we włoskim Arteco, które także działa globalnie.

Yury Akhmetov, dyrektor ds. rozwoju biznesu w AxxonSoft, uważa, że biznes rozwijał się różnie w zależności od regionu. *Notujemy np. wzrost na rynku w Afryce, ale na Bliskim Wschodzie dochodzi do spowolnienia. Przyczyniają się do tego sytuacja zarówno finansowa, jak i polityczna. Naszym zdaniem są to normalne wahania. W najbliższym dziesięcioleciu będziemy obserwować wzrosty w branży*

*zabezpieczeń, w szczególności w obszarze telewizji dozorowej.*
Johan Paulsson, dyrektor ds. technicznych (CTO) w Axis Communications, zauważa, że chociaż całościowo rynek telewizji dozorowej zwolnił, dział kamer IP jest w dobrej kondycji. *Trend wzrostowy sprzedaży na rynku kamer sieciowych jest napędzany głównie wzrostem zapotrzebowania w największych regionach rozwijających się, większym udziałem w małych instalacjach oraz szybkim postępem technologicznym, który tworzy nowe możliwości biznesowe.*

## Jak sobie radzą

Przy agresywnej postawie dostawców z Chin zachodni specjaliści w branży nie angażują się w „wyścig w dół" – cięcie cen i redukcję marży w celu zdobycia rynku. Skłaniają się raczej ku inwestycjom w nowe technologie i rozwiązania wykorzystujące zaawansowane oprogramowanie do analizy danych, zapewniające użytkownikom lepszy zwrot z inwestycji, niższy całkowity koszt eksploatacji, a także poprawę jakości analityki biznesowej.
*W swojej strategii wzrostu stawiamy na te funkcje i technologie, które zapewnią lepszy stosunek wartości do ceny niż u konkurencji* – wyjaśnia Karen Sangha, menedżer ds. marketingu na region Wielkiej Brytanii w firmie Panasonic. – *Zwracamy się do klientów z prośbą o bardziej holistyczne podejście do kosztorysów potencjalnych systemów. Oznacza to kalkulacje obejmujące całkowity koszt posiadania, w tym dokładną analizę kosztów eksploatacji i konserwacji, ale także korzyści finansowe wynikające z dodatkowych funkcji nowoczesnych systemów dozorowych.*
Użytkownicy końcowi stawiają coraz większe wymagania względem urządzeń systemów zabezpieczeń, dlatego dostawcy zwracają uwagę na metody analizy danych i inne rozwiązania wykraczające poza sektor zabezpieczeń, które pomagają klientom w usprawnianiu ich działalności biznesowej.
*Coraz więcej firm włącza w swoje działania inteligentną analitykę i analizę big data, pozwalające uprościć procesy i optymalizować działania sprzedażowe w organizacjach.*

Przy agresywnej postawie dostawców z Chin zachodni specjaliści skłaniają się ku inwestycjom w nowe technologie i rozwiązania wykorzystujące zaawansowane oprogramowanie do analizy danych.

*Tym samym analiza biznesowa wkracza na wyższy poziom* – podkreśla Jumbi Edulbehram, prezes regionalny na region Ameryki Płn. i Ameryki Płd. w firmie Oncam. – *Nasz model biznesowy wspiera integrację systemów zarządzania obrazem (VMS) czołowych producentów oraz deweloperów, którzy dzięki zdjęciom zrobionym naszą kamerą uzyskają prawdziwe narzędzie analizy i analityki biznesowej.*
*Rynek telewizji dozorowej nie może być dalej postrzegany jedynie jako rynek zastosowań security* – mówi J. Paulsson. – *Ponieważ rynek produktów CCTV rośnie i dojrzewa, Axis kontynuuje inwestowanie w rozwój nowych produktów.*
Rynki poszczególnych sektorów obfitują w tego typu przykłady.
*Nasze algorytmy analizy wieku i płci, a także rozpoznawania twarzy znajdują różne zastosowania poza sektorem zabezpieczeń. Na targach ISE w Amsterdamie pokazaliśmy niedawno np. rozwiązanie dla sektora handlu detalicznego łączące narzędzia analityczne z Digital Signage, co pozwala na dopasowanie treści reklamowej do wieku i płci osób znajdujących się w pobliżu* – wyjaśnia K. Sangha.
– *Na targach pokazaliśmy technologię rozpoznawania twarzy opracowaną przez naszych inżynierów, która jest obecnie wykorzystywana do automatycznego rejestrowania wykładów w szkolnictwie wyższym. Wykładowcy mogą np. nagrywać swoje wystąpienia bez zastanawiania się, czy są w danym momencie w kadrze, ponieważ kamera przez cały czas za nimi podąża.*

**Yury Akhmetov**
**dyrektor ds. rozwoju biznesu, AxxonSoft**

**Steve Birkmeier**
**wiceprezes ds. rozwoju sprzedaży i biznesu, Arteco**

**Jumbi Edulbehram**
**prezes regionalny na region Ameryki Płn. i Płd., Oncam**

**Peter Kim**
dyrektor,
IDIS America

## MEDIA SPOŁECZNOŚCIOWE I *CROWDSOURCING*

Choć głównym źródłem danych wizyjnych jest sieć kamer zainstalowanych u klienta, to coraz więcej danych pochodzi z postów w mediach społecznościowych i filmów z urządzeń użytkowników.

*Obecnie niektóre technologie umożliwiają zbieranie postów z mediów społecznościowych i scalanie tych danych. W odniesieniu do ochrony osób i mienia mnogość danych z mediów społecznościowych skorelowana z możliwością przypisania im lokalizacji i czasu jest cenionym rozwiązaniem. Możliwość porzewidywania pozwoli operatorom dostrzec potencjalne ryzyko, zanim stanie się ono realne.*

*Najlepszym obiektywem i najbardziej inteligentną czujką jest nadal człowiek. Uzbrojeni w smartfony (każdy z nas posiada inteligentny system wideo z lokalizatorem GPS, narzędzie do komunikacji i zdolności współpracy), jesteśmy w stanie dostarczyć ogromne ilości użytecznych informacji, pomocnych w egzekwowaniu prawa, poprawie bezpieczeństwa biznesowego i usprawnianiu procesów operacyjnych* – mówi Udi Segall, dyrektor ds. rozwoju biznesu w izraelskim Qognify.

**Francis Lachance**
dyrektor ds. grupy produktów monitoringu i akcesoriów, Genetec

*Nasza technologia jest już wykorzystywana w obszarach spoza sektora zabezpieczeń. Podam dwa przykłady. Pierwszy – handel detaliczny i branża turystyczna wykorzystują nagrania z kamer 360° w sklepach, hotelach czy kurortach do liczenia ludzi czy śledzenia wzorców poruszania się, co z kolei pozwala uprościć operacje biznesowe. Drugi przykład – szkoły, gdzie zapotrzebowanie na kamery dozorowe wynika z konieczności zapewnienia bezpieczeństwa, jednak placówki oświatowe zaczynają stosować obraz wideo także do poprawy jakości nauczania i śledzenia zaangażowania uczniów* – mówi J. Edulbehram.

**Johan Paulsson,**
dyrektor ds. technicznych (CTO), Axis Communications

## Trendy

Większość przewidywanych kierunków zastosowań urządzeń CCTV na rok 2017 odzwierciedla ogólne dążenie do wspierania użytkowników w zwiększaniu ich oszczędności oraz doskonalenia analityki biznesowej. Co jednak najistotniejsze, w świetle niedawnego ataku DDoS najbardziej wrażliwym i najpilniejszym obszarem jest cyberbezpieczeństwo. Oto wybrane kierunki rozwoju w obszarze telewizji dozorowej:

### CYBERBEZPIECZEŃSTWO

Atak DDoS na amerykańską spółkę zarządzającą m.in. serwerami DNS spowodował wstrzymanie usług popularnych serwisów, takich jak Amazon i Netflix. Okazało się, że w roli zdalnie sterowanych napastników użyto kilku kamer sieciowych i rejestratorów NVR produkcji chińskiej, zainfekowanych przez malware Miari. Incydent ponownie zwrócił uwagę na zagadnienie cyberbezpieczeństwa, zwłaszcza że coraz więcej urządzeń wideo ma połączenie z internetem.

*W minionym roku nieoczekiwanie na pierwszy plan wysunął się problem cyberbezpieczeństwa w obszarze Internetu Rzeczy. Bezpieczeństwo nieprzerwanie połączonych urządzeń budziło obawy, jednak skala luk w zabezpieczeniach i łatwość, z jaką hakerzy przejęli kontrolę nad urządzeniami i uzyskali dostęp do danych, były dla wielu zaskakujące* – mówi B. Reich.

*Możemy oczekiwać, że w tym roku biznes jako całość będzie bardziej skoncentrowany na zagrożeniach cyberświata, których stale przybywa i które stanowią nie lada wyzwanie zarówno dla liderów biznesu, jak i branży zabezpieczeń. Muszą oni o krok wyprzedzać przestępców i oszustów* – ocenia Kevin Wine, wiceprezes ds. marketingu w firmie Verint Systems.

Dzięki wysiłkom dostawców urządzenia są bezpieczniejsze niż dotychczas. *Coraz więcej producentów, tworząc aktualizacje sprzętowe i programowe, bierze pod uwagę potencjalne włamania na wielką skalę. Zaostrzają wymagania dotyczące haseł, wdrażają silne szyfrowanie danych, stawiają na szkolenie integra-*

Biznes będzie bardziej skoncentrowany na zagrożeniach cyberświata, których stale przybywa i które stanowią nie lada wyzwanie zarówno dla liderów biznesu, jak i branży zabezpieczeń.

**Brandon Reich**
**dyrektor ds. rozwiązań w monitoringu, Pivot3**

*torów systemów i użytkowników końcowych w zakresie odpowiednich procedur zabezpieczających informację podczas jej zbierania* – zaznacza J. Edulbehram.
*Przy tak dużej ilości danych wideo coraz ważniejszy staje się problem prywatności. Technika maskowania osób udostępniana przez Panasonic gwarantuje ochronę tożsamości klientów i pracowników* – dodaje K. Sangha.
*Dużą rolę odgrywa też edukacja. Faktem jest, że liczba niedostatecznie zabezpieczonych urządzeń i systemów IP rośnie, a odpowiedzialność za cyberbezpieczeństwo nie spoczywa wyłącznie na działach IT. Wszyscy, którzy działają na rynku zabezpieczeń technicznych – od konsultantów, przez integratorów, po użytkowników końcowych – mają do odegrania swoją rolę.*
*A zatem wyzwaniem będzie edukacja: będziemy musieli informować klientów, gdzie kryją się zagrożenia, uczyć ich, jak unikać pułapek i jak się chronić, a także pokazać, jak mogą zarządzać ryzykiem przy instalowaniu niechronionych urządzeń i systemów bezpieczeństwa* – mówi Francis Lachance, dyrektor ds. grupy produktów monitoringu i akcesoriów w firmie Genetec.

Ten rok przyniesie kontynuację analizy *big data*, a urządzenia IoT pozwolą na zbieranie mnóstwa danych z systemów, usług i urządzeń.

**USŁUGI ABONAMENTOWE**

Dozór wizyjny jako usługa (VSaaS - *Video Surveillance as a Service*) zyska w tym roku na popularności jako zapewniająca wiele korzyści, m.in. mniejszy koszt inwestycji i ochrona przed cyberzagrożeniami. *Uważam, że użytkownicy końcowi zaczną postrzegać swoje bezpieczeństwo przez pryzmat usługi: zdalne-*

## INTERNET RZECZY I BIG DATA

Gdy urządzenia wizyjne są połączone z innymi urządzeniami sieciowymi w ramach IoT, ilość generowanych danych rośnie. *Badania pokazują, że dane wizyjne są najczęściej wykorzystywane w przypadkach zagrożenia lub popełnienia przestępstwa. Jak dowodzą statystyki, dzieje się tak w odniesieniu do maksymalnie 10% przypadków. Dlatego wspólnie z klientami musimy przedefiniować cele gromadzenia tych danych, aby wykorzystywać 100% zebranych informacji* – podkreśla Pieter van de Looveren, starszy menedżer ds. komunikacji marketingowej w Bosch Security Systems. – *Dlatego wszystkie nasze kamery sieciowe, począwszy od serii IP 4000, mają standardowo wbudowane narzędzia analizy danych. Ten rok przyniesie kontynuację analizy big data, a urządzenia IoT pozwolą na zbieranie mnóstwa danych z systemów, usług i urządzeń. Proces ten umożliwi branżom śledzenie zagrożeń w sposób bardziej inteligentny. Firmy będą mogły przewidywać wyprzedzająco działania na podstawie zebranych danych, by w kolejnych latach osiągać cele biznesowe i strategiczne założenia*– wyjaśnia K. Wine (Verint).

**Karen Sangha**
**menedżer ds. marketingu, region Wielkiej Brytanii, Panasonic**

*go hostingu i monitoringu wizyjnego własnego domu czy firmy, wykonywanej samodzielnie albo przez specjalistów, którzy nie tylko przejmą ciężar zarządzania złożonymi systemami, ale także pomogą obniżyć koszty aktualizacji i utrzymania systemów* – zapowiada J. Paulsson. – *W ten sposób zostaną uwolnione zasoby wewnętrzne, które będzie można spożytkować w innym obszarze, a także poprawić skuteczność systemu zabezpieczeń i zarządzanie urządzeniami, a także wzmocnić cyberbezpieczeństwo.*

*Spodziewamy się, że ten rok przyniesie dalszy wzrost znaczenia usług abonamentowych i zarządzanych. Użytkownicy będą zainteresowani umowami okresowymi, w mniejszym stopniu będą chętni do kupowania licencji wieczystych. Oprócz istotnych oszczędności i elastyczności związanej z tym typem własności transfer ogromnej liczby danych i procesów obliczeniowych do chmury pozwoli firmom przenieść istotną część ryzyka związanego z cyberbezpieczeństwem na wyspecjalizowane firmy, w których globalne zespoły skupiają się na utrzymaniu bezpieczeństwa danych* – F. Lachance z firmy Genetec potwierdza opinię wyrażoną przez J. Paulssona.

**GŁĘBOKIE UCZENIE (*DEEP LEARNING*)**

Przez lata analityka obrazów wideo napotykała problemy związane z poprawnością i niezawodnością, nie spełniając pokładanych w niej nadziei. W tym roku mogą się pojawić pierwsze zmiany, ponieważ zarówno algorytmy, jak i infrastruktura stały się bardziej dojrzałe. Takie funkcje, jak inteligentne wyszukiwanie, będą więc bardziej skuteczne. *Wykorzystując deep learning, można dziś rozpoznać człowieka, samochód, dziecko czy drzewo, a nawet rozróżnić poszczególne osoby ze wskazaniem poprawnych identyfikacji, pozwalającym na zastosowanie praktyczne* – podkreśla U. Segall (Qognify). – *Przez wiele lat wykorzystywaliśmy głębokie uczenie jako część aplikacji do analizy obrazu Suspect Search, która w kilka sekund pozwala określić miejsce pobytu osoby będącej w zasięgu kamery systemu monitoringu wizyjnego.*

Perspektywy dalszego rozwoju *deep learning* nie są jednak oczywiste. *Technologie wykorzystujące głębokie uczenie oraz sztuczną inteligencję mają szansę na szersze zastosowanie w sektorze zabezpieczeń. Nasza branża niejednokrotnie doświadczyła niespełnionych nadziei w zakresie analizy wideo i mamy tego świado-*

*mość, gdy mowa o deep learning. Naszym zdaniem technologia ta musi zostać dopracowana, zanim wejdzie na rynek* – twierdzi J. Paulsson.

**ULTRA HD I ZAAWANSOWANA KOMPRESJA**

Rozdzielczość 4K (inaczej 8 Mpix) obiecuje obraz wyraźniejszy niż dotychczas. Niektórzy jednak traktują 4K jako kolejne modne i kosztowne hasło, którego celowość zastosowań w systemach zabezpieczeń jest obecnie ograniczone.

*Dominuje trend technologiczny 2 Mpix. Chociaż głośno jest o 4K – takich kamer jest sporo i mogą spełnić pokładane w nich nadzieje – potrzeby większości użytkowników nie wymagają zastosowania technologii 4K* – mówi Peter Kim, dyrektor w IDIS America. *– Rozdzielczość 4K ma obecnie zastosowania niszowe, ale jest perspektywiczna. Jednak moim zdaniem bardziej odpowiednim, a przede wszystkim wydajniejszym kosztowo rozwiązaniem jest użycie większej liczby kamer. Kamery 2-Mpix, zwłaszcza przy zastosowanych nowych kodekach, są obecnie propozycją optymalną. Kamera 8-Mpix dostarcza doskonały obraz, ale jak objąć nią front i tył budynku? 4K stanie się standardem, ale nie wcześniej niż za dwa, trzy lata. Ważna jest edukacja w zakresie korzyści płynących z technologii 4K i jej odpowiedniego stosowania, aby obecne hasło marketingowe przekształciło się w praktyczne zastosowania z korzyścią dla użytkownika.*

Wysoka rozdzielczość obrazów wymaga m.in. nowych metod kompresji. Oprócz kodeków w nowym standardzie H.265, są oferowane kodeki hybrydowe umożliwiające dozór *live* w H.264, a rejestrację – w H.265.

Istotnym problemem związanym z większymi rozdzielczościami obrazu ultraHD są dziś nowe metody kompresji. Standard H.264 jest nadal najbardziej popularny, ale rozpowszechnienia wymaga niezbyt jeszcze popularny standard H.265. *W najbliższych miesiącach i latach H.265 będzie częściej wykorzystywany. Firma Bosch przewodzi stawce, wprowadzi go w kwietniu lub maju tego roku do swojej oferty. Następna generacja urządzeń przyniesie oszczędności transferu, ułatwi zarządzanie danymi i zmniejszy wymagane przestrzenie dyskowe oraz obciążenie sieci do minimum, nawet o 80% dzięki jednoczesnemu zastosowaniu inteligentnego kodowania, inteligentnej dynamicznej redukcji szumów* (Intelligent Dynamic Noise Reduction) *oraz standardu H.265* – ocenia P. van de Looveren (Bosch Security Systems).

Masowe przejście na nowy standard wiąże się również z kolejnymi wyzwaniami. *H.265 ma mniejsze zapotrzebowanie na pasmo w porównaniu z H.264 przy tej samej jakości obrazu. Wymaga jednocześnie bardziej złożonego kodowania i dekodowania, a tym samym procesorów CPU i graficznych GPU o większej mocy obliczeniowej, co może wymusić kosztowną aktualizację sprzętu. Systemy zarządzania obrazem oparte tylko na mocy obliczeniowej procesora głównego i dekoderach nie będą w stanie zapewnić płynnej transmisji obrazów w standardzie H.265* – podkreśla F. Lachance (Genetec). *Aby w standardzie H.265 zapewnić wydajność dekodowania porównywalną do H.264, należy umiejętnie wykorzystać sprzętowe technologie procesorów graficznych. Bez tego przy zmianie standardu na H.265 użytkownicy nic nie zyskają.*

Firma IDIS oferuje natomiast kodeki hybrydowe, dzięki którym przejście z H.264 na H.265 stanie się płynniejsze. *Nasze rozwiązanie umożliwia monitoring na żywo w H.264 i nagrywanie w H.265. Pozwala czerpać korzyści z obu rozwiązań* – wyjaśnia P. Kim. *– Nie trzeba rozbudowywać procesora czy komputera. Strumień na żywo jest w standardzie H.264, ale użytkownik potrzebuje mniej przestrzeni na archiwizację, ponieważ nagranie wykonano w standardzie H.265.*

## Żeby pozostać w grze

W sytuacji zwiększonej konkurencyjności na rynku telewizji dozorowej sposobem dla firmy na pozostanie w grze jest zapewnienie użytkownikom większej funkcjonalności urządzeń systemów zabezpieczeń i wspieranie ich w usprawnianiu procesów biznesowych innych niż tylko security. To wyzwania aktualne nie tylko na ten rok...

**Udi Segall**
**dyrektor ds. rozwoju biznesu, Qognify**

**Pieter van de Looveren**
**starszy menedżer ds. komunikacji marketingowej, Bosch Security Systems**

**Kevin Wine**
**wiceprezes ds. marketingu, Verint Systems**

# Nie tylko kamery

## Tematyka i wyniki badań projektu COPCAMS

W latach 2013–2016 Politechnika Gdańska uczestniczyła w projekcie współfinansowanym przez Narodowe Centrum Badań i Rozwoju oraz inicjatywę unijną ARTEMIS.

**dr inż. Piotr Szczuko**
Wydział Elektroniki, Telekomunikacji i Informatyki,
Katedra Systemów Multimedialnych,
Politechnika Gdańska

Projekt COPCAMS *(Cognitive and Perceptive CAMeraS)*, w polskiej wersji „Kamery umożliwiające kontekstowe rozumienie pozyskiwanego obrazu", dotyczył opracowania i przetestowania nowych inteligentnych rozwiązań dla kamer przemysłowych, systemów dozoru wizyjnego, diagnostyki wizyjnej na liniach produkcyjnych i innych dziedzin zastosowania analityki wizyjnej. Założono wytworzenie i oprogramowanie nowych typów układów elektronicznych, wielordzeniowych jednostek obliczeniowych zdolnych do wydajnych obliczeń przy zmniejszonym zużyciu energii w stosunku do typowych procesorów CPU.
W projekcie COPCAMS brały udział uczelnie techniczne i instytuty badawcze z Francji, Hiszpanii, Turcji, Danii, Słowenii, Wielkiej Brytanii i Polski, łącznie było 25 partnerów.

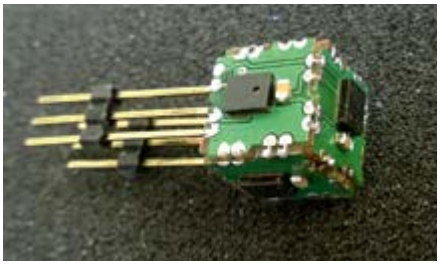
Dwa zespoły naukowców z Wydziału Elektroniki, Telekomunikacji i Informatyki Politechniki Gdańskiej, z Katedry Inżynierii Mikrofalowej i Antenowej oraz Katedry Systemów Multimedialnych już przed rozpoczęciem projektu były zaangażowane w prace koncepcyjne, formułowanie założeń projektu, a po uzyskaniu pozytywnej oceny i finansowania, w kolejnych etapach – dobór i testowanie układów, wytwarzanie nowoczesnych elementów elektronicznych, opracowywanie oprogramowania oraz testowanie prototypów w warunkach rzeczywistych.
Politechnika Gdańska koordynowała pakiet zadań „Zaawansowane koncepcje dla systemów kamer" *(Advanced Concepts for Cognitive & Perceptive Video Systems)* poświęcony nowym metodom przetwarzania obrazów wideo i danych wielomodalnych, tj. pochodzących z dodatkowych czujników różnego typu oraz kompresji sygnałów wizyjnych i transmisji danych.

### Autorskie koncepcje i prototypy

Opisywane prace zostały zrealizowane przez zespół Katedry Systemów Multimedialnych (KSM). Opracowano autorskie koncepcje i wykonano prototypy, które zaowocowały trzema patentami.

### Radar akustyczny zintegrowany z kamerą obrotową

Pierwszym z innowacyjnych rozwiązań jest **radar akustyczny zintegrowany z kamerą obrotową.** Jego zadaniem jest analizowanie na żywo danych o wektorowym gradiencie ciśnienia akustycznego, z których można pozyskać informacje o położeniu źródeł dźwięku w całej przestrzeni wokół kamery.
Zastosowanie specjalizowanego sensora akustycznego opracowanego przez zespół naukowców KSM *(fot. 1)* umożliwia analizowanie kierunkowości nadchodzących dźwięków z dużą rozdzielczością



**Fot. 1. Sensor akustyczny opracowany przez zespół naukowców KSM Politechniki Gdańskiej**

kątową i natychmiast, bez konieczności przestrajania czy obracania sensora.
W odróżnieniu od stosowanych od wielu lat macierzy mikrofonów z kształtowaną wiązką *(beamforming)* lub mikrofonów kierunkowych obsługa tego sensora jest łatwa i wyróżnia się bardzo małym rozmiarem: czujnik 5 x 5 x 5 mm i dodatkowe elementy elektroniczne wielkości karty kredytowej, grubości 10 mm.
Odpowiednie oprogramowanie do detekcji i lokalizacji źródeł dźwięków istotnych z punktu widzenia bezpieczeństwa jest w stanie wykryć i skierować obrotową kamerę w miejsce krzyku, wybuchu, wystrzału czy stłuczonej szyby. Algorytm klasyfikacji źródeł dźwięków został „wytrenowany" rzeczywistymi nagraniami i rozróżnia przykładowe ich klasy, nie reagując na dźwięki typowe, np. hałas uliczny i rozmowy.
Liczba zdarzeń analizowanych i wykrywanych jednocześnie nie jest ograniczona, a od operatora zależy, w jaki sposób zadziała oprogramowanie sterujące, np. czy ustawi kamerę na najbliższe źródło, czy na najgłośniejsze, czy wyższy priorytet ma mieć krzyk lub wystrzał itp. Ponadto informacje z jednego sensora mogą być użyte do pozycjonowania kilku kamer jednocześnie, np. każdej na inne źródło.
Rozwiązanie było testowane w warunkach rzeczywistych w pobliżu ruchliwej ulicy w Gdańsku oraz w specjalnym środowisku akustycznej komory bezechowej KSM. W wyniku badań potwierdzono wysoką skuteczność i precyzję określania kierunku, z którego dochodzi dźwięk. Dodatkową zaletą urządzenia jest brak konieczności rejestracji próbek dźwięku, gdyż analizuje ono tylko kierunki i na bieżąco przekazuje wyniki końcowe (rozpoznane typy dźwięków i lokalizacje źródeł) do modułu sterowania kamerą PTZ.

## Kierunkowa antena wielosektorowa

Drugim kluczowym autorskim opracowaniem jest **kierunkowa antena wielosektorowa** do wykrywania i lokalizacji aktywnych znaczników radiowych wykonanych w technologii RFID. Typowo RFID w wersji pasywnej, tj. bez wbudowanej baterii, są stosowane do ochrony dóbr i towarów w sklepach. Wykrycie kradzieży jest możliwe tylko w momencie przechodzenia przez wąskie bramki stanowiące anteny nadawczo-odbiorcze, indukujące zasilanie w takim układzie i stwierdzające jego obecność. Nowe opracowanie z aktywnymi znacznikami i anteną kierunkową umożliwia ciągłe monitorowanie obecności i lokalizowanie chronionego przedmiotu oraz automatyczne pozycjonowanie na niego kamery PTZ.
W połączeniu z typowymi systemami ochrony obiektów, np. z kartami identyfikacyjnymi, antena i znaczniki zwiększają skalę zastosowań tego rozwiązania: staje się możliwe zarządzanie poziomami uprawnień do wykorzystania kluczowych dóbr w firmie, m.in. szybkie lokalizowanie przedmiotów, wykrywanie przeniesienia urządzenia przez osobę o niewłaściwych uprawnieniach, przypisanie automatycznie chronionego wyposażenia do osoby, która logowała się kartą identyfikacyjną itd.

### Prace programistyczne

W projekcie skupiono się na krytycznej analizie dotychczasowych, jednowątkowych algorytmów przesyłania obrazu przeznaczonych na procesory CPU. Miało to na celu zidentyfikowanie możliwości poprawy działania tych metod poprzez wykonanie ich wersji przeznaczonych na platformy wieloprocesorowe, charakteryzujące się dużymi możliwościami zrównoleglenia obliczeń. Przykładowo w ostatnich latach dynamicznie rozwijają się platformy programistyczne CUDA i OpenCL umożliwiające uruchamianie różnorodnych obliczeń w trybie równoległym na procesorach kart graficznych (technika nazywana GPGPU – *General-Purpose Computing on Graphics Processing Units*, obliczenia ogólnego przeznaczenia na procesorach graficznych).

Odpowiednie oprogramowanie do detekcji i lokalizacji źródeł dźwięków istotnych z punktu widzenia bezpieczeństwa wykrywa i kieruje kamerę w miejsce krzyku, wybuchu, wystrzału czy stłuczonej szyby.

Układ GPGPU zwykle ma setki, a nawet tysiące rdzeni, co skutkuje przyspieszeniem obliczeń i zmniejszeniem poboru energii w porównaniu do procesora CPU wykonującego to samo zadanie.
W projekcie COPCAMS zespół KSM wykorzystywał dostępne na rynku zestawy uruchomieniowe układów nVidia Jetson TK1 i nowszy TX1, akcelerator obliczeń Keystone II firmy Texas Instruments, prototypowy akcelerator STHORM firmy STMicroelectronics wykonany specjalnie na potrzeby projektu COPCAMS oraz układy GPGPU kilku kart graficznych. Rosnąca popularność wielu testowanych układów przełoży się na ich dalszą miniaturyzację i upowszechnienie. Przewiduje się wykorzystanie tego wydajnego rozwiązania w kamerach monitoringu wizyjnego zgodnie z koncepcją Edge Computing, czyli w odległych punktach w urządzeniach końcowych, bez konieczności przesyłania dużych ilości danych, strumieni wideo lub innych do centralnego komputera.
Szczególnie interesujące i potrzebne jest usprawnienie **metod wykrywania ruchu i śledzenia obiektów.** Algorytmy stosowane obecnie w niektórych kamerach są uruchamiane na mało wydajnych procesorach, w związku z czym nie mogą być zbyt złożone i w konsekwencji reagują często na ruch w niepożądany sposób, np. falowanie liści, wody, odbicia, uniemożliwiając stosowanie w praktyce (zbyt duża liczba fałszywych alarmów). Algorytmy działające skuteczniej wymagają szybszych obliczeń. Przykładowo w algorytmach badanych i optymalizowanych przez zespół KSM obiekty ruchome są wykrywane na zasadzie statystycznego modelowania tła i wyznaczania różnicy między aktualną klatką z kamery a tłem, następnie filtrowanie obiektów o właściwym rozmiarze, śledzenie ciągłości ich ruchu.
Elementarną operacją wykonywaną na każdym pikselu obrazu jest modelowanie tła w taki sposób, aby adaptować się do powolnych zmian w obrazie (np. zachmurzenie zmieni jasność i kolorystykę całego kadru i nie może być interpretowane jako ruch) oraz szybkich cyklicznych zmian (np. ruch listowia na tle nieba powoduje naprzemienne zmiany koloru z zielonego na niebieski i oba te kolory są tłem, a nie pierwszoplanowym obiektem

ruchomym). Dla klatki wideo o rozmiarze 1 Mpix konieczne jest obliczanie i aktualizowanie 24 razy na sekundę miliona pikseli w modelu tła. Operacja ta jest najbardziej wymagająca obliczeniowo. Jej przyspieszenie i przeniesienie na układy akceleracji okazało się najbardziej korzystne.

Podobnie bardzo istotne i korzystne było zoptymalizowanie i zrównoleglenie **metody analizy przepływu optycznego w strumieniu wideo** *(Optical Flow)*. Algorytm identyfikuje każdy piksel w następujących po sobie klatkach wideo i określa, czy się przemieścił, w jakim kierunku i jak daleko. W tym celu odpowiednimi deskryptorami opisuje się cechy wizualne danego piksela i jego najbliższego otoczenia, w kolejnej klatce obrazu poszukuje się najbardziej podobnego wycinka obrazu. Różnica w położeniach wzorca i nowego wycinka to wektor przepływu. Dla całej klatki liczone są miliony takich porównań, a z puli wektorów przepływu są wybierane te o wspólnym kierunku i długości, z których odczytuje się reprezentację ruchu dużego obiektu pokrywającego wiele sąsiadujących ze sobą pikseli.

Kierunkowa antena wielosektorowa z aktywnymi znacznikami umożliwia ciągłe monitorowanie obecności i lokalizowanie chronionego przedmiotu oraz automatyczne pozycjonowanie na niego kamery PTZ.

Metoda przepływu została wykorzystana w projekcie do algorytmu tzw. wirtualnej bramki, zliczającej liczbę osób w bardzo dużych grupach i w tłumie *(fot. 2)*. Ponadto z powodzeniem zastosowano ją do analizy obrazu z kamery ruchomej umieszczonej na pokładzie lecącego drona. Drgania i ciągły ruch kamery nie pozwalają stosować modelowania tła opisanego wcześniej, ale do wykrywania i śledzenia obiektów ruchomych przepływ optyczny nadaje się z powodzeniem.

Rozwiązania zostały przetestowane w warunkach rzeczywistych w trzech scenariuszach:

- nadzór rozległych terenów za pomocą współpracujących ze sobą kamer obrotowych zmiennoogniskowych i szerokokątnych,
- zautomatyzowana linia produkcyjna wykorzystująca analitykę wideo do oceny poprawności wykonania elementów oraz lokalizację i identyfikację RFID do zarządzania kluczowymi urządzeniami i narzędziami w hali produkcyjnej,
- monitoring otoczenia i wnętrza budynków wykorzystujący kamery, sensory akustyczne do lokalizowania źródeł dźwięków znamionujących zagrożenia, a także lokalizację i identyfikację RFID do ochrony wyposażenia.

W praktyce zweryfikowano korzyści ze stosowania dedykowanych platform obliczeniowych i wykorzystania zrównoleglonych wersji najbardziej złożonych algorytmów. Zanotowano wysoce zadowalające wartości oszczędności całkowitej energii oraz energii zużywanej w trakcie wykonywania elementarnych zadań. Przykładowo analiza jednej klatki wideo metodą przepływu optycznego na CPU odbywa się w 0,2 s i przy zastosowaniu procesora 110 W na jedną klatkę zużywa się ponad 6 mWh energii, natomiast GPU o mocy 220 W realizuje obliczenia około pięciokrotnie szybciej i zużywa połowę tej energii, tj. 3 mWh.

Wśród prac naukowych partnerów z pozostałych krajów szczególnie wyróżniały się:

- usprawnienie algorytmów kalibracji kamer i wyznaczania głębi 3D dla stereopar,
- optymalizacja wymiany danych w sieciach z wieloma klientami, kamerami i odbiorcami,
- przyspieszenie działania algorytmów detekcji ruchu w nagraniach archiwalnych (analiza w czasie 35 razy szybszym od rzeczywistego, 1 doba nagrania w 40 minut),
- połączenie możliwości monitorowania akustycznego i radiowego z wizyjnym w celu poprawy możliwości skutecznego oraz precyzyjnego wykrywania i śledzenia zdarzeń istotnych z punktu widzenia bezpieczeństwa,
- rozwinięcie metod współpracy między algorytmami sterującymi kamer szerokokątnych i kamer obrotowych w celu nadzoru rozległego terenu,
- usprawnienie metod poprawy czytelności obrazu w przypadku zamglenia i niedoświetlenia,
- stworzenie wydajnych i intuicyjnych środowisk programistycznych dla producentów kamer, układów obliczeniowych i innych podzespołów.

**Fot. 2. Przykład działania metody przepływu optycznego: barwy wskazują kierunek ruchu, intensywność koloru oznacza prędkość**

**Wyniki projektu udostępniono w kilku raportach i publikacjach: www.copcams.eu**

# System monitoringu i ochrony pracowników

ACTIVE TRACK ACTIVE GUARD

- *Serwis i usługi*
- *Ochrona*
- *Sprzątanie*
- *Logistyka*

## Chroni pracowników

- Natychmiastowe wezwanie pomocy
- Dokładne rozliczanie godzin pracy
- Dwukierunkowa komunikacja głosowa

## Sprzyja pracodawcom

- Identyfikuje tożsamość pracownika
- Weryfikuje rzetelność wykonywanych obowiązków
- Oferuje aplikację w chmurze do zarządzania i raportowania - ActiveView
- Jest odporny na niesprzyjające warunki pracy

## Gwarantuje jakość usług użytkownikowi końcowemu

- Dostarcza raporty potwierdzające wykonanie usługi solidnie i na czas
- Minimalizuje szkody na obiekcie
- Jest gwarancją bezpieczeństwa i profesjonalizmu

EBS

CREATING A SENSE OF SECURITY
SINCE 1989


www.ebs.pl

EBS Sp. z o.o.
ul. B.Czecha 59, 04-555 Warszawa

e-mail: sales@ebs.pl
tel. 22 518 84 00

# Wskazówki dla integratorów systemów, by rozwijali się wraz z branżą

**Prasanth Aby Thomas**
a&s International

Branża zabezpieczeń rozwija się, ewoluując w kierunku sfery usług. **Integratorzy systemów muszą być czujni,** aby nadążać za nowymi trendami. Muszą jednocześnie śledzić potrzeby i wymagania nie tylko użytkowników końcowych, ale także producentów, gdyż **tylko wtedy będą w stanie zaoferować rozwiązania korzystne dla wszystkich zainteresowanych.**

## Błędy popełniane przez integratorów

Integratorzy systemów są w pewnym sensie przedstawicielami producentów, umożliwiającymi dotarcie do użytkowników końcowych. Od sposobu, w jaki integrator przedstawi ofertę swojego zleceniodawcy, zależy wiedza użytkownika o jego produktach. Funkcja integratora jest sztuką utrzymania równowagi pomiędzy poznaniem oferty producenta a zaspokajaniem wymagań klienta. To niełatwe, biorąc pod uwagę, że ten pierwszy wciąż rozwija swoje produkty, drugi zaś oczekuje redukcji kosztów i tzw. wartości dodanej. Przy takiej presji nie do uniknięcia są pomyłki popełniane przez integratorów podczas realizacji projektów. Mogą być natury technicznej albo dotyczyć strategii biznesowej, ale co ważne – mogą okazać się krytyczne.

**Producenci podzielili się z nami uwagami odnośnie do najczęściej spotykanych błędów, podpowiadając sposoby ich korygowania.**

### Zbyt mało szkoleń

Bardzo ważne dla integratorów są szkolenia produktowe oferowane przez producentów. Większość integratorów kieruje na nie swoich pracowników, by poznali nowe technologie i kierunki rozwoju. Według Tyco Security Products niektórzy jednak ograniczają udział w szkoleniach do niewielkiej liczby techników. Koszty takich „oszczędności” mogą być od-

czuwalne zarówno dzisiaj, jak i w przyszłości, gdyż wszyscy technicy w firmie integratora powinni zostać przeszkoleni w zakresie najnowszych technologii.

*Zdarza się, że integratorzy szkolą tylko kilku specjalistów w zespole. Uważają, że szkolenie jest tożsame z poświęceniem czasu, który można by przeznaczyć na pracę w terenie* – mówi Perry Levine, starszy menedżer produktu w Dziale Oprogramowania w Tyco Security Products. – *Ważne, aby WSZYSCY technicy byli odpowiednio przeszkoleni i zdobyli certyfikaty zarówno w zakresie instalacji, jak i wykonywania czynności serwisowych. Nie można zakładać, że przeszkolony z jednego produktu ma wiedzę o wszystkich oferowanych rozwiązaniach, a skoro odbył szkolenie na starszej wersji, dodatkowe jest niepotrzebne. Rozwiązania z zakresu security coraz bardziej bazują na technologiach IT, niezbędna jest zatem aktualna wiedza teoretyczna i praktyczna. Aby integratorzy mogli utrzymać wysoki poziom obsługi klienta i rozwijać działalność, powinni inwestować w szkolenia wszystkich pracowników działu technicznego.*

## Podkreślanie wagi standardów zamiast rozwiązań

Branża zabezpieczeń technicznych przywiązuje ogromną wagę do rozwiązań opartych na standardach. Standardy są rzeczywiście kluczowe, aby branża mogła się rozwijać. Jednak dyskusje na ten temat przysłaniają często kluczowy aspekt, jakim jest dostarczanie klientowi właściwego rozwiązania. Zwrócił na to uwagę Marwan Khoury, regionalny menedżer ds. marketingu w Axis Communications, wyjaśniając, czego integratorzy systemów NIE powinni robić.

*Prezentując klientom możliwości do wyboru, powinni mniej skupiać się na standardach i kartach katalogowych, a więcej uwagi poświęcać wartości, jaką jest jakość zachowana we wszystkich fazach dostarczania technologii: od projektu, przez produkcję, po instalację* – mówi M. Khoury. – *Ułatwi to integratorom dostarczanie klientom produktów o dłuższej żywotności, dla których całkowity koszt posiadania będzie niższy, a zakłócenia w działalności firmy minimalne.*

## Zbyt późny kontakt z producentem

Problemy w codziennej pracy, jakie napotykają integratorzy, są zjawiskiem naturalnym, zwłaszcza w aspektach technicznych. Integrator powinien wówczas jak najszybciej skontaktować się z producentem, by je skutecznie rozwiązać. Jak zauważa Mitchell Kane, prezes Vanderblit Industries, nie zawsze tak się dzieje. Bywa, że integratorzy dostrzegają problem zbyt późno, co wywołuje niepotrzebne komplikacje. Negatywne skutki są jeszcze większe, gdy technicy nie są odpowiednio przeszkoleni w danej materii.

*W niektórych sytuacjach w miarę upływu czasu problemy się nasilają* – mówi M. Kane. – *Często nikt nie kontaktuje się z producentem, aż w końcu użytkownik znajduje się w sytuacji podbramkowej. Wiele problemów można sprawnie rozwiązać, jeśli od razu producent zostanie zaangażowany. Zdarza się np. że integratorzy nie konsultują się z producentem w fazie opracowywania interfejsu wykonanego na zamówienie czy integrowania podzespołów innych producentów. Niedoceniane wysiłki nikomu nie służą. Zdarza się też, że integratorzy wysyłają do klienta techników niezorientowanych w danej tematyce, a to już prosta droga do katastrofy.*

M. Kane dodaje, że wielu producentów oferuje programy szkoleniowe online lub z trenerem, aby zapobiegać ewentualnym problemom. Integratorzy powinni w pełni z nich korzystać. Stwierdzenie to wpisuje się w opinię Tyco, że wszyscy technicy-integratorzy systemów powinni zostać odpowiednio przeszkoleni.

## Sprzedawanie technologii zamiast rozwiązań

System zabezpieczenia technicznego nie oznacza już tylko kilku kamer zainstalowanych w terenie i podłączonych do rejestratora. Rozwiązania do zastosowań security mają sprostać wyzwaniom również w innych sektorach. W wielu przypadkach są kluczowe dla działalności i wyników finansowych firm, powinny więc mieć wysoki priorytet.

Przedstawiciele Verint Systems podkreślają, że integratorzy powinni umieć rozpoznawać takie sytuacje i skoncentrować się na rozwiązaniach. – *Często integrator jest zbyt skupiony na sprzedawaniu technologii zamiast rozwiązań* – zauważa Kevin Wine, wiceprezes ds. marketingu w Verint Systems. – *Określenie „bezpieczeństwo" dzisiaj nie oznacza już kamer rozlokowanych wokół budynku. To zdecydowanie więcej: bezpieczeństwo biznesu, personelu czy danych poufnych. Dlatego konieczne jest, aby integratorzy, musząc sprostać wymaganiom klientów nie tylko obecnie, ale także w przyszłości, inwestowali w rozwój własnej wiedzy w dziedzinie IT.*

Rozwiązania z zakresu security coraz bardziej bazują na technologiach IT, niezbędna jest zatem aktualna wiedza teoretyczna i praktyczna.

Integratorzy powinni inwestować w szkolenia WSZYSTKICH pracowników działu technicznego.

## Oferowanie odpowiednich rozwiązań w wymagających okolicznościach

Integratorzy są obecnie zmuszeni z dużą uwagą śledzić dynamiczne zmiany zachodzące na rynku. Nowości technologiczne pojawiają się częściej niż dotychczas, a klienci żądają najnowszych, coraz bardziej zaawansowanych rozwiązań.

Niestety, nie sposób jednoznacznie wskazać, jaką politykę integratorzy powinni w tej sytuacji przyjąć. Pod taką presją rośnie ryzyko popełnienia przez nich błędów. Producenci są gotowi do udzielania pomocy, ponieważ tym samym wspierają własną branżę.

To nie są łatwe czasy dla integratorów, gdy do branży security migruje coraz więcej nowych technologii, takich jak Internet Rzeczy czy *deep learning*.

# Co integratorzy systemów powinni robić częściej?

**Działalność związana z integracją systemów staje się coraz bardziej złożona. Nowe technologie pojawiają się niemal z dnia na dzień, a wymagania klientów rosną, ponieważ inwestując swój kapitał, oczekują coraz więcej. Integratorzy muszą dziś zachować elastyczność, żeby móc wyjść naprzeciw zróżnicowanym żądaniom i dotrzymać kroku postępowi technologicznemu, by tym samym zapewnić sobie korzystne wyniki finansowe. W tej sprawie również warto skorzystać z rad producentów. Oto ich sugestie.**

## Bezpieczeństwo to wyzwanie biznesowe

Zapewnienie bezpieczeństwa to obecnie nie tylko kwestia ochrony – jest ono ściśle powiązane z działalnością biznesową firmy. Naruszenie procedur bezpieczeństwa np. w banku ma poważne konsekwencje dla zaufania, jakim go darzą klienci. Mogą się także pojawić problemy prawne, ponieważ organy władzy przywiązują wielką wagę do bezpieczeństwa.

*Integratorzy muszą zrozumieć specyfikę branży, dla której pracują, i wyzwania dotyczące bezpieczeństwa, z jakimi mierzą się ich klienci* – twierdzi Kevin Wine, wiceprezes ds. marketingu w Verint Systems. – *Bezpieczeństwo i ryzyko stanowią dzisiaj istotne problemy biznesowe. Zarządzający wysokiego szczebla dostrzegają niebezpieczeństwo kosztownych i szkodliwych zakłóceń w działaniu firmy przy niewystarczającej kontroli ryzyka. W efekcie zespoły ds. bezpieczeństwa IT, zabezpieczeń technicznych oraz cyberbezpieczeństwa powinny ze sobą współpracować, by lepiej zarządzać ryzykiem i je eliminować.*

*To oczywiste, że granice między tzw. silosami (działami w organizacji) zacierają się, stwarzając konkretne możliwości dla firm zajmujących się integracją systemów zaawansowanych* – dodaje K. Wine. – *Jako zaufany partner, integrator może pomóc w dialogu pomiędzy liderami IT i zabezpieczeń technicznych, wspierając współpracę między zespołami. Pozwoli ona wdrożyć odpowiednie zabezpieczenia techniczne oraz zapewni ochronę sieci i danych. Aby tego dokonać, integrator musi się wcielić w rolę konsultanta, a nie tylko sprzedawać i instalować technologie. Integratorzy muszą także inwestować w poszerzanie swojej wiedzy, by lepiej rozumieć wpływ urządzeń systemów zabezpieczeń na spójność sieci. Umiejętność komunikowania tych wyzwań specjalistom z obszaru IT i zabezpieczeń pomoże klientom w proaktywnej identyfikacji luk. Takie podejście ustawi integratorów w pozycji zaufanych partnerów i zapewni długotrwałe relacje z klientami.*

## Systematyczny udział w programach szkoleniowych

Najlepsze szkolenia zawsze organizują producenci, większość z nich stale zachęca integratorów do udziału w programach. Nie tylko zapewniają one wiedzę przydatną do pracy w terenie, lecz także pomagają w utrzymaniu ścisłej relacji między producentem a integratorem.

*Integratorzy powinni inwestować w rozwój swoich zespołów, nawiązując relacje z dostawcami w trakcie programów szkoleniowych i niezależnych programów certyfikujących. Ważne również, by skupiali się na sprzedaży*

*rozwiązań kompleksowych, które zwiększą ich wartość i zapewnią lepsze wsparcie dla klientów* – twierdzi M. Khoury.
Inni producenci podkreślają aspekt partnerstwa i to, jak bardzo producenci cenią sobie bliskie relacje z integratorami.
*Integratorzy są dla nas kluczowymi partnerami w komunikacji z użytkownikiem końcowym. Dostarczają najlepsze i odpowiednie rozwiązania* – mówi Alex Tan z Działu Kontroli Dostępu na region Azji Południowo-Wschodniej (ASEAN) w HID Global. – *Mamy nadzieję, że nasi integratorzy, oferując użytkownikom najnowsze produkty i technologię, podążą za trendami rynku. Zachęcamy ich także do udziału w szkoleniach, by na bieżąco znali najnowsze produkty i rozwiązania.*
Integratorzy mogą też korzystać z wiedzy niezależnych firm szkolenionych. W praktyce jednak szkolenia u producentów traktują jako podstawowe.

## Stały kontakt z użytkownikiem końcowym

Dla producenta jednym z atutów integratorów jest ich stały kontakt z użytkownikiem końcowym. Wspomagają więc producentów w poznaniu potrzeb klienta i dostosowaniu oferowanych rozwiązań.
*Pozycja integratorów systemów zabezpieczeń daje wyjątkowe możliwości poznania potrzeb użytkowników i dostarczenia im odpowiednich rozwiązań od producenta* – mówi M. Kane. – *Integratorzy powinni dbać o to, aby kanały komunikacji były zawsze otwarte, ponieważ to nimi płyną informacje o trendach w branży: od telewizji dozorowej, przez archiwizację danych wideo, po systemy zarządzania awaryjnego, alarmy, kontrolę dostępu i tak dalej.*

## Tworzenie systemów otwartych

M. Kane radzi integratorom, by oferowali rozwiązania oparte na platformach otwartych, zapewniając użytkownikom maksymalny zwrot z inwestycji.
*Integratorzy systemów security powinni postawić sobie za cel stosowanie i sprzedaż produktów umożliwiających łatwą integrację w ramach platformy otwartej. Wsłuchiwanie się w potrzeby klienta i dostarczanie mu rozwiązań umożliwiających ich bezproblemową współpracę z nowościami świadczy o trosce integratorów o najlepszą obsługę klienta. Gdy użytkownik zrozumie, że integrator ma na względzie jego dobro, powstanie partnerska relacja oparta na zaufaniu* – twierdzi M. Kane.
Integratorzy wiedzą, że można połączyć najwyższy poziom usług oferowanych klientom z osiąganiem własnych zysków. Na przykład kontrakty na usługi serwisowania czy hostingu umożliwią integratorom świadczenie usług w pełni zarządzanych.

Producenci są zainteresowani tym, aby integratorzy systemów chcieli poszerzać wiedzę na temat działalności użytkowników końcowych. Mogą w tym pomóc programy szkoleniowe. Ważna jest też rola integratora jako łącznika między użytkownikiem a producentem, która zapewni lepszą jakość usług i poprawi kondycję całej branży.

Integrator musi się wcielić w rolę konsultanta, a nie tylko sprzedawać i instalować technologie. Takie podejście ustawi integratorów w pozycji zaufanych partnerów i zapewni długotrwałe relacje z klientami.

# Wskazówki dla integratorów systemów, by mogli poprawić swoje wyniki biznesowe

Każdy producent ma własne rady dla integratorów systemów. Jedni podkreślają ogromne znaczenie programów szkoleniowych, inni sugerują, że powinni oni identyfikować potrzeby użytkownika wykraczające poza zastosowania security.

## Nie pomijaj możliwości spoza obszaru security

Według IDIS niektóre firmy zajmujące się integracją systemów typowych dla zastosowań zabezpieczeń technicznych nie dostrzegają możliwości znajdujących się poza ścisłym obszarem swojej działalności. Keith Drummond, dyrektor ds. sprzedaży w IDIS America, uważa, że takie podejście zamyka integratorom możliwości osiągania większych zysków.
*Uważam, że największym błędem integratorów jest przekonanie, że ich działalność polega na pozyskiwaniu zleceń, mnożeniu zysków, tworzeniu szans i zwiększaniu sprzedaży* – mówi K. Drummond. – *Odnoszę wrażenie, że często pomijają oni wiele okazji, nie korzystają z nich wcale lub korzystają, ale nie w takim*

*stopniu, w jakim mogliby to robić. W przypadku klientów indywidualnych priorytety są inne, natomiast jeśli chodzi o klientów biznesowych, efektem bądź celem ich działalności jest zwiększenie rentowności. To poprawa kultury biznesowej, lepsza wydajność i skuteczność. Telewizja dozorowa często jest postrzegana jedynie jako narzędzie zapewnienia bezpieczeństwa, ale integratorzy systemów powinni zdawać sobie sprawę z tego, że ma ona więcej możliwości. Może stanowić narzędzie analityki biznesowej lub marketingowe. Innymi słowy, telewizja dozorowa przyniesie użytkownikom różne dodatkowe korzyści w zależności od ich rodzaju działalności i branży.*

Stosując tego typu podejście, z systemu 10 kamer integratorzy mogą uczynić system działający jak 15-kamerowy, a z systemu 50 kamer – system 100-kamerowy. Jeśli będą potrafili uświadomić użytkownikom korzyści, jakie oferują rozwiązania security – szczególnie technologia HD, megapikselowa i zastosowanie narzędzi analitycznych – przyczynią się do rozwoju swojego biznesu.

*Przykładowo w sklepie można umieścić pięć kamer przy każdym wejściu albo rozlokować piętnaście kamer w całym obiekcie, dodać do tego narzędzia analityczne i w ten sposób zyskać narzędzie marketingowe lub analityki biznesowej* – kontynuuje K. Drummond. – *Odnoszę wrażenie, że integratorzy stricte systemów zabezpieczeń nadal myślą, że jest to dla nich jedyne zastosowanie. Gdy do projektu włączają się integratorzy IT mający doświadczenie spoza sektora security, widzą te kwestie szerzej. Natomiast integratorzy systemów zabezpieczeń często nie dostrzegają szans na rozwój własnej działalności.*

David Ella, wiceprezes ds. marketingu produktu w AMAG Technology, sugeruje, że integratorzy powinni najpierw wsłuchać się w swoich klientów i poznać funkcjonowanie ich biznesu, by na tej podstawie zaproponować zintegrowane technologie zabezpieczeń zapewniające klientom wartość dodaną. Tym samym przestaną konkurować wyłącznie ceną.

Łatwiej to powiedzieć, niż wykonać. Ale poświęcenie czasu na poznanie możliwości platform zarządzających przyniesie w perspektywie długoterminowej znaczne korzyści.

## Korzystanie ze szkoleń

Omawiając temat błędów popełnianych przez integratorów, David Ella zauważa, że producenci nie powinni pouczać integratorów. *Zrozumienie i wiedza o tym, w jaki sposób system monitoringu lub kontroli dostępu można przeobrazić w potężną zintegrowaną platformę proaktywnego zapewnienia bezpieczeństwa, może rozszerzyć wartość relacji z klientem w ujęciu długofalowym* – mówi D. Ella.

– *Zbyt dużo systemów monitoringu wizyjnego informuje dziś ludzi o tym, co już się wydarzyło, nie współpracując z innymi dostępnymi technologiami w celu powstrzymania naruszeń bezpieczeństwa, zapobiegania im i minimalizacji ich skutków.*

Użytkownicy zatrudniają integratorów ze względu na ich wiedzę, nie chcą tracić czasu na pozyskiwanie informacji. System powinien działać. Mają ogólne wyobrażenie na temat efektu, lecz oczekują, że integrator będzie mózgiem przedsięwzięcia, będzie miał dane i niezbędną wiedzę w zakresie najnowszych technologii.

*Dlatego uważam, że integratorzy powinni się przede wszystkim szkolić. W branży jest za dużo takich, którzy zawsze działają tak samo, nigdy nie próbując postępować inaczej* – podkreśla K. Drummond. Akcentuje tym samym, że szkolenia powinny stanowić pierwszy krok edukacji integratorów systemów.

– *Trzymają się tego, co jest im znane, czując się komfortowo z daną technologią, produktem czy producentem, nie zwracają uwagi na potrzeby klientów* – kontynuuje K. Drummond. – *A to nie jest dostosowanie do potrzeb użytkownika. Trzeba być na bieżąco przede wszystkim w zakresie nowości technologicznych, szkolić się i stosować w praktyce nabytą wiedzę.*

## Podejmowanie wyzwań

Mimo wszystko dostawcy usług zgodnie twierdzą, że przed integratorami stoją dzisiaj istotne wyzwania mające wpływ na ich biznes.

*Integratorzy nie mogą dłużej instalować systemów kontroli dostępu i dozoru wizyjnego bez zrozumienia potrzeb bezpieczeństwa użytkownika oraz jego potrzeb biznesowych* – podkreśla D. Ella. – *Powinni mieć bieżące rozeznanie w każdej technologii i wiedzieć, jak pomóc klientowi w usprawnieniu procesów, uproszczeniu operacji i unikaniu ryzyka. Zrozumienie biznesu klienta wymaga czasu, podobnie jak nauka nowych technologii oraz możliwości ich integracji. Czas na to poświęcony to czas dobrze spożytkowany. Integratorzy staną się wtedy ekspertami technologicznymi, na których klient będzie polegać i do których będzie się zwracać w sprawie ulepszeń czy rozbudowy.*

Telewizja dozorowa często jest postrzegana jedynie jako narzędzie zapewnienia bezpieczeństwa, ale integratorzy powinni zdawać sobie sprawę, że ma ona więcej możliwości. Może stanowić narzędzie analityki biznesowej lub marketingowe.

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

# Optymalizacja zarządzania ochroną obiektów z użyciem oprogramowania integrującego

**Jak skutecznie zabezpieczyć wszystkie oddziały przedsiębiorstwa**, zachowując jednolite standardy ochrony w każdym z nich? Czy można centralnie administrować rozproszonymi instalacjami bezpieczeństwa?

Zarządzanie organizacją mającą oddziały w różnych lokalizacjach wymaga uwagi oraz nakładów czasu i środków. Dotyczy to każdego aspektu działania firmy, w tym obsługi systemów ochrony. Powstają specjalne rozwiązania umożliwiające centralny nadzór nad autonomicznymi systemami bezpieczeństwa, jednocześnie ułatwiające i usprawniające cały proces. Ich wdrażaniem zajmuje się integrator – podmiot odpowiedzialny za opracowanie i przygotowanie powstającej lub istniejącej infrastruktury na potrzeby programów integrujących.

Przykładem takiego narzędzia jest **INTEGRUM** – oprogramowanie zaprojektowane przez inżynierów SATEL.

## W czym pomaga zintegrowane zarządzanie bezpieczeństwem?

**INTEGRUM** umożliwia łączenie wielu instalacji w jeden skalowalny system bezpieczeństwa. Sprawdzi się wszędzie tam, gdzie występuje rozproszona struktura organizacyjna. Dzięki niemu każda placówka instytucji czy firmy wielooddziałowej, takiej jak sieci handlowe, banki czy agencje rządowe ma zapewnioną stałą ochronę na najwyższym poziomie.

INTEGRUM jest narzędziem umożliwiającym proste administrowanie siecią placówek i ich użytkownikami, zapewniającym optymalizację kosztów i oszczędność czasu. To idealne rozwiązanie dla osób dbających o bezpieczeństwo wielooddziałowych organizacji.

Aby taki system działał sprawnie i wydajnie, powinien być wdrożony i obsługiwany przez profesjonalnego integratora, który cały proces przeprowadzi odpowiedzialnie i fachowo, a po jego zakończeniu będzie służył kompleksowym doradztwem.

Więcej na:
**integrum.satel.pl**

## KORZYŚCI ZASTOSOWANIA INTEGRUM

**Mobilność**
Koordynator w drodze do odbioru technicznego nowego obiektu „Oddział Konin" otrzymuje informację o awarii w „Oddziale Sopot". Może zalogować się do systemu ze smartfonu i szybko wskazać źródło problemu. Natychmiastowe wysłanie serwisu jest jedynie formalnością.

**Zdalne zarządzanie użytkownikami**
Osoba z Działu Kadr w Gdańsku przyjmująca nowego pracownika może utworzyć dla niego profil użytkownika z kartą zbliżeniową dającą dostęp do obiektu w Elblągu, gdzie ma rozpocząć pracę. Karta po okresie próbnym może automatycznie przestać działać, a po przedłużeniu umowy dostęp zostanie zdalnie odnowiony.

**Kontrola konfiguracji**
W poznańskiej placówce bankowej miało miejsce włamanie. Specjalista ze stołecznego biura ochrony może w kilka minut sporządzić zestawienie zmian ustawień centrali alarmowej i przekazać je policji.

Będzie to pomocne w ustaleniu, czy w ostatnim okresie nie dokonano sabotażu konfiguracji instalacji.

**Raportowanie**
Po przeprowadzeniu konserwacji systemów alarmowych w oddziałach automatycznie zostaje wygenerowany raport rozbieżności między wcześniejszą a bieżącą konfiguracją central. Dzięki temu administrator może szybko sprawdzić, czy nie został odłączony istotny element instalacji.

**Wygoda obsługi**
Dozorca otrzymuje informację o alarmie w strefie „Garaż". W panelu sterowania wybiera widok planu obiektu, na którym znajduje się ta strefa. Z poziomu mapy może uruchomić podgląd z kamer i zweryfikować, czy alarm nie jest fałszywy. W zależności od sytuacji może go skasować lub wezwać służby oraz umieścić stosowny komentarz przy zarejestrowanym zdarzeniu.


# Skuteczna obserwacja wymaga dobrego zarządzania

Zarządzającym wydaje się, że obserwacja za pomocą kamer dozorowych jest prosta, jak oglądanie telewizji. Badania naukowe i doświadczenia specjalistów Akademii Monitoringu Wizyjnego pokazują, że rzadko jest prowadzone w sposób celowy i systematyczny, co wpływa negatywnie na skuteczności systemów CCTV. **Algorytmy analizy obrazu obiecują skuteczność, ale automatyzacja może rozleniwiać obserwatorów. Jak więc zapewnić skuteczny dozór?**

**Paweł Wittich**
**psycholog, specjalista ds. personelu systemów CCTV, Akademia Monitoringu Wizyjnego**

Podczas oglądania programu „Kuchenne rewolucje" moją uwagę przykuł fragment, kiedy kucharze z nietęgimi minami przed prowadzącą tłumaczyli się z brudu w piekarnikach i grillach, mówiąc „bo mamy na głowie za dużo obowiązków", „bo są ważniejsze sprawy". Na pytania skierowane do operatorów i kierowników systemów monitoringu wizyjnego, dlaczego nie wyznaczają celów obserwacji dla kamer i na tej podstawie nie prowadzą metodycznej obserwacji, padają podobne odpowiedzi. Inne typowe usprawiedliwienia: „to nie ma sensu", „to strata czasu", „tam się nic nie dzieje", „już próbowaliśmy i to nic nie dało" (choć nie został ślad w formie katalogu celów lub zarys strategii prowadzenia obserwacji). Niezależnie od środowiska – czy to kuchnia, czy centrum monitoringu wizyjnego – uzyskanie wysokiej jakości działania wymaga zmiany nawyków pracowników i zarządzających[1]. Żeby operatorzy mogli prowadzić skuteczną obserwację, należy wdrożyć takie zasady, które będą zachęcały ich do metodycznego monitorowania podległych im obszarów.

## Podstawowy błąd zarządzających

Przyglądam się zarządzającym systemami monitoringu wizyjnego od 10 lat i, niestety, ciągle spotykam się z mieszanką niefrasobliwości, braku wiedzy i nonszalancji w podejściu do obserwacji. Część kierowników uważa, że prowadzenie dozoru za pomocą kamer to tak banalna praca, że nie ma potrzeby formułować celów i wymagań dla operatorów. Zarządzający błędnie zakładają, że operatorzy wiedzą, co mają robić. Na jakiej podstawie, nie wiadomo, gdyż rzadko kontrolują jakość pracy podwładnych. Prowadzone przeze mnie audyty organizacyjne pokazują, że operatorzy różnią się aktywnością, liczbą wykrytych zagro-

żeń i sprawnością w prowadzeniu kamer. Co najistotniejsze, różnią się podejściem do pracy. Jak w każdej branży, są zarówno odpowiedzialni i zaangażowani pracownicy, jak i tacy, którym się nie chce pracować lub nie mają predyspozycji do pracy na danym stanowisku.
Ludzie są ewolucyjnie i kulturowo nastawieni na współpracę. Chętnie tworzą zespoły, ponieważ to pozwala im rozwiązywać problemy i osiągać korzyści[2]. Praca zespołowa wymaga koordynacji, w przeciwnym razie bowiem każdy członek zespołu robi, co chce. Najczęstszym podstawowym błędem kierującymi systemami CCTV jest założenie, że nie muszą zarządzać operatorami lub pracownikami ochrony obsługującymi kamery monitoringu. Co ciekawe, dzieje się tak w miejskich systemach monitoringu wizyjnego, w sklepach i zakładach przemysłowych.
Z kontroli przeprowadzonej w polskich miastach przez Najwyższą Izbę Kontroli wynika, że najlepsze wyniki osiągają te systemy, w których zostały określone standardy prowadzenia obserwacji[3]. Jeżeli kierownik nie wyznacza celów, nie motywuje i nie ocenia operatorów, to nie wykorzysta potencjału ludzi i techniki CCTV. Ten uniwersalny problem nie dotyczy tylko Polski[4].

## Co to jest skuteczna obserwacja?

Mówiąc wprost, są to wiedza, co obserwować, i jej metodyczne wykorzystanie.
W kolejnych wydaniach Polskiej Normy nie zmienia się część dotycząca określenia celów dla systemu monitoringu wizyjnego. Zaleca ona ustalenie dla każdego obszaru typów zagrożeń, częstotliwości i konsekwencji ich wystąpienia (straty). Na tej podstawie zarządzający mogą określić cele, priorytety, warunki, miejsca szczególnego zainteresowania, osoby, obiekty oraz procesy podlegające obserwacji i zakres pożądanej reakcji. Te same zalecenia można znaleźć w opracowanej przez brytyjską policję metodzie „Wytycznych funkcjonalnych”[5].

> Skuteczniejsi są ci operatorzy, którzy zwracają uwagę na zachowanie osób – ich gesty, postawę, mimikę, na co lub na kogo kierują wzrok.

Badania dotyczące efektywności obserwacji wskazują, że skuteczniejsi w wykrywaniu zagrożeń są ci operatorzy, którzy większą uwagę zwracają na zachowanie osób, w szczególności na ich gesty, postawę, mimikę i na co lub na kogo kierują wzrok[6]. Oznacza to, że operatorów należy szkolić w prawidłowym odczytywaniu mowy ciała.
Z połączenia wyników badań na temat pracy operatorów z zaleceniami dotyczącymi wyznaczania celów wynika, że zarządzający systemem CCTV powinien stworzyć mechanizm, który spowoduje, że operatorzy będą • w zaplanowany sposób, kolejno obserwować miejsca w polu widzenia kamery, w których • ludzie najczęściej generują zagrożenia, • zwracając uwagę na ich zachowanie, ponieważ to • zapewni największe prawdopodobieństwo wykrycia zdarzenia.

## Wzorcowy model częstochowski

Tomasz Pasieka, kierownik miejskiego systemu CCTV w Częstochowie, opracował mechanizm prowadzenia skutecznej obserwacji przez operatorów. Każda kamera ma kartę, w której zostały opisane cele i priorytety dozoru oraz miejsca szczególnego zainteresowania, np. przystanek autobusowy ze wskazaniem na występujące tam zagrożenia. Operator jest zobowiązany do patrolowania tych miejsc za pomocą kamery i ich znakowania (tagowania) w zapisie obrazu, kiedy kieruje na nie obiektyw. Tagowanie jest podstawowym kryterium oceny pracy operatora. Zmusza to obserwatorów do gruntownego poznania obszarów objętych dozorem i uważnego przyglądania się miejscom, gdzie dochodzi do zagrożeń.
W efekcie operatorzy mają także okazję przyglądać się zachowaniom ludzi, którzy przebywają w tych miejscach. W związku z tym prawdopodobieństwo, że zauważą niepokojące sygnały, się zwiększa. Wysoko oceniani są ci operatorzy, którzy wychwytują sytuacje przeradzające się w zdarzenia oraz niewymagające interwencji, ale obserwowane sygnały mowy ciała świadczą, że osoby robią coś nietypowego, być może niebezpiecznego. Wskazuje to na koncentrację i zaangażowanie obserwatora.
Mechanizm zachęcania do prowadzenia obserwacji jest uzupełniany przez ćwiczenia, szkolenia i coaching, co buduje i utrwala dobre nawyki operatorów. Częstochowska straż miejska opracowała aplikację, która pomaga kierownikowi monitorować i oceniać pracę operatorów monitoringu miejskiego.

## Automatyzacja wymaga dobrego zarządzania

Współczesna technika zapowiada wygodę i dużą skuteczność, także w branży systemów CCTV (VSS). Coraz więcej użytkowników sięga po algorytmy analizy obrazu. Przyglądając się tego typu rozwiązaniom, okazuje się, że nie wszędzie można je zastosować ze względu na dużą liczbę fałszywych alarmów. Skuteczność części algorytmów jest ograniczona z powodu złożoności zjawiska, jakie mają wykrywać, lub zależy od czynników środowiskowych (oświetlenie, zawartość tła). Często wymagają od użytkowników rozłożonej w czasie konfiguracji i systematycznego weryfikowania skuteczności, z czym – jak pokazują konsultacje prowadzone przez specjalistów Akademii Monitoringu Wizyjnego – użytkownicy radzą sobie z różnym skutkiem.
Wydaje się więc, że nie należy łatwo ulegać słodkiej obietnicy lenistwa, którą oferuje automatyzacja. Stereotypowe podejście operatorów „to się nagra” może być uzupełnione o „to się wykryje”, co stwarza ryzyko, że w systemie bezpieczeństwa miasta, sklepu czy zakładu przemysłowego powstaną dziury. W mojej ocenie zawsze warto wracać do podstaw, czyli:

1) przeprowadzić analizę bezpieczeństwa i ustalić wymagania dla systemu CCTV,
2) określić, które obszary wymagają obserwacji prowadzonej przez operatorów, a gdzie jest możliwe zastosowanie algorytmów,
3) weryfikować skuteczność algorytmów dla różnych warunków i scenariuszy.

Ponadto należy stawiać cele i zadania, motywować i oceniać pracowników prowadzących dozór za pomocą kamer lub obsługujących wideoalarmy.

1) S.R. Covey, *7 nawyków skutecznego działania*, Warszawa 2017.
2) J. Haidt, *Prawy umysł. Dlaczego dobrych ludzi dzieli religia i polityka?*, Sopot 2014.
3) P. Wittich, *Skuteczny monitoring czy maszynka do wystawiania mandatów?* „Systemy Alarmowe” 4/2014.
4) www.cctv.org.pl/publikacje/poradniki-brytyjskiej-policji-police-scientific-development-branch/
5) J. Aldridge, *Wytyczne funkcjonalne dla systemu CCTV, Make it Work*, Akademia Monitoringu Wizyjnego, Gliwice 2005
6) http://eis.bris.ac.uk/-psidg/download/HTGBH2009.pdf

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

Kamera WiseNetIII SNO -6085R

**Realizacje security w obiektach infrastruktury krytycznej należą do szczególnie wymagających i są ważne dla branży zabezpieczeń.**

# Dla najbardziej wymagających

**Sławomir Szlufik**
**Hanwha Techwin**

Infrastruktura krytyczna obejmuje dwanaście sektorów czy też gałęzi gospodarki, takich jak energetyka, surowce energetyczne i paliwa, łączność, sieci teleinformatyczne, sektor finansowy, zaopatrzenie w żywność i wodę, ochrona zdrowia, transport i ratownictwo, systemy składowania oraz wytwarzania substancji chemicznych i promieniotwórczych. Systemy telewizji dozorowej stanowią tam bardzo ważny element bezpieczeństwa i całości systemów zarządzania.

## Pęd ku przyszłości

Hanwha Techwin Europe jest spadkobiercą, a jednocześnie kontynuatorem działalności firmy Samsung Techwin. Powstała w Korei w 1952 r. jako Korea Explosives była i jest koreańską firmą prywatną. Została utworzona jako zakład produkujący materiały wybuchowe. Dynamit stanowił istotny element podczas odbudowy kraju zniszczonego przez wojnę koreańską. W latach 1964–80 zarząd postanowił poszerzyć działalność i rozpoczął inwestowanie w zakłady przemysłowe, m.in. elektrownie, kopalnie, stalownie, huty i zakłady wytwarzające elektronikę, centra dystrybucyjne i serwisowe produktów B2B, a także instytucje finansowe. Od roku 2007 firma prowadzi intensywną ekspansję na nowe rynki: mechatroniki, przemysłu lotniczego i kosmicznego (aerospace), energetyki słonecznej, przemysłu chemicznego oraz rozwiązań security z zakresu CCTV. W roku 2014 Hanwha Group stała się właścicielem kilku oddziałów B2B firmy Samsung Electronics, w tym również spółki Samsung Techwin oferującej rozwiązania CCTV. Do końca 2016 r. zanotowała niespotykany rozwój – w ciągu 24 miesięcy wprowadziła około 100 nowych produktów.

## Od Quality do eXtreme – 60 nowych modeli kamer

Hanwha Techwin ma w swoim portfolio kamery analogowe i kamery AHD (analogowe o zwiększonej rozdzielczości do 2 Mpix), jak i tanie kamery IP serii WiseNet Lite czy nowe kamery serii Q w rozdzielczościach 2 i 4 Mpix. Tam, gdzie zaprojektowano system z zaawansowaną analityką obrazu, zastosowanie znajdą kamery z procesorem WiseNet III oraz nowa linia urządzeń serii P. Sztandarowym produktem są obecnie kamery serii X wyposażone w najnowszy procesor WiseNet V (urządzenia do eXtremalnych warunków z eXtra możliwościami zastosowań). Jest to oferta dla różnych inwestycji wymagających specjalizowanych urządzeń dopasowanych do potrzeb konkretnego projektu.

## Technologia analogowa nadal ma się dobrze

Firma przygotowała kompleksową ofertę rozwiązań na potrzeby wszystkich sektorów i systemów infrastruktury krytycznej. Kamery analogowe z serii Beyond (np. modele SCB – 5000/5003/5005) zainstalowano w wielu elektrowniach, centrach logistycznych, więzieniach czy szpitalach. To sprawdzone i niezawodne urządzenia, które nawet w czasach popularnego IP są chętnie kupowane przez instalatorów. Ich wieloletnia bezawaryjna praca stanowi ogromną zaletę w obiektach, w których obowiązują specjalne procedury instalacji czy serwisu urządzeń. Serię

Network kontroler SPC-7000

urządzeń analogowych powoli zastępuje nowa linia produktów w technologii AHD *(Analog High Definition resolution)*, czyli urządzeń pozwalających przesyłać kablem koncentrycznym obrazy w rozdzielczości 2 Mpix i większej. Hanwha Techwin w 2016 r. uzupełniła swoją ofertę o linię takich urządzeń.

## (Nie)bezpieczne miasto

Nawet najlepsze kamery nie spełnią swojej roli, jeśli system nie zostanie wyposażony w sprawdzone urządzenie do rejestracji. Hanwha Techwin proponuje rejestratory PRN – 4011/4000 o wysokim stopniu niezawodności, z podwójnymi zasilaczami, systemem RAID 5 i 6 bądź dyskami typu *hot swap*, czyli wyjmowanymi podczas rejestracji bez zatrzymywania zapisu. Coraz więcej miast czy strategicznych obiektów państwowych wymaga rejestracji w pełnej rozdzielczości wielomegapikselowej i archiwizacji nawet do 90 dni. Wybór odpowiedniego rejestratora jest więc bardzo ważny.

## Porządna klawiatura jest dobra na wszystko

Po wystąpieniu zdarzeń często padają opinie, że wprawdzie system jest nowy, zainstalowano nowe kamery, ale obserwowanie obrazów ze 100 kamer na trzech 24-calowych monitorach z podziałem na 16 nie może być skuteczne. To ważne spostrzeżenie, tymi urządzeniami i wyświetlaniem z nich obrazów należy odpowiednio zarządzać. Do tego celu posłuży prosty system sterowania kamerami i wyświetlaniem obrazów na monitorach.
Hanwha Techwin proponuje klawiaturę SPC-7000, która po zaprogramowaniu pozwoli na sterowanie kamerami, a także wyświetlanie obrazów z poszczególnych kamer na konkretnych monitorach. Jej atutem jest możliwość zaprogramowania różnych parametrów lub wgrania własnego programu do sterowania, np. kamerą na głowicy obrotowej.

## Widzimy i wyświetlamy, ale nie zarządzamy...

Kamery i rejestratory bez odpowiedniego oprogramowania do zarządzania, przeglądania czy wyświetlania obrazów stanowią tylko 30% całego rozwiązania. Kolejne 45% to oprogramowanie, pozostałe 25% – dobrze wyszkolona obsługa oraz właściwe scenariusze zachowań czy reakcji w sytuacjach kryzysowych. Tylko wtedy system telewizji dozorowej spełnia swoje zadania. Dlatego Hanwha Techwin, opierając się na wieloletnich doświadczeniach z rynku, opracowała oprogramowanie SSM w dwóch wersjach: Professional i Enterprise oraz „uszyte na miarę" oprogramowanie w wersjach SSM Transport, SSM Safe City i SSM Retail – oprogramowanie dla sklepów, centrów handlowych oraz sieci sprzedaży detalicznej.

## Bezpieczeństwo a cyberprzestępcy

Branża security – o czym należy wspomnieć – również wkroczyła w świat cyberprzestrzeni, a co za tym idzie cyberprzestępców. Dlatego wybierając dane rozwiązania, należy sprawdzić, a nawet zażądać od dostawcy potwierdzenia, że proponowany system oraz urządzenia są zabezpieczone przed cyberatakami i nie posiadają tzw. furtek dla nieautoryzowanych użytkowników. Wielu producentów a do takich należy również Hanwha Techwin, już na wstępie informuje klientów o tym, że urządzenia zostały sprawdzone pod kątem bezpieczeństwa sieciowego.

Delta-Opti
ul. Graniczna 10,
60-713 Poznań
www.delta.poznan.pl

# Wielofunkcyjny tester CCTV – nieoceniona pomoc dla każdego instalatora

**CS-HBF-72MQ jest testerem zaprojektowanym z myślą o instalacjach telewizji dozorowej.** O szerokiej przydatności urządzenia decyduje jego wielofunkcyjność. Największym atutem, zapewniającym uniwersalne wykorzystanie, jest wielosystemowość.

Łatwość i wygodę użytkowania zapewnia przejrzysty interfejs graficzny w języku polskim oraz 7-calowy ekran dotykowy o rozdzielczości 1024 x 600 pikseli. Sterowanie funkcjami może się odbywać w sposób dotykowy lub za pomocą przycisków. Akcesoria mocujące i długi czas pracy na akumulatorze gwarantują instalatorowi bezpieczną i wygodną pracę.
Tester wspiera wszystkie obowiązujące standardy przesyłu sygnału wizyjnego w systemach telewizji dozorowej, takie jak AHD, HD-CVI, HD-TVI, HD-SDI oraz IP w wysokiej rozdzielczości obrazu full HD. Jest również zgodny ze starym analogowym standardem CVBS. Umożliwia zatem przetestowanie kamery pracującej w dowolnej z wymienionych technologii.
Urządzenie może też pracować jako źródło zasilania kamer, dostarczając napięć 5 VDC, 12 VDC oraz PoE (48 V). Tester pozwala na sterowanie kamerami obrotowymi PTZ dzięki zaimplementowaniu ponad 30 protokołów i interfejsom RS-232 oraz RS-485. Umożliwia również monitorowanie danych portu szeregowego RS-232 lub RS-485.
W odniesieniu do kamer IP tester ma funkcję wyszukiwania i podglądu kamer zgodnych z Onvif oraz wbudowane aplikacje umożliwiające podgląd obrazów z kamer IP wielu producentów. Urządzenie może być też źródłem zasilania kamery IP zgodnym ze standardem PoE, dzięki czemu można ją szybko przetestować w miejscu instalacji jeszcze przed podłączeniem jej do istniejącej infrastruktury. Należy również wspomnieć o innych funkcjach sieciowych testera, takich jak monitorowanie połączeń LAN, skanowanie adresów IP, testowanie łącza – PING, wykrywanie podłączonego portu w switchu, testowanie skrętki komputerowej lub kabli telefonicznych, współpraca ze switchami PoE, pomiar zasilania PoE. Tester ma zainstalowaną przeglądarkę internetową oraz obsługuje sieci Wi-Fi, co umożliwia dostęp do internetu w celu np. zweryfikowania dostępu do systemu monitoringu przez interfejs www.
Do przydatnych funkcji należy też reflektometr TDR umożliwiający wykrywanie i lokalizację miejsca przerwania lub zwarcia kabla (koncentrycznego lub UTP). Możliwa jest także identyfikacja przewodu w wiązce. W przypadku kabli światłowodowych można zlokalizować uszkodzenia włókien – lokalizator VLS (VFL) oraz dokonać pomiaru mocy optycznej.
W urządzeniu nie zabrakło miejsca na generator obrazu testowego, tester audio, miernik cyfrowy (pomiar napięcia, prądu, rezystancji, pojemności elektrycznej, test ciągłości, test diody), kalkulator, a nawet wbudowaną latarkę. Tester umożliwia zapis materiału wideo na kartę microSD (8 GB w zestawie) z możliwością odtwarzania nagrań.
Warto wspomnieć o bardzo dobrym stosunku ceny urządzenia do jego jakości i liczby zaimplementowanych funkcji oraz interfejsów.

Więcej informacji można uzyskać na stronie Delta-Opti: **www.delta.poznan.pl**, pod nr. tel.: 61 864 69 70 bądź przez **e-mail: technika@delta.poznan.pl.**

Assa Abloy Poland
ul. Jana Olbrachta 94,
01-102 Warszawa
www.assaabloy.com.pl

# ABLOY® PROTEC2 CLIQ – inteligentne zarządzanie bezpieczeństwem

Instytucje państwowe i publiczne, duże przedsiębiorstwa, ale też małe firmy swoją działalność opierają na **możliwości ciągłego świadczenia usług 24 godziny na dobę.**

Przerwy i zakłócenia w dostawach prądu, wody lub danych telekomunikacyjnych stanowią zagrożenie ich funkcjonowania i bezpieczeństwa, mogą powodować utratę zysków, a nawet zagrażać zdrowiu i życiu ludzi. Dlatego tak ważny jest wybór systemu zapewniającego wysoki poziom ochrony przed nieuprawnionym dostępem.
Kluczowe obiekty infrastruktury krytycznej są często rozproszone na ogromnych obszarach lub położone w oddalonych i odizolowanych miejscach. Stanowią one łatwy cel ataków zorganizowanych grup przestępczych, sabotażu czy aktów wandalizmu. Ich ochrona nabiera zatem niezwykłej wagi.
Podstawą zabezpieczeń są surowe procedury bezpieczeństwa, kontrolowany dostęp personelu i izolowanie sprzętu przed dostępem osób nieuprawnionych. Niezbędne są też rozwiązania, dzięki którym codzienne operacje przebiegają płynnie i bez problemu. Systemem pozwalającym sprawnie zarządzać kluczami i monitorować ich użytkowanie jest PROTEC2 CLIQ marki ABLOY.

**PROTEC2 CLIQ to prosty w użytkowaniu i skalowalny system zarządzania dostępem do klucza przez internet, oszczędzający czas i koszty obsługi.** Kontrola dostępu została oparta na cylindrach wykonywanych w technologii dyskowej o wysokim poziomie zabezpieczenia oraz szyfrowanej identyfikacji elektronicznej. Integracja techniki mechanicznej i elektronicznej pozwoliła w tym przypadku uzyskać podwójne zabezpieczenie i podwójną kontrolę. System jest łatwy w obsłudze dla pojedynczego użytkownika, ponieważ dostęp do odpowiednich miejsc zapewnia tylko jeden symetrycznie ukształtowany klucz. ABLOY PROTEC2 CLIQ można dowolnie rozbudowywać lub aktualizować, wprowadzając do niego nowe lokalizacje i zamki. Dzięki temu system można dostosować do potrzeb firmy lub organizacji, w której ma funkcjonować.
Do zarządzania systemem służy dedykowany program CLIQ Web Manager działający z wykorzystaniem przeglądarki internetowej i umożliwiający zmianę praw dostępu niezależnie od miejsca i czasu. Administrator może nadawać lub odbierać uprawnienia użytkownikom oraz nadzorować ich czynności. W przypadku zgubienia klucza można go łatwo usunąć z systemu i wprowadzić nowy. Ponadto program zapisuje każdorazowe użycie klucza, dzięki czemu zarządca obiektu otrzymuje pełen raport dotyczący wejść, wraz z dokładną godziną w odniesieniu do wszystkich lokalizacji.
Co ważne, komunikacja, w tym transfer danych i prawa dostępu, są szyfrowane. Oprócz aplikacji CLIQ Web Manager dla wygody użytkowników wprowadzono również mobilną aplikację CLIQ Connect pozwalającą w dowolnym miejscu i czasie pobierać oraz aktualizować uprawnienia dostępu na swoim kluczu. Do programowania kluczy można więc wykorzystać zarówno dedykowane urządzenia (zdalne programatory), jak i smartfon. Dzięki temu uprawniony personel może natychmiast otworzyć zabezpieczone przejścia.

## Mobilny wykrywacz przemytu

# SAS-Hitech-Xpose dla straży granicznej i wojska


Mobilny wykrywacz kontrabandy SAS-Hitech-Xpose to flagowy sprzęt SAS R&D Services, dostawcy dla sektora obronnego USA specjalizującego się w sprzęcie do detekcji przemytu. **Co wyróżnia ten miernik gęstości – oprócz nowoczesnej technologii zamkniętej w kompaktowej budowie – spośród rozwiązań konkurencyjnych?**

### MOBILNY WYKRYWACZ KONTRABANDY

*Wykrywacz Xpose służy nie tylko do kontroli granicznej znajduje, też zastosowanie w ochronie mienia. Korzysta z niego również wojsko, kontrolując pojazdy w zagrożonych strefach* – wyjaśnia Krzysztof Rydlak, specjalista ds. bezpieczeństwa ze sklepu detektywistycznego Spy Shop, oferującego rozwiązania SAS R&D na rynku polskim. – *Xpose sprawdzi się w obiektach, w których ze względów bezpieczeństwa należy dokonywać kontroli, czy na ich teren nie są przemycane niedozwolone przedmioty.*

Lekki i niewielki miernik gęstości w trwałej obudowie z odlewu uretanowego ma zwartą konstrukcję, w której wykorzystano materiały trwalsze niż w dotychczasowych rozwiązaniach. Wykrywacz jest odporny na upadek z wysokości 1 m i pracuje w szerokim zakresie temperatury (-25...55°C). Jest wodoodporny (IP56), a podświetlany ekran pokryto twardym szkłem Gorilla Glass. Dzięki zredukowanej masie miernik gęstości może być przenoszony w zabezpieczającym, przypiętym do paska pokrowcu ochraniającym sprzęt. W przypadku inspekcji trudno dostępnego miejsca, np. ciężarówki, można skorzystać z teleskopowego uchwytu (1,4 do 2,5 m) oraz dodatkowego ekranu Xtreme, mocowanego na wysięgniku i łączącego się kablem USB lub bezprzewodowo przez Bluetooth.

Chociaż w projektowaniu wykrywacza SAS-Hitech-Xpose brali udział oficerowie amerykańskiej policji i zastosowano w nim zaawansowane rozwiązania, sprzęt jest łatwy w obsłudze, a wyniki prezentowane czytelnie.

Urządzenie spełnia restrykcyjne wymagania stawiane rozwiązaniom do detekcji przemytu bez czasochłonnego demontażu lub uszkodzenia pojazdu czy innego obiektu. Sprawdza trudno dostępne miejsca, takie jak opony, grodzie, puste przestrzenie w pojeździe lub łodzi.

SAS-Hitech-Xpose ma dwa główne tryby pracy. W trybie Survey działa jako miernik promieniowania, lokalizując materiały radioaktywne. Z kolei w trybie Inspect mierzy gęstość badanego obiektu i wskazuje jej zmiany w trybach cyfrowym oraz graficznym, prezentując na ekranie przebieg zmian gęstości w ciągu 30 s. Wyniki mogą być pokazywane w wartościach bezwzględnych, w odniesieniu do gęstości zmierzonej jako bazowa lub w odniesieniu do wartości „0".

Zmiany gęstości powyżej wartości progowej mogą być również sygnalizowane alarmem dźwiękowym. Urządzenie może pracować także ze słuchawkami (złącze jack 3,5 mm). Dane pomiarowe można skopiować na komputer przez USB dzięki oprogramowaniu Xpose Tools na DVD. SAS-Hitech-Xpose zasilany bateriami pracuje do 40 godz. bez przerwy, a czas czuwania jest nawet 2,5 razy dłuższy niż u konkurencji – do 6 miesięcy. Sprzęt jest bezpieczny dla operatora i otoczenia. Dawka promieniowania odbierana przez użytkownika lub osobę postronną nie przekracza 0,05 mR/h na całe ciało. W testach zarówno przy otwartej, jak i zamkniętej osłonie źródła promieniowania odnotowano dawkę 0,01 do 0,03 mR/h. Urządzenie jest zwolnione z obowiązku rejestrowania, ponieważ aktywne źródło promieniowania Ba 133 nie przekracza 10µCi, 370 kBq. Twórcy poprawili właściwości wykrywania – miernik prześwietla materię na głębokość nawet 15 cm.

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

# Termowizja – rewolucja w systemach bezpieczeństwa

**Coraz częściej kamery termowizyjne są stosowane w różnych dziedzinach,** takich jak energetyka, budownictwo, ratownictwo czy zakłady produkcyjne.

**Maciej Pietrzak**
Sales Support Engineer

W procesach produkcyjnych nadzorują jakość produktów i wykrywają wszelkie nieprawidłowości. Są też pomocnym narzędziem do kontroli kondycji maszyn wykorzystywanych w procesach produkcyjnych. Pierwszym symptomem zużywających się łożysk jest zwiększone tarcie elementów, a w jego efekcie ich wyższa temperatura. Termowizja umożliwia wykrycie anomalii już we wczesnym stadium, co pozwala na podjęcie reakcji, zanim elementy ulegną definitywnemu uszkodzeniu, a co za tym idzie unieruchomią linię produkcyjną, co wiąże się z ogromnymi stratami dla przedsiębiorstwa.
Kamery termowizyjne wyróżnia przede wszystkim możliwość obserwacji tego, czego zwykła kamera czy oko ludzkie nie są w stanie dostrzec.
Kamery termowizyjne mierzą fale elektromagnetyczne emitowane przez ciała o temperaturze wyższej niż zero bezwzględne. Odczyt jest interpretowany i przedstawiany w formie graficznej, a każda wartość odczytanej temperatury ma przypisany inny kolor. To, jak intensywne jest promieniowanie termiczne danego obiektu, zależy od jego własnej temperatury, czyli mierząc promieniowanie podczerwone danego obiektu, mierzymy jego temperaturę.
Elementem kamery termowizyjnej służącym do pomiaru temperatury jest detektor promieniowania podczerwonego. Ze względu na budowę i zasadę działania można wyróżnić przetworniki termiczne, piroelektryczne, fotonowe, bolometry, z chłodzeniem kriogenicznym lub niechłodzone. Różnice wynikające z ich budowy i zasady działania nie tylko wpływają w znaczący sposób na dokładność, z jaką umożliwiają odczyt, ale także na możliwy czas pracy. Niestety wysoka dokładność pomiarów przy wykorzystaniu przetworników chłodzonych jest okupiona krótkim czasem eksploatacji i wysoką ich ceną. Kamery wyposażone w przetworniki chłodzone wymagają okresowych napraw eksploatacyjnych, co powoduje dodatkowe koszty. Dopiero wprowadzenie kamer termowizyjnych opartych na niechłodzonych układach detekcji pozwoliło na szerszą dostępność tej technologii i wykorzystanie jej w różnych dziedzinach. Są one znacznie tańsze oraz nie generują okresowych kosztów eksploatacyjnych. Z racji szybkiego rozwoju i poprawy jakości przetworników niechłodzonych zagościły one w systemach dozoru wizyjnego.

Kamery termowizyjne wykorzystujące przetworniki niechłodzone są stosowane już nie tylko w obiektach wojskowych czy ochronie granic państwa, ale również w rozwiązaniach cywilnych. Kamera termowizyjna, w odróżnieniu od kamer tradycyjnych, rejestruje promieniowanie emitowane przez obiekty, a nie światło odbite. Dzięki temu jest idealnym rozwiązaniem do obserwacji terenów nieoświetlonych, porośniętych roślinnością, która zwykle utrudnia obserwację za pomocą kamer optycznych.
Kamery termowizyjne są dostępne jako modele stałopozycyjne oraz obrotowe. Ofertę Dahua Technology wyróżnia model TPC-PT8620B – kamera 640 x 512 pikseli o zakresie spektralnym 7…14 µm, z przetwornikiem 2 Mpix. Oba moduły zostały wyposażone w obiektywy motozoom o szerokim zakresie ogniskowych. Kamera umożliwia pomiar temperatury, ma zaimplementowaną zaawansowaną analitykę obrazu, w tym detekcję ognia. Standardowa gwarancja obejmująca 42 miesiące jest potwierdzeniem jakości produktów Dahua.
Szybki rozwój technologii, spadek cen oraz rosnąca świadomość możliwości sprawiają, że kamery termowizyjne będą coraz częściej stosowane także w innych dziedzinach.

# Przegląd kamer

## Bosch: DINION IP THERMAL 8000

W miejscach z ograniczoną widocznością spowodowaną słabym oświetleniem, zadymieniem lub ciemnością kamera termowizyjna DINION IP thermal 8000 firmy Bosch sprawdzi się najlepiej. Kamery termowizyjne wychwytują energię cieplną wydzielaną przez nieruchome oraz poruszające się obiekty, a następnie przetwarzają ją na obraz termowizyjny. Działają nawet tam, gdzie naturalne bariery, takie jak liście czy rośliny zasłaniają pole jej widzenia. Kamera może mieć rozdzielczość QVGA lub VGA, zapewniając doskonały poziom szczegółowości danych, które łatwo interpretować.

Konieczność koncentrowania się na niewielkich zmianach w obrazach termowizyjnych może stanowić wyzwanie dla operatorów, zwłaszcza gdy trzeba dokładnie monitorować obrazy z wielu kamer. Wyjątkowość tej kamery polega na połączeniu obrazu termowizyjnego z funkcją inteligentnej analizy obrazu bezpośrednio w urządzeniu. Analiza obrazu umożliwia powiadamianie użytkownika o wszelkich potencjalnych zagrożeniach tuż po ich wystąpieniu. Oprogramowanie Intelligent Video Analytics odróżnia faktyczne zagrożenie od wyuczonych przyczyn błędnych ostrzeżeń, takich jak opady, wiatr (poruszające się gałęzie drzew) czy światło odbijające się od powierzchni wody.
Kamera sprawdza się w zastosowaniach wymagających dozoru z analizą zawartości obrazu na dużych odległościach (do 762 m), umożliwiając wczesne wykrywanie obiektów. Konfigurację funkcji analizy ułatwia wbudowany żyroskop. Dokonuje on pomiarów najważniejszych wartości potrzebnych do automatycznej konfiguracji. Aby ją ukończyć, wystarczy wprowadzić wysokość, na jakiej znajduje się kamera.
Kamera DINION IP thermal 8000 wyróżnia się również wyjątkową odpornością na korozję. Wszystkie wymienione cechy sprawiają, że idealnie nadaje się do najtrudniejszych zadań, takich jak ochrona zewnętrzna lotnisk, kluczowych elementów infrastruktury, budynków rządowych czy mostów. Gwarantuje wczesne wykrywanie przy ograniczonej widoczności spowodowanej słabym oświetleniem, zadymieniem lub ciemnością.

## CBC Poland: GANZ serii GenSTAR


Kamery termowizyjne GANZ z serii GenSTAR stanowią optymalne rozwiązanie do obserwacji terenu zewnętrznego dzięki wykorzystaniu wydajnych mikrobolometrycznych przetworników niechłodzonych IRFPA. Zapewnia to bezawaryjny czas pracy w trybie 24/7, który jest znacznie dłuższy niż w konstrukcji z przetwornikami wymagającymi chłodzenia. Atutem tego rozwiązania jest również szybkość przesyłania obrazu do 30 kl./s przy rozdzielczości D1, co umożliwia obserwację w czasie rzeczywistym. Zgodnie z kryteriami Johnsona opcja rozpoznania obiektu jest dostępna już od 12 pikseli. Wykorzystanie obiektywu 50 mm umożliwia wykrycie pojazdu z odległości nawet 800 m w linii prostej od urządzenia.
Jedną z głównych zalet tej serii kamer jest zastosowanie zintegrowanego modułu detekcji oraz pomiaru temperatury. Zakres pomiaru wynosi od 0 do nawet 200° C, z dokładnością do 0,8°. W opisywanym urządzeniu można zdefiniować maksymalnie 8 niezależnych stref pomiaru temperatury oraz indywidualne progi alarmowe dla każdej, co w połączeniu z dwoma wbudowanymi wyjściami alarmowymi pozwala na wykorzystanie jej jako urządzenia niezależnego od systemu CCTV oraz sprzężenie z systemem alarmowym. Zaletami tej serii są też rozbudowane tryby kolorów, które oprócz podstawowej opcji Black Heat oraz White Heat umożliwiają ustawienie do 17 różnych wizualizacji danych z przetwornika, co pozwoli na dostosowanie kamery do każdego zastosownia.
Kamery serii GenStar są dostępne w pięciu wersjach: z obiektywem 8, 15, 25, 35 oraz 50 mm. Zakres temperatury pracy kamery zawiera się od -10°C do +50°C. Jest wyposażona w przetwornik mikrobolometryczny niechłodzony IRFPA.

# termowizyjnych

## CBC Poland: GANZ GXi termowizja + VCA


Połączenie technologii VCA z termowizją wyznacza nowe standardy skutecznych systemów dozoru wizyjnego. Wysoki odsetek incydentów związanych z bezpieczeństwem zdarza się w warunkach słabego oświetlenia lub ograniczonej widoczności. Dlatego ważne, aby system monitorowania działał skutecznie w dzień i w nocy, a także w różnych warunkach utrudniających widoczność.

Nowa seria inteligentnych kamer termowizyjnych GANZ z funkcją analizy obrazu VCA jest atrakcyjnym i skutecznym rozwiązaniem dozorowym w porównaniu do klasycznych metod współpracy standardowych kamer z pasywnymi czujkami ochrony obwodowej. Kamery zapewniają skuteczną detekcję włamań, wtargnięć potencjalnego intruza do strefy zabronionej niezależnie od warunków widoczności (noc, dym, śnieg, ulewny deszcz, mgła), a dzięki zaimplementowanej analizie VCA są potężnym narzędziem dla operatorów centrum monitoringu gwarantującym skuteczną pomoc w wykrywaniu podejrzanych działań bez generowania fałszywych alarmów. VCA skutecznie wykrywa najmniejszy ruch, analizując metadane związane z ruchem i właściwościami obiektów w treści strumienia wizyjnego. Kamery obsługujące funkcje analityczne oferują też inne usługi, np. zliczanie pojazdów i osób, alarmy oparte na kryteriach prędkości, kontroli temperatury itp.

Kamera termowizyjna serii GXi została wyposażona również w funkcję monitorowania temperatury, którą można skonfigurować do wykrywania anomalii temperaturowych (np. w procesach przemysłowych, logistyce, składach magazynowych), a także wczesnej detekcji zagrożenia pożarem. Określone zakresy temperatury mogą zostać przypisane do czterech niezależnych stref pomiaru w polu widzenia kamery. Wykrycie zmiany temperatury wykraczającej poza zdefiniowany zakres wywołuje akcję alarmową. Kamera jest dostępna w dwóch wersjach: z obiektywem 4 oraz 6,8 mm. Temperatura pracy kamery zawiera się od -40°C do +50°C. Wyposażono ją w przetwornik mikrobolometryczny niechłodzony z tlenku wanadu.

## FLIR: seria FC (dystrybucja Linc Polska)


Modele kamer FLIR FC ze względu na zaawansowane funkcje cieszą się obecnie dużą popularnością. Kamery są dostępne w trzech wersjach: S, R oraz ID. Każda z nich ma zastosowanie w innych projektach:

- **Seria FC-S** – przeznaczona przede wszystkim do ochrony perymetrycznej; zaprojektowana z myślą o pracy w trudnych warunkach, zapewnia niezawodną detekcję i elastyczne opcje alarmowania.
- **Seria FC-R** – radiometryczna, umożliwia jednoczesny monitoring obszaru oraz pomiar temperatury, generuje alarm po przekroczeniu wartości granicznej. Wyposażona w czujnik temperatury skalibrowany do wykrywania pożarów i monitorowania temperatury urządzeń zapewnia bezpieczeństwo ppoż.
- **Seria FC-ID** – kamery z wbudowaną zaawansowaną analityką obrazu, pozwalającą na automatyczne zaklasyfikowanie obiektu (człowiek czy pojazd) i przekazanie sygnału na wyjścia alarmowe. Algorytm AGC firmy FLIR zapewnia doskonałą jakość obrazu w warunkach słabego oświetlenia.

Kamery FC są kompatybilne ze standardem ONVIF, można je zintegrować z innymi systemami VMS lub DVR/NVR. Są wyposażone w wyjście analogowe oraz wyjście IP. Ich obudowa jest odporna na zmienne warunki pogodowe i niskie temperatury. Dzięki zastosowaniu tych kamer można uzyskać bardzo niski współczynnik fałszywych alarmów – wszystko to bez interwencji człowieka.


## Hikvision: DS-2TD4035D-25

**DS-2TD4035D-25** to bispektralna kamera PTZ wyposażona w przetwornik bolometryczny z tlenku wanadu VOx (25 Hz) o rozdzielczości 384 × 288 pikseli oraz optyczny CMOS o rozdzielczości 1920 x 1080 pikseli, generujące płynny obraz 25 kl./s.
Kamerę wyposażono w obiektyw pasma widzialnego z 30-krotnym zoomem optycznym, wspierany przez obiektyw o stałej ogniskowej 25 mm modułu termowizyjnego. Dzięki promiennikowi IR o zasięgu 150 m ta bispektralna kamera PTZ może być stosowana w dowolnym systemie dozoru wizyjnego, począwszy od monitoringu miejskiego, skończywszy na dozorowaniu kompleksów wojskowych.
W kamerze **DS-2TD4035D-25** zaimplementowano zaawansowane funkcje analityki obrazu, takie jak detekcja przekroczenia linii, detekcja intruza, wkroczenie na obszar, opuszczenie obszaru, detekcja temperatury, detekcja pożaru.
Zastosowano również zaawansowane algorytmy śledzenia obiektu (*Panorama Tracking, Event Tracking, Multi-Scenario Patrol Tracking*).
Kamery termowizyjne oferowane przez Hikvision nie podlegają regulacjom ITAR.

## Hikvision: DS-2TD8166-180ZE2F

Pod symbolem **DS-2TD8166-180ZE2F** kryje się bispektralny system pozycjonujący marki Hikvision. Dzięki dwóm sensorom – mikrobolometrycznemu i CMOS 1/1,9" – kamera pozwala uzyskać wysokiej jakości obraz o rozdzielczości full HD oraz obraz termowizyjny o rozdzielczości 640 x 512 pikseli nawet przy 50 kl./s.
W urządzeniu zastosowano dwa obiektywy: zmiennoogniskowy o zoomie 62x (12,5...775 mm) dla pasma widzialnego oraz zoomie 4x (45...180 mm) dla fal z zakresu podczerwieni (promieniowanie cieplne). Zapewniają one wysoką szczegółowość obrazu przy monitorowaniu rozległych obszarów, takich jak lotniska, porty, tereny wojskowe, graniczne itp.
Kamera udostępnia funkcje AGC (automatyczne sterowanie wzmocnieniem), DDE (optymalizacja kontrastu obrazu), 3D DNR (redukcja szumów). Charakteryzuje się wysoką czułością termiczną: NETD <50 mK (dla 25°C, F=1.0).
W kamerze zaimplementowano ponadto funkcje zaawansowanej analityki obrazu, takie jak detekcja przekroczenia linii, detekcja intruza, wkroczenie na obszar, opuszczenie obszaru, detekcja temperatury, detekcja pożaru. Zastosowano w niej także zaawansowane algorytmy śledzenia obiektu (*Panorama Tracking, Event Tracking, Multi-Scenario Patrol Tracking*).
Kamery termowizyjne oferowane przez Hikvision nie podlegają regulacjom ITAR.

## Hikvision: DS-2TD2166-7/15/25/35


Termowizyjna kamera sieciowa typu bullet, model **DS-2TD2166-7/15/25/35**, jest ekonomicznym rozwiązaniem wyróżniającym się znakomitym stosunkiem jakości do ceny. Kamera występuje w wersjach z obiektywem 7, 15, 25 oraz 35 mm, zapewniając doskonałej jakości obraz w rozdzielczości 640 x 512. Zastosowano w niej przetwornik bolometryczny z tlenku VOx (50 Hz), obraz może być generowany nawet z szybkością 50 kl./s.
W kamerze **DS-2TD2166** zaimplementowano funkcje zaawansowanej analityki obrazu, takie jak wykrywanie przekroczenia zdefiniowanej linii i naruszenia strefy chronionej, uruchomienie alarmu po wykryciu nieprawidłowej temperatury czy funkcję wykrywania ognia. Idealnie nadaje się do zastosowania w szeroko pojętej ochronie obwodowej oraz do obserwacji rozległych obszarów. Obudowa ma klasę szczelności IP66.
Kamera spełnia wymogi dotyczące pomiaru temperatury – jest wyposażona w funkcje pomiaru punktowego, liniowego i pełnoklatkowego. Użytkownicy mogą samodzielnie ustawić górną i dolną graniczną wartość. Gdy temperatura przekroczy wyznaczony poziom, zostaje uruchomiony alarm. Kamera może także śledzić rozkład temperatury na obrazie. Pozwala to na interpretację zdarzeń występujących w danym miejscu.
Kamery termowizyjne oferowane przez Hikvision nie podlegają regulacjom ITAR.

## MOBOTIX (dystrybucja Linc Polska)

Firma MOBOTIX jest producentem wysokiej klasy megapikselowych kamer IP.
Do ich zalet należy wysoka jakość zarówno generowanego obrazu, jak i wykonania, odporność na warunki atmosferyczne oraz zintegrowany procesor umożliwiający realizację wielu funkcji, w tym zaawansowaną analitykę w kamerze, powiadamianie czy nagrywanie na karcie pamięci i/lub na serwerze NAS. To nie są jedyne zalety kamer marki MOBOTIX. Dzięki wymiennym modułom przetworników mogą być one również wyposażone w przetwornik termowizyjny – taka konfiguracja znacznie zwiększa ich możliwości. Zaawansowana detekcja działa skuteczniej w kamerach termowizyjnych niż w kamerach tradycyjnych, ponieważ funkcjonowanie kamery nie zależy od natężenia oświetlenia. Co więcej, kamera termowizyjna jest odporna na trudne warunki środowiskowe i atmosferyczne, np. mgłę, deszcz czy pełne słońce. Kamera wyposażona w przetwornik termowizyjny stanowi zaawansowane narzędzie dozorowe w ochronie perymetrycznej oraz zabezpieczaniu infrastruktury krytycznej. Dodatkowo przetworniki termowizyjne w kamerach MOBOTIX mogą mieć funkcje radiometryczne, które umożliwiają dokładny pomiar temperatury, pozwalając na precyzyjne ustawienie punktów pomiarowych. Dzięki tym możliwościom ww. kamery można wykorzystać w wielu projektach. Nowością roku 2017 jest kolejna generacja kamer MOBOTIX – Mx6. Najważniejszą zmianą jest zastosowanie nowego procesora, który zapewnia dwa razy większą liczbę klatek na sekundę i wspiera funkcje analityczne. Dzięki zaimplementowaniu kodeka H.264 i obsłudze standardu ONVIF kamery marki MOBOTIX łatwiej będzie możnazintegrować z systemami firm trzecich.

# NIK o niebezpieczeństwie obiektów infrastruktury krytycznej

**W latach 2015-2016 Najwyższa Izba Kontroli przeprowadziła kontrolę prawidłowości zabezpieczeń obiektów infrastruktury krytycznej (IK) istotnych dla funkcjonowania państwa. Kontrolę przeprowadzono w wybranych podmiotach odpowiedzialnych za ochronę infrastruktury krytycznej, czyli w Rządowym Centrum Bezpieczeństwa, siedzibach trzech wojewodów oraz 15 samorządach szczebli powiatowego i gminnego.**

Na podstawie wyników kontroli NIK wskazała nieprawidłowości ujawnione wśród operatorów infrastruktury krytycznej. Stwierdzono, że:

- nie obejmowano ochroną fizyczną wszystkich obiektów infrastruktury krytycznej powiązanych ze sobą funkcjonalnie i niezbędnych do zapewnienia bezpieczeństwa funkcjonowania infrastruktury krytycznej;
- część terenów, na których znajdowały się obiekty infrastruktury krytycznej, nie była właściwie zabezpieczona przed dostępem osób nieuprawnionych, brakowało również monitoringu wizyjnego;
- wejścia do niektórych obiektów nie spełniały norm bezpieczeństwa i nie zostały objęte systemem kontroli dostępu, bramy wjazdowe nie zostały wyposażone w zapory zabezpieczające przed wtargnięciem;
- w dużej liczbie skontrolowanych podmiotów odpowiedzialnych za ochronę infrastruktury krytycznej nie wprowadzono rozwiązań w razie wystąpienia sabotażu lub wyrządzenia szkód przez pracowników na terenie obiektów infrastruktury krytycznej;
- we wszystkich skontrolowanych podmiotach nie wyodrębniono personelu kluczowego ze względu na przestrzeganie zasad bezpieczeństwa infrastruktury krytycznej;
- w większości podmioty te nie określały procedur umożliwiających sprawdzenie wybranego oferenta wykonującego usługi na rzecz operatora infrastruktury krytycznej pod kątem jakości wykonywanych usług oraz zachowania poufności wykonywanych prac.

Ponadto wystąpiły przypadki nierealizowania przez skontrolowane podmioty niektórych rekomendacji audytu sieci informatycznych działających na potrzeby obiektów infrastruktury krytycznej, nieopracowania kompleksowych regulacji wewnętrznych dotyczących bezpieczeństwa przemysłowego systemu teleinformatycznego czy też niezobowiązywania wykonawców do zachowania poufności uzyskanych informacji, mimo że podczas realizacji zadań mieli dostęp do kluczowych systemów służących do sterowania IK.

Brak odpowiednich zabezpieczeń m.in. w obszarach ochrony fizycznej i osobowej powodował wystąpienie niebezpiecznych incydentów na terenach obiektów infrastruktury krytycznej czy też związanych z prawidłową eksploatacją instalacji infrastruktury krytycznej. Jako przykład podano zaginięcie z obiektów IK dwóch dużych pojemników zawierających izotop promieniotwórczy Co-60. W przypadku ich zniszczenia i wydostania się na zewnątrz źródła izotopowego stanowiłyby poważne zagrożenie życia i zdrowia osób przebywających w pobliżu. Przyczyną tego incydentu był brak nadzoru jednego z operatorów nad pracownikami firmy zewnętrznej wykonującej usługi na terenie obiektu IK.

Kolejnym wydarzeniem było uszkodzenie połączenia transgranicznego – kabla prądu stałego 450 kV łączącego Polskę z jednym z krajów europejskich, strategicznego z punktu widzenia zapewnienia dostaw energii elektrycznej oraz mającego wpływ na bezpieczeństwo energetyczne państwa.

Brak odpowiednich zabezpieczeń m.in. w obszarach ochrony fizycznej i osobowej powodował wystąpienie niebezpiecznych incydentów.

Z kolei brak przygotowania i wdrożenia przez jednego z operatorów IK procedur kontroli transportów z wwożonymi surowcami energetycznymi przed ich wjazdem na teren obiektu IK spowodował skierowanie na przekaźnik taśmowy, wraz z ładunkiem biomasy, niewybuchu pocisku artyleryjskiego.

Niewłaściwe zabezpieczenie jednego z obiektów IK przed wtargnięciem osób trzecich (niskie ogrodzenie, brak monitoringu) było też przyczyną swobodnego przekroczenia ogrodzenia przez osoby nieuprawnione. Brak odpowiednich rozwiązań w zakresie ochrony obiektu umożliwiał w tym przypadku łatwe zatrucie ujęć wody dla setek tysięcy ludzi.

Zastrzeżenia NIK budziła również niewłaściwa realizacja zadań z zakresu ochrony IK przez skontrolowanych wojewodów oraz jednostki samorządu terytorialnego. Stwierdzono wiele przypadków niewywiązywania się przez wojewodów z obowiązku przekazywania organom gmin informacji o znajdującej się na ich terenach infrastrukturze krytycznej. W konsekwencji w trzech objętych kontrolą gminach, w związku z brakiem informacji o lokalizacji na ich terenie obiektów IK, nie podjęto żadnych działań w zakresie ochrony IK określonych w ustawie o zarządzaniu kryzysowym.

Znaczna liczba skontrolowanych starostów (prezydentów) oraz wójtów (burmistrzów) nie wykonywała zadań w zakresie ochrony IK wynikających z ustawy o zarządzaniu kryzysowym. Nie gromadzili oni i nie przetwarzali informacji dotyczących zagrożeń IK, nie opracowywali i nie wdrażali procedur na wypadek wystąpienia takich zagrożeń i rozwiązań w razie zniszczenia lub zakłócenia funkcjonowania IK. Często nie aktualizowano również powiatowych i gminnych planów zarządzania kryzysowego w zakresie dostosowania ich zapisów do wymogów dotyczących ochrony IK określonych w ustawie o zarządzaniu kryzysowym.

NIK zauważyła również, że w badanym okresie nie było ścisłej współpracy starostów (prezydentów) i wójtów (burmistrzów) z operatorami IK w zakresie ochrony IK. O zdarzeniach mogących mieć wpływ na bezpieczeństwo IK starostwa i gminy dowiadywały się głównie ze środków masowego przekazu.

W związku ze stwierdzonymi nieprawidłowościami NIK sformułowała wnioski pokontrolne do skontrolowanych podmiotów odpowiedzialnych za ochronę IK oraz wojewodów i organów z zaleceniem usunięcia stwierdzonych uchybień i realizowania zadań w zakresie ochrony IK zgodnie z przepisami prawa.

**www.nik.gov.pl**

## Czy wiesz że?

**NIK** kontroluje wszystkie urzędy, instytucje i przedsiębiorstwa, w których wydawane są publiczne pieniądze. Izba sprawdza, czy jednostki te wykonują swoje zadania na rzecz obywateli w sposób najbardziej efektywny i oszczędny.

# Zawsze jest pole do doskonalenia

## – mówi **Krzysztof Malesa zastępca dyrektora Rządowego Centrum Bezpieczeństwa**

**Jaką rolę pełni Rządowe Centrum Bezpieczeństwa w systemie ochrony obiektów infrastruktury krytycznej?**
Ochrona infrastruktury krytycznej to pojęcie, które w polskim systemie prawnym pojawiło się wraz z wejściem w życie ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym.
System ochrony IK od podstaw przygotowało Rządowe Centrum Bezpieczeństwa. Zarówno wymogi prawne, jak i dokumenty strategiczne, takie jak Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK), określają wszelkie działania RCB w zakresie koordynacji systemu ochrony infrastruktury krytycznej w Polsce.
Należy jednak pamiętać, że ochrona infrastruktury krytycznej jest obowiązkiem jej właściciela, a RCB na różne sposoby wspiera wszystkich operatorów infrastruktury krytycznej w tych działaniach.
NPOIK w wersji z roku 2013 jako priorytetowe określał podniesienie poziomu świadomości, wiedzy i kompetencji wszystkich uczestników programu w zakresie znaczenia IK dla sprawnego funkcjonowania państwa, a także sposobów jej ochrony. Z zadowoleniem mogę powiedzieć, że te cele w znacznym stopniu udało się zrealizować.
W aktualizacji NPOIK z 2015 r. nakreślono kolejne priorytety – pogłębienie współ-

**Krzysztof Malesa**
**zastępca dyrektora Rządowego Centrum Bezpieczeństwa**

pracy między uczestnikami programu w obszarze ochrony IK, identyfikacja zależności pomiędzy systemami IK, dokonanie oceny ryzyka zakłócenia funkcjonowania systemu IK oraz zainicjowanie skutecznej współpracy między uczestnikami programu.
Trzeba również pamiętać, że wymienione priorytety składają się na cel główny, jakim jest wzrost poziomu bezpieczeństwa IK. Nie obejmują wielu codziennych działań podejmowanych przez RCB. A jest ich bardzo dużo. Jako reprezentatywne wymienię np. system szkoleń operatorów IK i współpracującej z nimi administracji czy pracę nad planami OIK operatorów.

**Jak układa się współpraca z instytucjami odpowiedzialnymi za bezpieczeństwo infrastruktury krytycznej z sektora publicznego, a jak z biznesem?**
Jedną z podstawowych zasad NPOIK jest równość wszystkich operatorów IK. Nawet jeśli w sektorach prywatnym i publicznym mamy do czynienia z innym rodzajem motywacji, to ogólny cel przedstawicieli biznesu i administracji jest zbieżny: wszystkim zależy na poprawie bezpieczeństwa. Oczywiście w każdej organizacji spotykamy zarówno pasjonatów, jak i ludzi mniej zaangażowanych, ale na szczęście pasjonatów nie brakuje po obu stronach.

**Czy przedsiębiorcy, którzy są właścicielami obiektów IK lub nimi zarządzają, mają świadomość szczególnych wymagań dotyczących ochrony? Czy chętnie współpracują z RCB?**
Oczywiście, operatorzy mają tego świadomość. Już pierwszy NPOIK z 2013 r. jako fundamenty systemu ochrony IK określał informowanie i edukację. Po kilku latach pracy widać efekty takiego podejścia. Rządowe Centrum Bezpieczeństwa wprowadziło wiele narzędzi, np. system internetowej wymiany informacji czy spotkania w ramach forum IK. Zakładamy, że po kilku latach kampania informacyjna dotarła już do wszystkich. Operatorów nie trzeba długo namawiać do współpracy, tym bardziej że RCB proponuje wiele użytecznych inicjatyw, m.in. szkolenia czy opracowania dotyczące tego zagadnienia. Trzeba pamiętać, że to przede wszystkim operatorom zależy na zapewnieniu ciągłości działania własnej infrastruktury i zapewne dostrzegają zalety współpracy z RCB.

Należy mieć świadomość, że udany atak na infrastrukturę krytyczną może się wydarzyć w każdym kraju, bez względu na stosowane środki zaradcze...

**Ubiegłoroczny raport NIK na temat bezpieczeństwa infrastruktury krytycznej nie wypadł jednak pomyślnie. Wskazano sporo nieprawidłowości. W jakim obszarze dostrzega Pan największy problem?**
Zawsze jest pole do doskonalenia. Wyniki kontroli w zakresie działań i kompetencji RCB są jednak pozytywne. W swoich opracowaniach pokontrolnych NIK wprost wykazała właściwe podejście RCB do ochrony infrastruktury krytycznej.

**Czy to odpowiedzialni za IK lekceważą kwestie bezpieczeństwa?**
Nie mogę się zgodzić ze stwierdzeniem, że te osoby podchodzą lekceważąco do kwestii bezpieczeństwa. W krótkim kilkuletnim okresie funkcjonowania systemu IK w Polsce widać raczej duże zaangażowanie operatorów zarówno z administracji, jak i prywatnych. Oczywiście kluczowa jest tu motywacja poszczególnych osób. Zdarza się niedbałe traktowanie kwestii ochrony IK – operatorzy podejmują działanie jedynie po to, aby wypełnić wymogi formalne. W takich przypadkach można oczywiście zastosować elementy naprawcze, np. edukacja lub uświadomienie zagrożeń, jakie niesie zaniechanie pewnych działań.

**Jakie wyzwania mógłby Pan wskazać dla RCB w kontekście ochrony infrastruktury krytycznej? Co jest jeszcze do zrobienia?**
Przed nami mnóstwo pracy. Żyjemy w świecie niezwykle dynamicznych zmian. Klasyczny przykład cyklu Deminga (ciągłe doskonalenie przebiegające w czterech następujących po sobie etapach: planowanie, wykonanie, sprawdzenie, poprawienie) dowodzi konieczności ciągłego doskonalenia każdej organizacji i systemu. Myślę, że jednym z większych zadań stojących przed RCB w ramach ochrony infrastruktury krytycznej jest możliwość przejścia, w ramach wyłaniania IK, z systemu obiektowego do procesowego. Oznaczałoby to większy nacisk na ciągłość działania usług dostarczanych przez infrastrukturę krytyczną.

**Ochrona infrastruktury krytycznej jest kosztowna. Czy przewiduje się przeznaczenie na te działania większych środków? Jakie są potrzeby w tym zakresie?**
Mówiliśmy już o świadomości przedsiębiorców dotyczącej szczególnych wymogów ochrony IK. Zarząd spółki, który nowocześnie myśli o ciągłości działania i szeroko pojętym bezpieczeństwie, wie, że inwestycje w bezpieczeństwo nie są wyłącznie kosztem, lecz w dłuższej perspektywie pozwalają uniknąć o wiele większych kosztów usuwania poważnej potencjalnej awarii. Organizacje, które nie poczyniły takich inwestycji, mogą nie przetrwać i w tym też należy upatrywać zysku z inwestycji – przewagi konkurencyjnej. Rolą dobrego menedżera do spraw bezpieczeństwa jest nie tylko przekonanie zarządu, że pewne inwestycje są konieczne, ale też wykonanie rzetelnej analizy ryzyka, która pozwoli uniknąć wydawania pieniędzy na rzeczy niepotrzebne. Jeśli będziemy myśleć takimi kategoriami, koszty skutecznej ochrony IK mogą okazać się niższe, niżby się to wydawało na pierwszy rzut oka

**Coraz poważniejsze stają się zagrożenia cybernetyczne. Jakie działania RCB podejmuje w tym zakresie?**
Rządowe Centrum Bezpieczeństwa jest instytucją, której zadaniem w zakresie zapewnienia bezpieczeństwa infrastruktury krytycznej jest m.in. tworzenie ram w formie zaleceń oraz wymagań technicznych i organizacyjnych, którym podlegają operatorzy IK. Podstawowym dokumentem, który kompleksowo traktuje zagadnienia ochrony IK, jest załącznik nr 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej. Jego obszerną część zajmują wskazówki dotyczące właśnie sposobu zapewniania bezpieczeństwa infrastrukturze teleinformatycznej operatorów IK. Ponadto w zakresie współpracy RCB z konkretnymi sektorami są przygotowywane poradniki, np. w zakresie bezpieczeństwa infrastruktury teleinformatycznej, w tym przede wszystkim związanej z systema-

mi sterowania przemysłowego. W ostatniej fazie uzgodnień są poradniki dla sektora ropy i gazu. Są one przygotowywane we współpracy z przedstawicielami operatorów infrastruktury krytycznej.
Istotnym elementem ochrony infrastruktury krytycznej jest także przekazywanie operatorom informacji uzyskanych od Rządowego Zespołu Reagowania na Incydenty Komputerowe cert.gov.pl (główny zespół CERT w obszarze administracji rządowej, znajdujący się w strukturze ABW), dotyczących podatności w systemach użytkowanych przez operatorów, uwzględniając zarówno systemy tradycyjne IT, jak i systemy sterowania przemysłowego. Rządowe Centrum Bezpieczeństwa ściśle współpracuje również z Ministerstwem Cyfryzacji w zakresie strategii cyberbezpieczeństwa oraz ustawy implementującej dyrektywę NIS.

**Czy według Pana ryzyko ataku (konwencjonalnego lub cybernetycznego) na infrastrukturę krytyczną jest teraz większe? Jak się przed tym ochronić lub przynajmniej ograniczyć je?**
Ataki teleinformatyczne na system elektroenergetyczny Ukrainy w grudniu 2015 r. pokazują, że musimy brać pod uwagę nie tylko szkodliwe działanie pojedynczych osób, które z takiej czy innej przyczyny chcą zaszkodzić infrastrukturze krytycznej, ale również ataki inspirowane przez instytucje rządowe innych państw. Trzeba mieć świadomość, że w zakresie cyberbezpieczeństwa czy też bezpieczeństwa teleinformatycznego broniący się zawsze jest krok za atakującym, a idea stuprocentowego bezpieczeństwa jest nieosiągalna. W takim kontekście należy się zgodzić ze stwierdzeniem, że poziom ryzyka rośnie. Kraje w swoich strategiach coraz śmielej wspominają o możliwości wykorzystania środków teleinformatycznych w celach ofensywnych. Rządowe Centrum Bezpieczeństwa jest tego świadome i uwzględnia uwarunkowania międzynarodowe w swoich działaniach, w miarę ustawowych możliwości.
Należy mieć jednocześnie świadomość, że pomimo wzrastającego zagrożenia ataków na infrastrukturę krytyczną z zewnątrz do najbardziej powszechnych należą ataki nieświadome, czyli takie, które nie są nakierowane na infrastrukturę krytyczną, ale mają na celu znalezienie jakiejkolwiek luki w systemie. Chodzi tu nie tylko o np. oprogramowanie typu *ransomware* (szyfrowanie danych w celu wymuszenia okupu), ale także sieci botnet wykorzystywane w innych przestępstwach. Ataki celowane, takie jak Stuxnet, atak hakerski na instytucje Estonii czy ataki na system elektroenergetyczny Ukrainy są jednostkowe. Działania Rządowego Centrum Bezpieczeństwa w tym zakresie dotyczą odpowiedniego szkolenia pracowników, tworzenia odpowiedniej kultury organizacyjnej bezpieczeństwa teleinformatycznego – mają na celu minimalizację ryzyka materializacji zagrożeń.

> Trzeba mieć świadomość, że w zakresie cyberbezpieczeństwa czy też bezpieczeństwa teleinformatycznego broniący się zawsze jest krok za atakującym, a idea stuprocentowego bezpieczeństwa jest nieosiągalna.

Ostatnim równie istotnym elementem, o którym należy wspomnieć, jest kwestia tzw. *insider threat*, czyli zagrożeń związanych z pracownikami, w szczególności tymi, którzy posiadają wysokie uprawnienia w systemach teleinformatycznych. Przykładem jest szeroko opisywane w literaturze doprowadzenie przez hakerów do awaryjnego wygaszenia pieca hutniczego w Niemczech. Pomimo iż opublikowany w tej sprawie raport BSI pozostawił nieco niedopowiedzeń, było jasne, że źródłem problemów był pracownik huty. W tym zakresie RCB kładzie olbrzymi nacisk na odpowiednie zarządzanie uprawnieniami w systemach operatorów, ale również na dokładne weryfikowanie zatrudnionych przez operatora, zwłaszcza na stanowiska kluczowe. Narzędziami na tym polu są: weryfikacja autentyczności dokumentów, odpowiednie procedury zwalniania pracowników itp.
Należy mieć świadomość, że udany atak na infrastrukturę krytyczną może się wydarzyć w każdym kraju, bez względu na stosowane środki zaradcze, dlatego w naszych działaniach uwzględniamy również zagadnienia zapewnienia ciągłości działania i przywracania infrastruktury do funkcjonowania po niekorzystnym zdarzeniu. Pomimo dużego nakładu pracy Rządowego Centrum Bezpieczeństwa główna odpowiedzialność za funkcjonowanie infrastruktury krytycznej spoczywa jednak na jej operatorze, a RCB wspomaga operatora w tym zadaniu.

**RCB cyklicznie organizuje spotkania Forum Infrastruktury Krytycznej. Kiedy jest planowane kolejne i jakim zagadnieniom zostanie poświęcone?**
W zakresie ochrony infrastruktury krytycznej RCB zaproponowało cykliczne spotkania ujęte wspólną nazwą: Forum. Krajowe forum odbywa się raz do roku, a systemowe i regionalne fora (w każdym województwie) – dwa razy w roku. Krajowe forum zwykle jest organizowane jesienią. Nie chciałbym na razie zdradzać wszystkich szczegółów związanych z tegoroczną tematyką. Na pewno jak co roku będzie wiele bieżących, ważnych tematów z zakresu ochrony infrastruktury krytycznej.

**Dziękuję za rozmowę.**
Rozmawiał **Mariusz Kucharski**

# Zarządzanie ciągłością działania infrastruktury krytycznej

# Aspekty normalizacyjne

Normalizacja międzynarodowa dotycząca infrastruktury krytycznej jest prowadzona przez Komitety Techniczne ISO, głównie przez ISO/TC 292 oraz w mniejszym zakresie przez ISO/TC 262, ISO/TC 251 i ISO/TC 223. **W kraju współpraca z tymi komitetami jest zadaniem PKN i leży w zakresie prac Komitetu Technicznego KT 306 PKN ds. Bezpieczeństwa Powszechnego i Ochrony Ludności.**

**Andrzej Ryczer**
PKN – komisje KT 52, KT 306, KT232 Stowarzyszenie Polalarm, Stowarzyszenie Ekspertów Normalizacji, Walidacji i Certyfikacji NOWACERT

Komitet Techniczny **ISO/TC 292** *Security and resilience* istniejący od 2014 r. opracowuje normy dotyczące • terminologii • systemów zarządzania ciągłością działania • odporności organizacyjnej (*organisational resilience*) • zarządzania awaryjnego (*emergency management*) • odporności społeczności (*community resilience*) • systemów zarządzania bezpieczeństwem łańcucha dostaw (*security management systems for the supply chain*).

W Komitecie Technicznym **ISO/TC 262** *Risc management* (2011) opracowano normy w zakresie podstaw i zasad stosowania technik zarządzania ryzykiem.

Kolejny Komitet Techniczny **ISO/TC 251** *Asset management* (2010) zajmuje się zarządzaniem zasobów, a **ISO/TC 223** *Societal security* (2006) – bezpieczeństwem powszechnym i prowadzi normalizację związaną m.in. z wysokimi konsekwencjami katastrof naturalnych i katastrof spowodowanych przez człowieka. Fundamentalną część IK stanowią sieci łączności, w tym sieci teleinformatyczne; normalizacja dotycząca stosowanych tam technik bezpieczeństwa (*security techniques*) – zarządzania ryzykiem w bezpieczeństwie informacji – jest prowadzona przez wspólny Komitet Techniczny ISO/IEC JTC1.

Liczba norm i specyfikacji technicznych opracowanych przez wymienione komitety wynosi obecnie około 70, z tym że zakresy tych dokumentów ze względu na to, że dotyczą zarządzania, w wielu przypadkach nawzajem się przenikają. Podstawą przedstawianych tam procedur dotyczących zarządzania ciągłością IK jest klasyczne podejście PDCA (*Plan Do Check Act*), zalecane od dawna do stosowania w zarządzaniu jakością.

Ze znacznej liczby norm ISO dotyczących pośrednio albo bezpośrednio zarządzania infrastrukturą krytyczną można wydzielić normy podstawowe dotyczące terminologii, podstaw i zasad stosowania.

**W zakresie terminologii ustanowiono:**
- ISO Guide 73: 2009 *Risk management – Vocabulary*
- ISO/DIS 22300 *Security and resilience – Terminology*
- ISO 22301:2012 *Societal security – Terminology*
- ISO 55000: 2014 *Asset management – Overview, principles and terminology*
- ISO 55001: 2014 *Asset management – Management systems – Requirements.*

**Podstaw zarządzania infrastrukturą krytyczną dotyczą:**
- ISO 22301: 2012 *Societal security – Business continuity management systems – Requirements*
- ISO 22313: 2012 *Societal security – Business continuity management systems – Principles and attributes*
- ISO 22316: *Security and resilience – Organizational resilience – Principles and attributes*
- ISO 28000: 2007 *Specification for security management systems for the supply chain.*

**Zasady stosowania i dobre praktyki objęte są m.in. zakresem:**
- ISO/TS 22317: 2015 *Business continuity management systems – Guidelines for supply chain continuity*
- ISO 22320: 2011 *Security and resilience – Emergency management – Guidelines for incident response*
- ISO 28001: 2007 *Security management systems for the supply chain – Best practices for implementing supply chain security assessments and plans – Requirements and guidance*
- ISO 55002: 2014 *Asset management – management systems – Guidelines for the application of ISO 55001.*

W wymienionych normach i literaturze anglojęzycznej wykorzystuje się wiele pojęć o zbliżonym znaczeniu, np. *resilience, vulnerability, risc, hazard, security, safety, reliability, dependability.* Związki między tymi określeniami są często niejasne.
Na łamach **„a&s Polska"** będziemy prezentować ich definicje, które mogą się znacznie różnić w zależności od kontekstu i obszaru stosowania.

# Dylematy bezpieczeństwa

Edmund Basałyga

W obszarze bezpieczeństwa od początku tego roku odbyło się kilka ciekawych imprez edukacyjnych. Należała do nich m.in. konferencja *Kooperacja służb ratunkowych i sztabów zarządzania kryzysowego*[1], zorganizowana w Warszawie pod auspicjami Polskiego Instytutu Rozwoju Biznesu[2].
Redakcja „a&s Polska" objęła nad nią patronat medialny, doceniając dorobek organizatorów i program konferencji. Treści programowe i solidną ich realizację wpisano w pilne zapotrzebowanie na rzetelną edukację w zakresie bezpieczeństwa.
Warto wspomnieć, że ogólnodostępnych imprez z tego obszaru jest niewiele i są na

## AKTY PRAWNE DOT. ZARZĄDZANIA KRYZYSOWEGO

**Dyrektywa Rady 2008/114/WE z 8.XII.2008** o europejskiej IK (EIK) i potrzebach w zakresie jej ochrony (Dz.Urz. UE L 345/75, 23.12.2008)
– (4) W kwietniu 2007 r. Rada przyjęła konkluzje w sprawie EPOIK (Europejskiego Programu Ochrony IK), podkreślając ostateczną odpowiedzialność państw członkowskich za przygotowania do ochrony IK na ich terytorium, (...) oraz przyjęła starania na rzecz opracowania europejskiej procedury rozpoznawania i wyznaczania EIK (Europejskiej IK) oraz oceny potrzeb jej ochrony.
– (6) Zasadnicza i ostateczna odpowiedzialność za ochronę EIK spoczywa na państwach członkowskich i właścicielach/operatorach tej IK.

**Ustawa z 26.IV.2007 o zarządzaniu kryzysowym** (Dz.U. 2017, poz. 209)
Art. 2 i 3
– zarządzanie kryzysowe (ZK) – działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów IK;
– sytuacja kryzysowa – sytuacja negatywnie wpływająca na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołująca znaczne ograniczenia działań właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków;
– infrastruktura krytyczna (IK) – systemy i wchodzące w ich skład funkcjonalnie powiązane ze sobą obiekty (...) kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej oraz instytucji i przedsiębiorców (...).
Art. 5.1. Tworzy się krajowy oraz wojewódzkie/powiatowe/gminne „plany zarządzania kryzysowego".
Art. 5b. 1. RM przyjmuje uchwałą Narodowy Program Ochrony IK, którego celem jest stworzenie warunków do poprawy bezpieczeństwa IK (...).
5. Program podlega aktualizacji nie rzadziej niż raz na dwa lata (...).
Art.14.1. Organem właściwym w sprawach ZK na terenie województwa jest wojewoda (...).
Art.17.1. Organem właściwym w sprawach ZK na obszarze powiatu jest starosta (...).
Art. 19.1. Organem właściwym w sprawach ZK na terenie gminy jest wójt, burmistrz, prezydent miasta (...).

**Akty wykonawcze:**
Rozporządzenie RM z 30.IV.2010 – Narodowy Program Ochrony IK (Dz.U. 83/2010, poz. 541),
Rozporządzenie RM z 30.IV.2010 – plany ochrony IK (Dz.U. 83/2010, poz. 542).

**Ustawa z 10.VI.2016 o działaniach antyterrorystycznych** (Dz.U. 2016, poz. 904)
Art. 2.
– działania antyterrorystyczne – działania organów administracji publicznej polegające na zapobieganiu zdarzeniom o charakterze terrorystycznym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych przedsięwzięć, reagowaniu w przypadku wystąpienia takich zdarzeń oraz usuwaniu ich skutków, w tym odtwarzaniu zasobów przeznaczonych do reagowania na nie;
– zdarzenie o charakterze terrorystycznym – sytuacja, co do której istnieje podejrzenie powstania na skutek przestępstwa o charakterze terrorystycznym z art. 115 § 20 KK, lub zagrożenie zaistnienia takiego przestępstwa (...).

Rozporządzenie RM z 24.VI.2003 – obiekty szczególnie ważne dla bezpieczeństwa i obronności (Dz.U. 116/2003, poz. 1090)

**Kodeks karny** art. 115 § 20
Przestępstwem o charakterze terrorystycznym jest czyn zabroniony, zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu:
1) poważnego zastraszenia wielu osób,
2) zmuszenia organu władzy RP/innego państwa/organu organizacji międzynarodowej do podjęcia/zaniechania określonych czynności,
3) wywołania poważnych zakłóceń w ustroju/gospodarce RP/innego państwa/organizacji międzynarodowej i groźba popełnienia tego czynu.
W kodeksie nie występuje przestępstwo określane mianem „terroryzm", dlatego do czynu „o charakterze terrorystycznym" stosuje się art. 64 § 2.

[1] http://multiexpo.pl/konferencje-2017/31-01-2017-kooperacja-sluzb-ratunkowych-i-sztabow-zarzadzania-kryzysowego
[2] www.polib.pl

ogół płatne. Systemowej edukacji społecznej w tym obszarze prawie w ogóle brak, rośnie natomiast masowa wręcz produkcja aktów prawnych, i to coraz niższej jakości merytorycznej.
O wartości merytorycznej konferencji świadczy zakres wspomnianego pakietu programowego, z uwzględnieniem zagrożeń terrorystycznych. Oprócz tematów podstawowych dotyczących zarządzania kryzysowego prelegenci poruszyli następujące kwestie:

- rola mediów w przekazach sytuacji kryzysowych i ich wiarygodność (prof. St. Mocek, rektor Collegium Civitas),
- uwarunkowania prawne zagrożeń terrorystycznych (płk J. Mąka),
- zagrożenia terroryzmem w Polsce oraz profilaktyka i przeciwdziałania (R.J. Korsak),
- propozycje nowoczesnej techniki w ZK i bezpośrednich akcjach (dwie firmy specjalistyczne),
- zastosowania systemów bezpieczeństwa w infrastrukturze krytycznej metra i lotniska (specjaliści ZK).

Szczególne zainteresowanie wzbudziły trzy problemy, pozornie odległe od tematyki zarządzania kryzysowego:

– przekaz medialny a zagrożenia i bezpieczeństwo (prof. St. Mocek),
– prawne relacje obywatel – państwo (J. Mąka),
– profilaktyka i procedury w zagrożeniach terrorystycznych (R.J. Korsak).

Prof. St. Mocek przedstawił m.in. ciekawą tezę udziału mediów w „przemyśle strachu", generującym w świadomości społecznej tzw. przeszacowane ryzyko. Zakończył prostymi, ale bardzo istotnymi dla bezpieczeństwa pytaniami, na ile wiarygodny jest obraz sytuacji kryzysowej w mediach, czy można na nim opierać działania podmiotów odpowiedzialnych za bezpieczeństwo i ZK.

J. Mąka uzmysłowił mało znane aspekty prawne relacji państwo – obywatel, ujęte w kilka punktów:

- kodeksowy obowiązek denuncjacji (art. 240 kk),
- konstytucyjne gwarancje praw i wolności obywatelskich,
- obywatel: podmiot czy przedmiot współczesnej wojny informacyjnej,
- ustawa o ochronie prywatności – idea limitacji aktywności państwa w sferze bezpieczeństwa.

R.J. Korsak skupił się na profilaktyce antyterrorystycznej – od powszechnych szkoleń świadomościowo-obronnych, poprzez różne działania aktywne (procedury bezpieczeństwa, programy szkoleń pracowników ochrony, zmiany w zakresie bezpieczeństwa imprez masowych i obiektów szczególnych itd.), po kontrowersyjne problemy świadomej akceptacji ograniczeń praw człowieka i swobód obywatelskich.

Prelegenci – specjaliści wykazali profesjonalizm zawodowy i dydaktyczny. Ich prezentacje stanowiły skuteczną platformę dyskusji – zawsze żywych, merytorycznych, czasem burzliwych. W pełnym skupieniu i zupełnej ciszy obejrzano oryginalny, mocny film propagandowy ISIS[3] dostępny w prezentacji J. Mąki (komplet prezentacji jest dostępny na portalu organizatora[4]). Nie wspomniano natomiast o systemowej łączności zarządzania kryzysowego, a właściwie jej braku. Problem bardzo stary i nadal poważny – ciągle stanowi newralgiczny element systemu bezpieczeństwa powszechnego. Łączność ZK to „bazar" rozwiązań organizacyjnych, technicznych i innych.

W Polsce w zasadzie nie ma ani systemowej edukacji bezpieczeństwa, ani prób tworzenia takowej. Łatwiej produkować masową administracyjną makulaturę kulawych przepisów, w większości nieznanych Polakom. W administracyjnym dokumencie Narodowy Program Antyterrorystyczny 2015-2019 napisano: jednym z filarów systemu antyterrorystycznego jest polityka informacyjna i edukacyjna, za co odpowiada Minister Spraw Wewnętrznych i Administracji. Tylko ilu obywateli RP czytało ten dokument?
Potrzebę edukacji społecznej, nie tylko w zakresie bezpieczeństwa, potwierdza też część organów państwowych,

[3] https://videopress.com/v/mjRqgqAP
[4] http://multiexpo.pl

Znaczenie i złożoność zarządzania kryzysowego wymusza pilną potrzebę edukacji społecznej. Nie tylko w tym zakresie – bezpieczeństwo to obszar praktycznie bez granic.

m.in. Rzecznik Praw Obywatelskich i Najwyższa Izby Kontroli. RPO skierował w sierpniu ub.r. swoje uwagi do MSWiA w sprawie kontrowersyjnego projektu ustawy antyterrorystycznej. Wskazał m.in.:

- edukacja obywateli powinna polegać na przekazywaniu informacji jak najszerszemu kręgowi osób, a nie tylko na umieszczaniu ich na stronie internetowej,
- poradnik internetowy MSWiA *Terroryzm – co zrobić w sytuacji zagrożenia* częściowo tylko realizuje powierzone ministrowi zadanie.

Najwyższa Izba Kontroli z urzędu interesuje się problemami dotyczącymi obszaru bezpieczeństwa i przeprowadza pod tym kątem kontrole. Oto niektóre z nich.

## Kontrola bezpieczeństwa obiektów IK

Kontrolowano RCB, trzech wojewodów i 15 samorządów powiatów i gmin. Wnioski:

– brak ochrony fizycznej części obiektów IK powiązanych funkcjonalnie i niezbędnych do bezpieczeństwa funkcjonowania,
– ze strzeżonego obiektu specjalnego zginęły dwa duże pojemników zawierające izotop promieniotwórczy Co-60,
– uszkodzenie transgranicznego kabla prądu stałego 450 kV, łączącego Polskę z krajem europejskim,
– zaniechania wojewodów, przedstawicieli samorządów terytorialnych i operatorów IK w postaci braku stałych kontaktów służbowych i współpracy,
– w trzech kontrolowanych gminach z powodu niewiedzy o obiektach IK na ich terenie nie podjęto żadnych działań w zakresie ich ochrony,
– większość kontrolowanych podmiotów nie posiada procedur wyboru i sprawdzania oferentów usług.

## Kontrola organów administracji publicznej w zakresie ZK

Kontrolą objęto 91 jednostek - MSWiA, RCB, 16 UW, 17 starostw powiatowych, 49 UM i gmin, pięć komend PSP i straż miejską. NIK pozytywnie oceniła tylko 15% kontrolowanych jednostek.

## Kontrola bezpieczeństwa systemów teleinformatycznych i przechowywanych danych

W 2015 r. kontrola ochrony cyberprzestrzeni RP wykazała „brak przygotowania państwa do walki z zagrożeniami w cyberprzestrzeni".

## Kontrola ochrony cyberprzestrzeni RP

Skontrolowano osiem podmiotów państwowych związanych z bezpieczeństwem teleinformatycznym: Ministerstwa Administracji i Cyfryzacji, MON i MSW oraz ABW, RCB, KG Policji, Naukową Sieć Komputerową i Urząd Komunikacji Elektronicznej.

Negatywnie oceniono realizację zadań tych podmiotów w zakresie ochrony cyberprzestrzeni RP. Stwierdzono, że *nie podjęto działań w celu zapewnienia bezpieczeństwa teleinformatycznego Polski. Mimo że coraz więcej usług publicznych i innych aspektów życia jest realizowanych w internecie lub systemach teleinformatycznych, bezpieczeństwo Polski nadal jest postrzegane konwencjonalnie: zapobieganie i reagowanie na zagrożenia tradycyjne (powodzie, pożary, terror fizyczny, tradycyjne konflikty zbrojne itd.) [...] negatywny wpływ na realizację zadań w tym obszarze miało m.in. niewystarczające zaangażowanie najwyższego kierownictwa administracji rządowej. Przykładowo w latach 2008–2011 opracowano kolejno siedem niezatwierdzonych projektów narodowej strategii bezpieczeństwa cyberprzestrzeni [...].*

Z kolei w załączniku *Synteza wyników kontroli* napisano:
*RM i kierownictwo administracji państwowej nie opracowały narodowej strategii ochrony cyberprzestrzeni Polski, mogącej być podstawą konkretnych, systemowych działań podnoszenia poziomu bezpieczeństwa teleinformatycznego. Prace nad strategią prowadzono od 2008 r., ale ze względu na ich nierzetelne przygotowanie i sprzeczne interesy instytucji biorących w nich udział kolejne wersje nie były zatwierdzone. Dopiero w czerwcu 2013 r. RM przyjęła Politykę Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej – wynik braku porozumienia i źle rozumianego kompromisu, o niskiej jakości, nieprecyzyjny, obarczony wieloma błędami merytorycznymi. Nieliczne zadania w niej zawarte nie były realizowane przez większość kontrolowanych podmiotów, co pozwala twierdzić, że jej praktyczne zastosowanie dla poprawy bezpieczeństwa teleinformatycznego było symboliczne.*
Ciekawych materiałów pokontrolnych nt. bezpieczeństwa jest sporo i zmuszają do określonych refleksji. Warto zajrzeć na www.nik.gov.pl/dla-dziennikarzy.

BIO

**Edmund Basałyga**
Doświadczony praktyk branży ochrony, wieloletni wykładowca oraz publicysta tematyki bezpieczeństwa czasopism specjalistycznych. Rzeczoznawca Polskiej Izby Ochrony.

# Infrastruktura krytyczna w świetle obecnych wyzwań

**Należy zwrócić uwagę na dwa wyzwania, które dotyczą infrastruktury krytycznej, a w mojej ocenie są niewystarczająco dostrzegane.** Co więcej, odnoszą się one pośrednio lub bezpośrednio do innych dużych lub zaawansowanych technologicznie obiektów, których struktura lub poziom złożoności wpływają na podwyższenie ich ryzyka zagrożeń.

**Witold Strzelecki**
prezes Stowarzyszenia POLALARM

*Infrastruktura krytyczna to rzeczywiste i cybernetyczne systemy (obiekty, urządzenia, instalacje) niezbędne do minimalnego funkcjonowania gospodarki i państwa*[1] – taką definicją posługuje się Rządowe Centrum Bezpieczeństwa (RBC). W skład infrastruktury krytycznej wchodzą systemy zaopatrzenia w energię, surowce energetyczne i paliwa, zaopatrzenia w żywność i wodę, systemy łączności, sieci teleinformatycznych, finansowe, ochrony zdrowia, transportowe, ratownicze oraz produkcji, składowania, przechowywania oraz stosowania substancji chemicznych i promieniotwórczych. Definicja w takim lub nieco zmodyfikowanym brzmieniu jest przytaczana przez większość osób zajmujących się infrastrukturą krytyczną (IK).

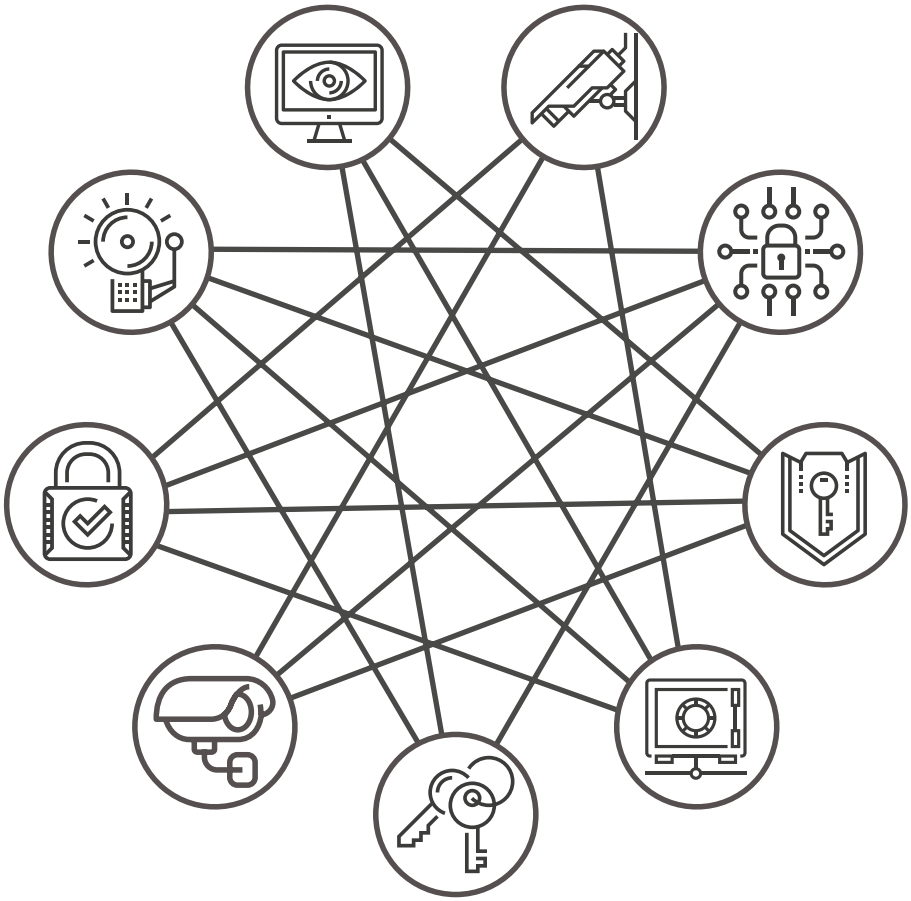
Ochrona infrastruktury krytycznej – cytując RCB – polega na ochronie fizycznej, technicznej, osobowej, teleinformatycznej i prawnej oraz na tworzeniu i wykorzystywaniu planów odtwarzania. Nie sposób nie zgodzić się z taką klasyfikacją RCB. Natomiast zagrożenia IK przez jedne źródła są klasyfikowane jako zagrożenia naturalne (powodzie, susze, inne anomalie pogodowe itp.), zagrożenia techniczne (awarie chemiczne, katastrofy komunikacyjne, katastrofy budowlane itp.), terroryzm oraz pozostałe (proliferacja broni masowego rażenia, lawinowo rosnąca skala migracji, niepokoje społeczne, przestępczość zorganizowana, cyberprzestępczość).
Inni specjaliści tematu podają prostszy podział – zagrożenia IK dzielą na celowe (stanowiące celowe działanie człowieka) oraz niezamierzone (błędy konstrukcyjne lub powodowane niewłaściwą eksploatacją urządzeń i instalacji).
Wskazane zagrożenia są realne, wymagają ciągłego monitorowania i przeciwdziałania. Zachodzące w Europie i na świecie zmiany społeczno-polityczne powodują, że poszczególne typy zagrożeń okresowo aktywują się, skupiając zainteresowanie społeczeństw i reakcję służb odpowiedzialnych za przeciwdziałanie im. Sytuacja, w której dany typ zagrożenia okresowo jest niedolegliwy, nie jest sytuacją stałą, niewymagającą jego monitoro-

[1] http://rcb.gov.pl/infrastruktura-krytyczna/

wania. Doświadczenie uczy, że okresowa cisza często świadczy o utajonej modyfikacji sposobów lub form działania, a nie o zaniku takiego lub innego zagrożenia. Z tego względu monitorowanie zagrożeń i analiza zmian charakterystyki ich powstawania oraz przebiegu jest procesem niezbędnym i ciągłym.

Należy zwrócić uwagę na dwa rodzaje zagrożeń, które niezbyt często pojawiają się w analizach ekspertów w tej dziedzinie, co może wskazywać na ich niedostrzeganie lub lekceważenie. Mają one charakter globalny i są związane z lawinowym postępem technologicznym.
Większość specjalistów zajmujących się zabezpieczeniami technicznymi jeszcze do niedawna dzieliła systemy służące wykryciu i zapobieganiu sytuacjom niepożądanym na systemy włamania i napadu, dozoru wizyjnego oraz kontroli dostępu. Podobnie postrzegali je użytkownicy czy zarządzający chronionymi obiektami. Tak określone pozwalały na realizację zasad zabezpieczania, czyli przede wszystkim na ograniczenie fizycznego dostępu do obiektów osobom do tego nieuprawnionym. Umożliwiały też detekcję wtargnięcia intruzów oraz obserwowanie obiektu lub instalacji i ujawnienie działań skierowanych przeciw bezpieczeństwu osób lub mienia. Detektory każdego z tych systemów wysyłały określone informacje do central alarmowych czy stacji zarządzających, a za ich pośrednictwem do centrum monitorowania zdarzeń. Oprócz informacji o zdarzeniu alarmowym sygnalizowały m.in. załączenie, rozłączenie, awarię, sabotaż itp. Systemy telewizji dozorowej przesyłały także informacje odpowiadające zdarzeniom obserwowanym przez kamerę.

Istotnym zagrożeniem dla bezpieczeństwa infrastruktury krytycznej jest – charakterystyczne i często niestety spotykane w Polsce – lekceważenie istniejących uregulowań formalnoprawnych.



W sytuacji modelowej dane te były analizowane przez operatora systemu. Wnioski z zaobserwowanych zdarzeń przekładały się na jego reakcję, skutkując interwencją mającą na celu przeciwdziałanie zaistniałej sytuacji niepożądanej.
Warto wspomnieć, iż jest to model nadzoru systemów zabezpieczenia przez operatora, a nie wymóg takiego rozwiązania. Bywa, że wszystkie alarmy pochodzące z systemów alarmowych są jedynie rejestrowane i analizowane dopiero po wystąpieniu zdarzenia. Takie rozwiązanie, choć błędne, może być czasem zastosowane. Percepcja operatora umożliwia obserwowanie ograniczonej liczby systemów. Problemem są m.in. różnice technologiczne zainstalowanych systemów, z których każdy może pochodzić od innego producenta i zwykle musi być obsługiwany w inny sposób. Kolejnym problemem jest ilość informacji niewskazujących na rzeczywisty alarm, a jedynie ujawniających błędne działanie systemu, czyli tzw. fałszywe alarmy. Takie informacje operator powinien „odsiać", notując ich wystąpienie, ale nie inicjując reakcji na zdarzenie, które nie zaistniało.
Podsumowując, należy przyznać, iż model takiego zorganizowania systemów zabezpieczenia technicznego sprawdzał się przez lata, zwłaszcza że ceny systemów służących zabezpieczeniu technicznemu obiektów powodowały, iż liczba detektorów w każdym systemie była ograniczana, zaś w przypadku dużych obiektów zwykle można było zwiększyć liczbę operatorów.
Obecnie obserwuje się pewne zmiany. Ceny systemów są relatywnie niższe. Tańsze są też elementy detekcyjne. Ponadto pojawiające się informacje o wystąpieniu indywidualnych zdarzeń o charakterze terrorystycznym czy kryminalnym powodują, że świadomość istnienia zagrożeń wśród osób odpowiedzialnych za bezpieczeństwo obiektów stopniowo wzrasta. Coraz częściej w obiektach, zwłaszcza stanowiących elementy infrastruktury

krytycznej, działają systemy, które nadzorują znacznie więcej typów potencjalnych niepożądanych zdarzeń, m.in. systemy radarowe, systemy śledzenia geograficznej lokalizacji pojazdów lub osób, systemy sonarowe, rozbudowane systemy RFID, radary pogodowe, systemy śledzenia bezzałogowych statków powietrznych i inne. W coraz większej liczbie obiektów do ogromnej ilości informacji wpływających na poziom bezpieczeństwa dochodzą ewentualne alarmy z urządzeń technologicznych lub wskazania stanów ich działania.

Należy też wspomnieć o jeszcze jednym zjawisku. Po raz pierwszy zdefiniował je w 1999 r. Kevin Ashton. Nosi ono nazwę Internet Rzeczy (IoT – *Internet of Things*). *To koncepcja, według której jednoznacznie identyfikowalne przedmioty mogą pośrednio albo bezpośrednio gromadzić, przetwarzać lub wymieniać dane za pośrednictwem instalacji elektrycznej inteligentnej KNX lub sieci komputerowej*[2]. Gdy je definiowano, było zjawiskiem w znacznej części teoretycznym. Zgodnie ze stanowiskiem Cisco Internet Business Solutions Group (Cisco IBSG) o IoT można mówić wtedy, gdy liczba rzeczy i obiektów podłączonych do internetu przekroczyła liczbę ludności[3], co nastąpiło w 2009 r. Nie jest niczym zaskakującym, że IoT ma przełożenie na systemy zabezpieczenia technicznego obiektów, zwłaszcza złożonych technologicznie, ważnych, wyposażonych w wiele systemów zabezpieczenia, jakimi są obiekty infrastruktury krytycznej państwa.

Różnorodność i wielość systemów zabezpieczeń technicznych, a także wykorzystywanie w nich elementów działających zgodnie z IoT powoduje zalew informacji napływających do stanowiska operatora. Czy jest on w stanie prawidłowo zinterpretować ogromne ilości informacji? Niestety część istotnych danych z różnych systemów pozostanie niedostrzeżona w masie innych. Możliwości percepcji człowieka nie są nieograniczone i nawet dobre wyszkolenie może tę sytuację poprawić w ograniczonym zakresie.

Lekceważenie zidentyfikowanych zagrożeń czy zdefiniowanych zaleceń postępowania mających na celu zachowanie bezpieczeństwa obiektów i instalacji jest – oprócz nieprzestrzegania przepisów – objawem braku wyobraźni osób decyzyjnych odpowiedzialnych za bezpieczeństwo.

Kolejne zagadnienie, mające bezpośredni wpływ na bezpieczeństwo obiektów, wiąże się z potencjalnymi niepokojami społeczności lokalnych lub społeczności reprezentujących skrajne przekonania, np. proekologiczne, skierowane bezpośrednio przeciwko konkretnym obiektom. Choć oczywiście istnieje oprogramowanie pozwalające monitorować potencjalne pojawienie się tego typu zagrożeń, należy zadać pytania, czy operator systemu jest w nie wyposażony, czy potrafi i ma czas z nich korzystać, czy umie właściwie zinterpretować informacje pozyskane w wyniku ich zastosowania.

Odpowiedzią na nowe wyzwania są zintegrowane platformy do zarządzania systemami zabezpieczeń obiektów i instalacji: PSIM (*Physical Security Information Management*) czy nawet CSIM (*Converged Security and Information Management*). Szczególnie systemy CSIM pozwalają gromadzić wiele informacji z różnych systemów, nie tylko alarmowych. Zapewniają korelację zdarzeń, z uwzględnieniem czasu ich wystąpienia, rodzaju czujki i jej lokalizacji czy wagi alarmu. Pozwalają logicznie łączyć kilka lub kilkanaście alarmów wskazujących na wystąpienie zdarzenia, a także włączać do procesu preselekcji alarmów informacje z systemów analizy wizyjnej. Dopiero taka wstępnie automatycznie obrobiona informacja wraz z instrukcją dotyczącą adekwatnego sposobu reakcji na zaistnienie niepożądanego zdarzenia jest przekazywana operatorowi systemu.

Innym, rzadko akcentowanym wyzwaniem, które zasługuje na potraktowanie jako istotne zagrożenie bezpieczeństwa infrastruktury krytycznej, jest – charakterystyczne szczególnie w Polsce i często niestety spotykane – lekceważenie istniejących uregulowań formalnoprawnych. Na stronach NIK pojawiła się informacja o kontroli obiektów infrastruktury krytycznej pod kątem prawidłowości ich zabezpieczenia. Skontrolowano wybrane podmioty odpowiedzialne za ochronę IK, a także samorządy powiatowe i gminne[4]. W raporcie NIK wskazała wiele nieprawidłowości. (Piszemy również na ten temat na str. 44-45). Wynik kontroli NIK pokazał i uwypuklił brak odpowiedzialności i nonszalancję wielu decydentów odpowiedzialnych za bezpieczeństwo obiektów i instalacji. „Skoro dotychczas nic złego się nie wydarzyło, to i w przyszłości na pewno nic złego się nie przytrafi" – to pogląd z gruntu błędny. Wydarzenia w Europie i na świecie, zwłaszcza akty terroru, pokazują, że poczucie bezpieczeństwa nie jest stanem stałym. To proces, nad którym trzeba nieprzerwanie pracować. Wymaga od osób za nie odpowiedzialnych dużej wyobraźni.

**Lekceważenie zidentyfikowanych zagrożeń czy zdefiniowanych zaleceń postępowania mających na celu zachowanie bezpieczeństwa obiektów i instalacji jest – oprócz nieprzestrzegania przepisów – objawem braku wyobraźni osób decyzyjnych odpowiedzialnych za bezpieczeństwo. Wyzwania, które nie znajdują adekwatnej reakcji czy to ze względu na brak wiedzy o zagrożeniach, czy z uwagi na ich lekceważenie, przekształcają się w groźne incydenty.**

[2] *Internet Rzeczy to pięta achillesowa Polski*, http://biznes.interia.pl
[3] D. Evans, The Internet of Things – How the Next Evolution of the Internet Is Changing Everything, CISCO Internet Business Solutions Group (IBSG) White Paper, 4.2011, s. 2; za artykułem Ewy M. Kwiatkowskiej w internetowym „Kwartalniku Antymonopolowym i Regulacyjnym", 2014, nr 8(3)
[4] https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-obiektow-infrastruktury-krytycznej.html

**Coraz więcej mówi się o bezpieczeństwie infrastruktury krytycznej. To dobry symptom,** bo choć odgrywa ona kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli, to w wielu przypadkach poziomjej ochrony jest daleki od założeń.

# Wyzwania dla bezpieczeństwa infrastruktury krytycznej

**Sergiusz Parszowski**

Po upływie niespełna dziesięciu lat od wejścia w życie ustawy o zarządzaniu kryzysowym trudno wprawdzie oczekiwać pełnej dojrzałości systemu, ale okres wczesnego dzieciństwa ma on już za sobą. Jakie zatem wyzwania dla bezpieczeństwa infrastruktury krytycznej można wskazać na najbliższe lata?

## Żyjemy w erze współzależności

To jedno z podstawowych i zarazem głównych wyzwań dla bezpieczeństwa infrastruktury krytycznej. I chociaż jest ono dość ogólne, to w praktyce pociąga daleko idące konsekwencje. Jeszcze niedawno o współzależności mówiono głównie w kontekście rynków finansowych i ich międzynarodowych powiązań. Obecnie coraz większego znaczenia nabierają współzależności infrastrukturalne oraz uzależnienie nieprzerwanego działania poszczególnych systemów

od pracy innych. W rzeczywistości jest to właśnie jedno z podstawowych kryteriów odróżniających infrastrukturę krytyczną od infrastruktury niemającej aż takiego znaczenia. Współzależności zwiększają potencjalne skutki przyszłych incydentów, a także utrudniają przywrócenie normalnego funkcjonowania systemów i realizacji usług.
Jako przykłady zdarzeń potwierdzających głęboką współzależność kluczowej infrastruktury mogą posłużyć przypadki awarii w systemie elektroenergetycznym, jaka miała miejsce w Szczecinie w 2008 r. (nie działała większość usług powszechnych), oraz pożar mostu Łazienkowskiego w Warszawie w 2015 r. (następstwem było także odcięcie komunikacji telefonicznej Urzędu Miejskiego w Białymstoku). Wymienione przykłady świadczą o tym, jak ważne jest odpowiednie zidentyfikowanie współzależności występujących pomiędzy systemami oraz prawidłowe określenie priorytetów w zakresie odtwarzania infrastruktury krytycznej.

## Wzmocnienie układu immunologicznego

Wyzwaniem jest również rozwój i wzmocnienie mechanizmów odpornościowych. Nie chodzi tylko o to, by za wszelką cenę zapobiegać zagrożeniom, wszak coraz częściej jest to niemożliwe. W takich sytuacjach ważne jest budowanie właściwej odporności, zapewnienie organizacji lub infrastrukturze zdolności przetrwania nawet w niesprzyjających warunkach. Jeżeli nie jesteśmy w stanie czemuś zapobiec, musimy się na to odpowiednio przygotować. Jednym z pozytywnych przykładów działań w tym kierunku jest budowa odporności miast (tzw. *urban resilience*) polegająca na adaptacji przestrzeni i infrastruktury miejskiej do zmian klimatu.
Według raportu Europejskiej Agencji Środowiska (EEA) *Urban adaptation to climate change in Europe 2016. Transforming cities in a changing climate* wyróżnia się trzy sposoby adaptacji do zmian klimatycznych: stawianie czoła (*coping*), stopniową adaptację (*incremental adaptation*) oraz adaptację przez transformację (*transformational adaptation*). W pierwszym przypadku (*coping*) podejmowane działania ograniczają się do reagowania na skutki zagrożeń po ich wystąpieniu,

> Znaczna część infrastruktury krytycznej jest własnością podmiotów prywatnych. Zapewnienie jej bezpieczeństwa nie jest zatem możliwe bez ścisłej współpracy administracji publicznej ze środowiskiem biznesowym.

w drugim przypadku (*incremental adaptation*) korzystamy głównie z tradycyjnych rozwiązań stanowiących przede wszystkim fizyczną barierę ochronną (ogrodzenia, wały, izolacja), natomiast w przypadku adaptacji poprzez transformację (*transformational adaptation*) staramy się eliminować źródła wrażliwości (np. rozwiązaniem na porywiste wiatry będzie rezygnacja z budowy linii napowietrznych).

## Właściwa identyfikacja zagrożeń

Od tego wszystko się zaczyna. Jakiekolwiek działania ukierunkowane na poprawę bezpieczeństwa i zapewnienie ciągłości działania infrastruktury krytycznej muszą zostać poprzedzone rzetelną oceną ryzyka. Jeżeli chcemy czemuś zapobiegać, musimy wiedzieć dokładnie, przed czym należy się bronić. Co więcej, zidentyfikowane zagrożenia trzeba odpowiednio zhierarchizować. Czy zajmowanie się określonym zagrożeniem tylko dlatego, że jest w danym momencie na topie i poświęca się mu większość publikacji oraz wydarzeń branżowych, jest uzasadnione? Czy zagrożenie terrorystyczne lub cyberbezpieczeństwo to zagadnienia, którym powinniśmy poświęcić większość czasu i zaangażowania?
Wiele organizacji na co dzień boryka się z bardziej prozaicznymi problemami, takimi jak dewastacje i kradzieże elementów infrastruktury technicznej czy też przypadki nieprzestrzegania obowiązujących zasad i procedur przez personel wykonawczy. Niska kultura bezpieczeństwa już wielokrotnie była przyczyną zatrzymania procesów technologicznych oraz przerwania dostaw lub świadczenia usług.
Właściwa identyfikacja i pomiar zagrożeń dla określonych systemów (obiektów, urządzeń, instalacji) nie jest zadaniem łatwym i wymaga zaangażowania wielu niezależnych podmiotów. Sprawę komplikuje fakt, że poszczególni operatorzy infrastruktury krytycznej, a także organy administracji publicznej stosują różne metodyki oceny zagrożeń, co stanowi dodatkowe ograniczenie.

## Współpraca na linii państwo – biznes

Znaczna część infrastruktury krytycznej jest własnością podmiotów prywatnych. Zapewnienie jej bezpieczeństwa nie jest zatem możliwe bez ścisłej współpracy administracji publicznej ze środowiskiem biznesowym. Nałożony na właścicieli infrastruktury krytycznej obowiązek zapewnienia jej odpowiedniej ochrony jest jak najbardziej słuszny, lecz nie można zapominać, że to przede wszystkim państwo dysponuje aparatem oraz instrumentarium pozwalającym skutecznie przeciwdziałać niektórym zagrożeniom.
Najwyższa Izba Kontroli przeprowadziła w latach 2015–2016 kontrolę, w której wykazała brak ścisłej współpracy wójtów (burmistrzów) i starostów (prezydentów) z operatorami infrastruktury krytycznej. W niektórych przypadkach gminy w ogóle nie wiedziały o lokalizacji na ich terenie obiektów IK lub posiadały taką wiedzę jedynie ze źródeł nieoficjalnych. W konsekwencji część skontrolowanych jednostek samorządu terytorialnego nie wywiązywała się z obowiązków w obszarze ochrony infrastruktury krytycznej, a wynikających z ustawy o zarządzaniu kryzysowym. Według ustaleń kontrolerów nie gromadzono i nie przetwarzano informacji dotyczących zagrożeń dla IK, nie opracowywano i nie wdrażano procedur na wypadek wystąpienia takich zagrożeń oraz rozwiązań na wypadek zniszczenia lub zakłócenia funkcjonowania IK.
Współpraca państwa z podmiotami prywatnymi, jako cecha charakterystyczna skutecznego zarządzania w sytuacjach kryzysowych, musi uwzględniać nakładanie obowiązków na operatorów IK, a także rozwijać mechanizmy współpracy partnerskiej w zakresie wymiany doświadczeń oraz stanowienia standardów i zestawów dobrych praktyk.

# Bezpieczeństwo infrastruktury krytycznej

Zintegrowanie systemów staje się dziś koniecznością, przynajmniej na poziomie wymiany informacji i monitorowania zdarzeń w czasie rzeczywistym.

## Współpraca na linii biznes – biznes

Współpraca w zakresie ochrony infrastruktury krytycznej musi również przebiegać na linii biznes – biznes. Konieczna jest współpraca zarówno pomiędzy podmiotami z tego samego obszaru infrastruktury krytycznej, jak i podmiotów, pomiędzy którymi występują silne współzależności. Nie będzie to możliwe bez wzajemnego zaufania i zrozumienia, że leży to we wspólnym interesie podmiotów, które na co dzień ze sobą konkurują. Istnieje także wiele bardziej obiektywnych przeszkód dla swobodnego dzielenia się informacjami pomiędzy firmami. Ze względu na potrzebę ochrony tajemnicy przedsiębiorstwa oraz utrzymania przewagi konkurencyjnej, konsekwencje prawne, obawy przed stratami reputacyjnymi lub spadkami kursów akcji podmioty prywatne nigdy nie będą chętne do całkowitego dzielenia się informacjami. Zbudowanie wzajemnego zaufania pomiędzy przedsiębiorcami oraz przekonania o korzyściach wynikających z podejmowanej współpracy zajmie zapewne wiele lat.

Nadal nierozwiązany pozostaje spór, czy współpraca pomiędzy przedsiębiorcami powinna przebiegać na zasadzie dobrowolności, czy może konieczne jest wprowadzenie mechanizmów czyniących współpracę obligatoryjną.

## Integracja systemów

W wielu obiektach infrastruktury krytycznej wykorzystuje się sprzęt oraz systemy różnej generacji i różnych technologii. Co więcej, poszczególne systemy zazwyczaj działają niezależnie od siebie i nie wymieniają między sobą informacji.

Jak już podkreślono, tak jak zbyt głęboka współzależność może być problemem dla bezpieczeństwa, tak nie mniejszym kłopotem może być również brak jakiejkolwiek integracji pomiędzy systemami. Jest to szczególnie widoczne w przypadku największych obiektów, gdzie równolegle funkcjonują różne systemy alarmowe, zabezpieczenia mechaniczne, systemy bezpieczeństwa informacji, ochrona fizyczna, systemy automatyki budynkowej, systemy łączności i komunikacji, systemy automatyki przemysłowej, systemy pozycjonowania, systemy radarowe oraz inne urządzenia i systemy dostarczające w każdej sekundzie ogromne ilości danych. Jeżeli dodać do tego informacje pochodzące z zewnętrznych baz danych, źródeł medialnych, serwisów internetowych, to określenie „szum informacyjny" jest z pewnością bardzo łagodne.

W konsekwencji wdrożenie kolejnych systemów, które z założenia powinny usprawnić i ułatwić zarządzanie, przysparza dodatkowej pracy i wymaga ogromnego zaangażowania personelu. Zintegrowanie systemów staje się dziś koniecznością, przynajmniej na poziomie wymiany informacji i monitorowania zdarzeń w czasie rzeczywistym.

## Przygotowanie społeczeństwa

Ostatnim wyzwaniem związanym z zapewnieniem bezpieczeństwa infrastrukturze krytycznej jest przygotowanie społeczeństwa. Należy zwrócić uwagę na dwa elementy. Konieczne jest ciągłe szkolenie i kształtowanie właściwych postaw pracowników, przy równocześnie monitorowaniu i wykrywaniu nieodpowiedzialnych zachowań pracowników. O konieczności budowy w każdej organizacji odpowiedniej kultury bezpieczeństwa raczej nie trzeba przekonywać. Jednocześnie konieczne jest przygotowanie społeczeństwa na sytuacje, kiedy w wyniku wystąpienia zakłóceń w działaniu poszczególnych elementów lub systemów infrastruktury krytycznej świadczenie określonych usług (np. dostawy mediów, łączność i komunikacja) nie będzie możliwe przez określony czas. Dotyczy to również instytucji publicznych i przedsiębiorstw prywatnych, które świadome podobnych zagrożeń muszą przygotowywać się na tego typu scenariusze. W tym obszarze jest dużo do zrobienia.

Obecnie mieszkańcy miast nie muszą myśleć o zapewnieniu dostaw podstawowych mediów – wszystkie są dostarczane przez dedykowane systemy. Oprócz oczywistych korzyści, powoduje to jednak wzrost wrażliwości społeczeństwa na wszelkie zakłócenia w tych systemach. By zauważyć brak przygotowania do takich sytuacji, wystarczy spojrzeć na zachowania ludzi w czasie chwilowych utrudnień w funkcjonowaniu komunikacji publicznej lub okresowych przerw w działaniu systemu elektroenergetycznego.

By zauważyć brak przygotowania ludzi, wystarczy spojrzeć na zachowania w czasie utrudnień w funkcjonowaniu komunikacji publicznej lub przerw w działaniu systemu elektroenergetycznego.

## Podsumowanie

Przedstawione wyzwania dotyczące bezpieczeństwa infrastruktury krytycznej wskazują priorytety działalności na najbliższe lata. Nie jest to katalog zamknięty i w zależności od sektora lub specyfiki systemów mogą one podlegać pewnym modyfikacjom i przewartościowaniom. Jednocześnie trzeba mieć świadomość występowania bardziej przyziemnych problemów, z którymi na co dzień zmagają się osoby odpowiedzialne za bezpieczeństwo infrastruktury krytycznej.

Ostatnie kontrole i raporty potwierdzają, że potrzeba wielu lat intensywnej pracy, by można było mówić o dojrzałości systemu ochrony infrastruktury krytycznej.

BIO

**Sergiusz Parszowski**, niezależny ekspert i doradca do spraw bezpieczeństwa. Audytor systemów bezpieczeństwa. Doświadczony trener i szkoleniowiec. Autor publikacji dotyczących ochrony osób i mienia oraz bezpieczeństwa i porządku publicznego.

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

# Rozwiązania Commend dla bezpieczeństwa

# ComWin

**Platforma ComWin jest atrakcyjnym systemem do zarządzania bezpieczeństwem w obiektach infrastruktury krytycznej.** Dzięki różnorodnym i nowoczesnym rozwiązaniom można ją łatwo przystosować do każdej infrastruktury.

Platforma ComWin jest dobrze znana użytkownikom rozwiązań firmy Commend. Stanowi element wielu systemów i pozwala na skupienie w jednym miejscu tak złożonej operacji, jaką jest ochrona obiektów, np. jednostki wojskowej, elektrowni czy lotniska. Operator ma do dyspozycji interfejs graficzny prezentujący obiekt, a także inne funkcje zintegrowane z już zaimplementowanymi systemami SSWiN, SKD czy CCTV.
Istotnym czynnikiem wpływającym na sprawne reagowanie na zagrożenie jest wykorzystanie komunikacji głosowej jako kluczowego elementu wspierającego działania służb ochrony.

## Łatwa integracja

Przygotowując rozwiązanie do funkcjonowania na rynku, integrator musi uwzględniać kilka czynników, m.in. obecność w obiekcie elementów systemów zabezpieczeń, niekiedy niezwiązanych ze sobą, takich jak CCTV, SKD, SSP czy SSWiN. Nie bez znaczenia są również przyzwyczajenia użytkownika do już funkcjonujących rozwiązań, m.in. systemów Galaxy czy Compas w obiektach wojskowych. Otwartość platformy ComWin czyni ją rozwiązaniem atrakcyjnym i prostym do zaadaptowania w każdej infrastrukturze, co jest szczególnie istotne, gdy klient chce zachować fragmenty instalacji.
Commend wspiera wiele protokołów integracyjnych, np. KNX, Modbus IP, OPC, SNMP, TAPI, ESPA 4.4.4, SIP, TETRA. Jednocześnie wykorzystując SDK, umożliwia napisanie własnego oprogramowania scalającego. Integracja urządzeń telewizji dozorowej – przede wszystkim kamer – odbywa się z poziomu platformy VDG.

## Prosta obsługa

Jedną z kluczowych funkcjonalności systemu jest prosta obsługa. Mimo że system jest przeznaczony do obiektów specyficznych, będzie obsługiwany również przez osoby, które nie mają doświadczenia w tego typu rozwiązaniach (np. dowódca plutonu musi sprawnie poradzić sobie z zadaniem, będąc na służbie itp.). Operator dysponuje widokiem w formacie 2D lub 3D, w zależności od potrzeb. Wszystkie funkcje pulpitu sterującego są wyświetlane na jednym monitorze lub kilku. Interaktywne ikony (symbole na ekranie) reprezentują monitorowane urządzenia: czujki, kamery, stacje interkomowe czy czytniki SKD. Wszystkie ikony są aktywne i zmieniają barwę w zależności od wymaganego poziomu uwagi operatora. Zadania do wykonania w związku z zaistnieniem sytuacji alarmowej są prezentowane w dodatkowych oknach. Znajdują się tam m.in. listy czynności do wykonania w zaistniałej sytuacji lub pomocne informacje. Okna są konfigurowane w zależności od potrzeb, aby zapewnić operatorom przegląd całego systemu i jednocześnie prezentować na ekranie wszystkie istotne szczegóły dotyczące zdarzeń.
ComWin pozwala również na automatyzację niektórych procesów, np. wysłanie komunikatu SMS czy e-mail może się odbywać bez angażowania operatora, zgodnie z określonymi procedurami.

## Komunikacja głosowa

ComWin wykorzystuje możliwości, jakie w zakresie komunikacji głosowej zapewnia producent – firma Commend. Nie bez znaczenia jest fakt, że połączenia między wybranymi osobami mogą odbywać się automatycznie. Impulsem do działania może być np. sygnał alarmowy. W takim przypadku system – na podstawie wprowadzonych danych – zestawia automatycznie połączenia pomiędzy wszystkimi wskazanymi stanowiskami, które mają być zaangażowane w akcję; może też przesyłać wcześniej przygotowany komunikat głosowy.
Jednak to nie wszystko. Platforma ComWin, wykorzystując funkcję systemu interkomowego, umożliwia integrację wszystkich środków łączności, jakimi dysponuje jednostka wojskowa, np. telefonii stacjonarnej analogowej, VoIP, DECT, radiotelefonów Tetra czy sieci komórkowej.
Intuicyjność i prostota obsługi oraz łatwość dostosowania platformy zarządzającej bezpieczeństwem do istniejących już systemów są niewątpliwymi atutami rozwiązania, które znajduje zastosowanie w najbardziej wymagających miejscach.

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

# Ochrona granic obiektów za pomocą kamer sieciowych

**Kamery sieciowe wnoszą nową jakość do ochrony obwodowej,** dostarczając obraz w czasie rzeczywistym i umożliwiając tym samym podjęcie szybkich i skutecznych działań.

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

Ochrona obwodowa jest jednym z istotnych elementów zapewnienia bezpieczeństwa. Uniemożliwia wtargnięcie intruza na teren chroniony, zapobiega kradzieżom oraz aktom wandalizmu w przypadku zarówno osiedli domów jednorodzinnych, jak i obiektów infrastruktury krytycznej.
W ochronie obwodowej znalazły zastosowanie różne technologie detekcji, takie jak radar bliskiego zasięgu, lasery skanujące, czujki ruchu, czujki montowane pod powierzchnią ziemi czy kable sensoryczne na ogrodzeniach sygnalizujące pojawienie się intruza w chronionej strefie. Mimo że wszystkie spełniają swoją funkcję, to mają oczywiste ograniczenia – nie pozwalają odróżnić alarmów rzeczywistych od fałszywych, a przy tym podają jedynie ograniczony zakres informacji. W przypadku alarmu nie wiadomo, czy naruszenie granic dozorowanego obszaru rzeczywiście wystąpiło i czy konieczne jest podjęcie działań interwencyjnych. Sprawdzenie tego stanu jest nie tylko czasochłonne. Częste fałszywe alarmy wywołane np. przez przechodzące zwierzęta prowadzą do rozluźnienia w przestrzeganiu procedur bezpieczeństwa przez służby ochrony.
Doceniając wagę opisanego problemu oraz mając świadomość natury potencjalnych zagrożeń, organizacje i firmy coraz częściej sięgają po kamery sieciowe, które wspomagają pracę detektorów ochrony obwodowej. Zastosowanie kamer termowizyjnych jako detektorów wizyjnych oraz kamer wysokiej rozdzielczości do wizyjnej weryfikacji alarmu (wykrytego zagrożenia) pozwala uzyskać ważne informacje o przyczynie wyzwolenia alarmu oraz rodzaju zaobserwowanej aktywności.
W połączeniu z tradycyjnymi detektorami ochrony zewnętrznej kamery sieciowe tworzą inteligentny i niezawodny sieciowy system dozorowy. Dzięki różnorodności kamer dostępnych na rynku można dobrać odpowiednie urządzenie do założonych wymagań. Nawet w trudnych warunkach atmosferycznych czy oświetleniowych wyraźny i klarowny obraz na żywo i zarejestrowany ułatwi wykrycie i identyfikację obiektów, osób oraz incydentów. Automatyczna detekcja oraz oprogramowanie do analizy obrazu pozwolą zredukować liczbę interwencji człowieka, a także liczebność personelu ochrony.

## Wyzwania i rozwiązania

Głównym celem każdego systemu ochrony obwodowej jest wykrycie rzeczywistych zagrożeń i naruszeń chronionej strefy na najwcześniejszym etapie – przez całą dobę, siedem dni w tygodniu. Obszary wymagające monitorowania, takie jak tereny kolejowe, zajezdnie autobusowe, parkingi, porty czy otoczenie obiektów przemysłowych, bywają rozległe,

### INTEGRACJA DZIĘKI TECHNOLOGII IP

**Przyszłościowe, w pełni skalowalne sieciowe systemy dozorowe, współpracujące z czujkami ochrony obwodowej montowanymi na ogrodzeniu czy pod ziemią sprawdzą się w wielu zastosowaniach, zwłaszcza w ochronie infrastruktury krytycznej, gdzie wiele sygnałów alarmowych wymaga równoczesnej obsługi.**

co samo w sobie stanowi nie lada wyzwanie. Problemem są również warunki oświetleniowe, ponieważ w nocy często brakuje jakiegokolwiek oświetlenia sztucznego lub jest ono niewystarczające, by obraz był odpowiedniej jakości.
Efektywnym rozwiązaniem w zabezpieczaniu takich wymagających lokalizacji w trudnych warunkach otoczenia jest zastosowanie kamer termowizyjnych z funkcjami analizy wizyjnej wspieranych kamerami kopułkowymi PTZ. Termowizyjne kamery sieciowe nie wymagają do pracy żadnego oświetlenia, co czyni je oczywistym wyborem do monitoringu nocnego, a w ciągu nawet bardzo słonecznego dnia sprawdzają się w wykrywaniu osób i obiektów przysłoniętych przez złożone tło czy głęboki cień. Dostępne obecnie na rynku są tak czułe i dokładne, że stanowią „pierwszą linię" ochrony. Kamerę termowizyjną z zaimplementowanymi funkcjami analitycznymi można skonfigurować w taki sposób, by po rozpoznaniu podejrzanego zdarzenia kierowała na nie drugą – kamerę PTZ pozwalającą zbliżyć ujęcie i dostarczyć obraz na żywo w jakości HD.
Pracujące równolegle dwa rodzaje kamer tworzą precyzyjny mechanizm ochrony granicy obiektu. W celu zapewnienia nieprzerwanego zapisu i maksymalnej funkcjonalności każda kamera działa niezależnie w sieci IP. W przypadku awarii łącza sieciowego urządzenia mogą zapisywać dane na wbudowanej karcie SD na potrzeby ewentualnej przyszłej ich analizy.

## Szybkie i właściwe działanie

Efektywny system ochrony obwodowej musi działać odstraszająco, zapewniając jednocześnie natychmiastową weryfikację wizyjną. Obrazy w czasie rzeczywistym dostarczane przez kamery sieciowe umożliwiają personelowi ochrony zarówno podjęcie szybkich i właściwych działań, jak i ograniczają do minimum fałszywe alarmy. W przypadku wystąpienia incydentu kluczowe znaczenie ma transmisja: zarejestrowany materiał wizyjny można przesłać do zainteresowanych osób jako załącznik do e-maila, alarm zaś – na telefon komórkowy. Kierownicy ochrony mają możliwość przeglądania obrazu na żywo ze wszystkich kamer sieciowych w systemie. Mogą też zalogować się do serwera w pomieszczeniu nadzoru i tam wyszukać zarejestrowany materiał. Kamery można skonfigurować do automatycznego włączania urządzeń alarmowych w rodzaju reflektorów czy sygnalizatorów akustycznych. Możliwe jest również emitowanie ostrzeżeń słownych poprzez sieciowe głośniki tubowe.
Urok technologii IP polega na tym, że oparte na nich systemy można integrować ze sobą, a także z istniejącymi w obiekcie systemami zabezpieczeń elektronicznych. Takie przyszłościowe, w pełni skalowalne sieciowe systemy dozorowe, współpracując z czujkami ochrony obwodowej montowanymi na ogrodzeniu czy pod ziemią, sprawdzą się w wielu zastosowaniach, zwłaszcza w ochronie infrastruktury krytycznej, gdzie wiele alarmów wymaga równoczesnej obsługi.
Co ważne, ani zaawansowane technologie, ani ceny kamer sieciowych nie stanowią już bariery do ich szerokich zastosowań. Mogą sobie na nie pozwolić zarówno mniejsze firmy, jak i zamknięte osiedla mieszkaniowe. Dzięki zaimplementowanemu oprogramowaniu analitycznemu oraz innym inteligentnym aplikacjom wizyjny system dozorowy może zostać w dużym stopniu zautomatyzowany, a także zoptymalizowany pod względem kosztów. Przetwarzanie strumieni wizyjnych już w kamerze zmniejsza zapotrzebowanie na przepustowość łącza i pojemność drogich systemów zapisu. Nawet niewielkie instalacje o podstawowych funkcjonalnościach są w stanie zapewnić wymaganą wysoką jakość obrazu.
Bogata oferta kamer sieciowych w połączeniu z dostępnymi aplikacjami analitycznymi umożliwia różnorodność zastosowań i opłacalność inwestycji. Ważne jest również wyeliminowanie stresu i problemów wywołanych przez błędną interpretację zdarzeń i fałszywe alarmy, a także spokój osób odpowiedzialnych za strzeżone obiekty.


Efektywny system ochrony obwodowej musi działać odstraszająco, zapewniając jednocześnie natychmiastową weryfikację wizyjną.

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

# REDSCAN

**Wykorzystanie technologii skanowania wiązką lasera**
do zapewnienia bezpieczeństwa w obiektach infrastruktury krytycznej.

Stosowanie nowoczesnych technologii oraz integracja systemów zabezpieczeń to najskuteczniejsza droga prowadząca do zapewnienia bezpieczeństwa w obiektach infrastruktury krytycznej. Producenci urządzeń security prześcigają się w stosowaniu coraz bardziej zaawansowanych rozwiązań. Wykorzystanie rozbudowanego systemu ochrony może prowadzić do występowania dużej liczby niepożądanych alarmów. Takie zjawisko daje efekty odwrotne do zamierzonych – brak wiary w skuteczność działania systemu i zniechęcenie operatora. Optex – największy na świecie producent zewnętrznych czujek ruchu – w swoich najbardziej zaawansowanych rozwiązaniach wykorzystuje technologię laserową.
REDSCAN RLS-3060 oraz REDSCAN RLS-2020 to dwa modele urządzeń wykorzystujących tę samą technologię skanowania przestrzeni wiązką lasera podczerwonego (dł. fali 905 nm, zakres niewidzialny). Promień lasera jest kierowany w określony punkt za pomocą lustra obracającego się na poduszce elektromagnetycznej – w przypadku RLS-3060 z prędkością 20 razy na sekundę, RLS-2020 – 40 razy na sekundę. Podstawowym parametrem do analizy jest czas przelotu, czyli czas od momentu emisji każdej wiązki do jej powrotu do odbiornika po odbiciu od przeszkody. Analiza zależności kąta, czasu i odległości dla każdej wiązki pozwala na obliczenie rozmiarów intruza oraz odległości, jaką pokonał. Stanowi to podstawę do wysłania sygnału alarmowego generowanego przez poruszającego się człowieka, a nie zwierzę czy pojazd. Wszystkie procesy obliczeniowe odbywają się w układach elektronicznych czujki i nie wymagają wsparcia przez komputer zewnętrzny. Czujki mogą być zasilane z wykorzystaniem *Power over Ethernet* (PoE) i mogą wysyłać alarmy za pomocą tradycyjnych wyjść przekaźnikowych lub używając komunikacji IP. Użycie czujek laserowych Optex jako uzupełnienie działania systemów dozoru wizyjnego pozwala zredukować liczbę fałszywych alarmów (wywoływanych np. przez opady atmosferyczne, słabe oświetlenie czy owady fruwające przed obiektywem kamery lub pełzające po nim) nawet o 70–80%. Urządzenia są zintegrowane z produktami wszystkich głównych producentów systemów telewizji dozorowej, np. Axis, Milestone, Geneteck, Hikvision, Gemos (więcej na www.optex-vms.com).
REDSCAN Manager – oprogramowanie do zarządzania wszystkimi czujkami skanującymi firmy Optex – ma duże możliwości konfiguracji parametrów, zapewnia dopasowanie kształtu obszaru detekcji do wymagań użytkownika, rozmieszczenie stref alarmo-

## Różnice pomiędzy modelami czujek skanujących REDSCAN

| Model | RLS-2020 | RLS-3060 |
|---|---|---|
| Minimalna wielkość wykrywanego obiektu | 2,5 cm | 13 cm |
| Wymiary | 146 x 160 x 160 mm (porównywalne z kamerą PTZ) | 334 x 144 x 155 mm |
| Masa | 1 kg | 2,5 kg |
| Strefa detekcji | 20 x 20 m, kąt 95° | promień 30 m, kąt 190° |
| Montaż | w środku strefy | narożny |
| Rozdzielczość skanowania | 0,25 stopnia | 0,25 stopnia lub 0,125 stopnia |
| Zasilanie | 12 V lub PoE | 24 V lub PoE+ |
| Regulacja wielkości wykrywanego obiektu | płynna | 3 poziomy: mały, średni, duży |

wych, wybór algorytmu pracy. Znacznym ułatwieniem dla operatora strojącego czujkę jest wizualizacja strefy detekcji – operator widzi to samo, co czujka. Takie rozwiązanie jest bliskie temu, z jakim mamy do czynienia, stosując funkcje analizy wizyjnej. REDSCAN RLS-3060 tworzy strefę detekcji o promieniu 30 m i kącie 190 stopni w poziomie lub w pionie (pod kątem). Duża szybkość i rozdzielczość skanowania sprawiają, że obszar działania jest niewidzialną taflą niewielkiej grubości, której kształt można dopasować do wymagań aplikacji. REDSCAN znajduje zastosowanie wszędzie tam, gdzie zachodzi potrzeba precyzyjnego ukształtowania strefy alarmowania. Łatwa integracja z systemami CCTV umożliwia szybką weryfikację zdarzenia. Czujka laserowa jest np. stosowana jako zewnętrzne zabezpieczenie dachu i ścian budynków, wirtualny sufit w centrach handlowych i magazynach czy kurtyna w muzeach. Doskonale sprawdza się w zakładach penitencjarnych, gdzie służy do zabezpieczenia murów i ogrodzenia, fasad pawilonów oraz wewnętrznej strefy podejścia do ogrodzenia. Czujkę RLS-3060 zastosowano w wielu projektach wymagających wysokiego poziomu zabezpieczenia.

Ochrona świetlika wewnątrz budynku

W konstrukcji swojego nowego produktu firma Optex wykorzystała doświadczenia i oczekiwania użytkowników czujek. Bardziej wydajny procesor pozwala na wykrywanie obiektów (przy instalacji wewnątrz budynków) poruszających się z większą prędkością – 16,2 km/h (biegacz) przy montażu prostopadle do podłoża lub 45 km/h (skuter) przy montażu pod kątem 30 stopni. Kolejnym ulepszeniem jest detekcja obiektów o małych rozmiarach. RLS-2020S może wykrywać obiekty wielkości pudełka zapałek. Ważną innowacją jest możliwość zmiany scenariusza działania z użyciem fizycznego wejścia (kontrola dostępu, przycisk, manipulator).

Wszystko to sprawia, że RLS-2020S może być stosowana w obiektach wysokiego ryzyka, takich jak lotniska, budynki administracji rządowej czy centra obróbki danych. Uwagę zwraca również niższa cena nowego rozwiązania. Technologia użyta w czujkach skanujących REDSCAN może zapewnić efektywną ochronę w miejscach wymagających wysokiego poziomu ochrony. Wprowadzenie do oferty nowego produktu o innej charakterystyce ułatwia projektowanie systemu i pozwala na optymalizację kosztów wdrożenia aplikacji.

Zastosowanie RLS-3060 w obiektach infrastruktury krytycznej

RLS-2020S zabezpiecza zewnętrzne ściany magazynu

ICS Polska
ul. Poleczki 82
02-822 Warszawa
www.ics.pl

# TAKEX
# ochrona obwodowa wymagających obiektów

Obiekty przemysłowe, takie jak elektrownie, rafinerie czy fabryki przetwórstwa chemicznego, muszą być dobrze chronione przed dostępem osób postronnych. **Podstawową rolę ochronną odgrywa solidne ogrodzenie, ale w wielu przypadkach to za mało.**

Nie ma ogrodzenia niemożliwego do sforsowania, dlatego w obiektach wysokiego ryzyka stosuje się systemy elektronicznej ochrony obwodowej. Wykrywają one próbę wtargnięcia na teren obiektu i sygnalizują służbom ochrony jej lokalizację. Na rynku jest wiele różnych rozwiązań ochrony obwodowej. Odpowiednim i niedrogim produktem są bariery podczerwieni. Jednym z najlepszych i najbardziej rozpoznawalnych na rynku producentów barier podczerwieni jest japońska firma Takex.
Produkty firmy Takex cieszą się dużym uznaniem wśród instalatorów i użytkowników na całym świecie. Obok produkcji pasywnych detektorów ruchu, zarówno wewnętrznych, jak i zewnętrznych, wizytówkę firmy stanowią aktywne bariery podczerwieni. Ponad kilkadziesiąt modeli świadczy o dużej różnorodności sprzętu i umożliwia użytkownikowi wybór odpowiedniego urządzenia. Nowatorskie rozwiązania, takie jak opatentowana podwójna modulacja wiązki, klasyfikują te urządzenia do najbardziej zaawansowanych technicznie barier podczerwieni dostępnych na rynku polskim.

## Wyeliminowanie fałszywych alarmów

Pula rozwiązań zastosowanych w barierach podczerwieni Takex gwarantuje ich dużą odporność na fałszywe alarmy. Bariera pracuje poprawnie nawet w przypadku 99-proc. tłumienia wiązki pomiędzy nadajnikiem a odbiornikiem. Decydują o tym: • podwójna modulacja częstotliwość wiązki • układ PLL • cztery kanały pracy • regulacja czasu naruszenia wiązki • układ AGC • regulacja mocy wiązki nadawanej • wyjście pogodowe • wysokiej jakości filtry światła białego.
Dodatkowe wyposażenie barier podczerwieni stanowią grzałki i termostaty, które zapewniają bezawaryjną pracę w nawet najostrzejszych okresach zimy. Dostępne obudowy kolumnowe o wysokościach od 1 do 3 m, w wersjach jednostronnej i dwustronnej, pozwalają na tworzenie układów wielobarierowych o zwiększonym bezpieczeństwie (bariera jest ukryta w obudowie, intruz nie wie, ile kompletów i na jakiej wysokości zamontowano) oraz dużej estetyce wykonania. Wszystkie produkty Takex są objęte pięcioletnią gwarancją.

## GAMA PRODUKTÓW

**W szerokiej ofercie produktowej firmy Takex znajdują się następujące urządzenia:**

- dwuwiązkowe bariery IR o zasięgach zewnętrznych 30 m (PB-30TK), 60 m (PB-60TK), 100 m (PB-100TK), 100 m (PB-100ST) z jedną częstotliwością pracy;
- dwuwiązkowe bariery IR o zasięgach zewnętrznych 20 m (PB-20TE), 40 m (PB-40TE), 60 m (PB-60TE) z czterema częstotliwościami pracy;
- czterowiązkowe bariery IR o zasięgach zewnętrznych 50 m (PB-50F), 100 m (PB-100F), 200 m (PB-200F) z jedną częstotliwością pracy;
- czterowiązkowe bariery IR o zasięgach zewnętrznych 50 m (PB-IN-50HF), 100 m (PB-IN-100HF), 200 m (PB-IN-200HF) z czterema częstotliwościami pracy, wyjściem pogodowym, pamięcią alarmu, regulacją mocy wiązek i wbudowanym sygnalizatorem ułatwiającym prawidłowe zestrojenie toru optycznego;
- czterowiązkowa bariera IR o zasięgu zewnętrznym 100 m (PB-IN-100AT), parametry jak w przypadku barier serii PB-IN-HF, a dodatkowo funkcja „antyprzeczołganie" oraz osobna regulacja czasu naruszenia dla 2 i 4 wiązek;
- bariery IR z reflektorem pryzmatowym o zasięgu wewnętrznym 1 m (PR-1B), 5 m (PR-5B), 10 m (PR-10B) oraz zasięgu zewnętrznym 11 m (PR-11B).

Opisane produkty są dostępne w ofercie firmy **ICS Polska**, która jest wyłącznym autoryzowanym przedstawicielem firmy Takex w Polsce.

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

# Zaawansowana ochrona obiektów kluczowych

**Strategiczne znaczenie obiektów przemysłowych i infrastruktury krytycznej wymusza nadzwyczajne podejście do ich ochrony i dozoru.** Co trzeba brać pod uwagę przy projektowaniu ich zabezpieczeń?


SATEL INTEGRA Plus

Ochronę na najwyższym poziomie gwarantuje system alarmowy SATEL bazujący na zaawansowanej centrali serii INTEGRA Plus, uzupełniony o wysokiej jakości urządzenia peryferyjne, takie jak dualne czujki ruchu OPAL Pro, nowoczesne czujki kurtynowe AGATE, manipulatory INT-TSI, INT-TSH, INT-TSG, INT-KLCDR, zasilacze buforowe APS-612 oraz moduły rozszerzeń INT-E i INT-O.

Zapewnienie ciągłości ochrony i natychmiastowej reakcji na niepożądane zdarzenia to podstawowe zadania systemów zabezpieczeń takich obiektów. Wdrażane zabezpieczenia techniczne muszą więc skutecznie zapobiegać wtargnięciu przez osoby nieupoważnione i możliwości podjęcia działań sabotażowych newralgicznych elementów zabezpieczanych zasobów. Takie rozwiązania powinny też być uzupełnieniem bezpośredniej ochrony fizycznej, świadczonej przez specjalistyczne służby.

## Zabezpieczenia najwyższej jakości

Podmiot odpowiedzialny za zapewnienie bezpieczeństwa w zakresie elektronicznych systemów zabezpieczeń musi brać pod uwagę wiele aspektów. Instalacja chroniąca wnętrza obiektów powinna spełniać wymagania odpowiednich aktów normatywnych, np. EN 50131 Grade 3 (norma dot. SSWiN instalowanych w budynkach), ściśle określających parametry stosowanych rozwiązań. Trzeba też pamiętać, że obiekty infrastruktury krytycznej lub przemysłowe to przeważnie rozległe zespoły budynków, wymagające ochrony nie tylko wewnętrznej, lecz także na zewnątrz. Dlatego wymagają zastosowania niezawodnego sprzętu najwyższej klasy, który może pracować w szerokim zakresie temperatur, w trudnych warunkach środowiskowych i który musi być odporny na zakłócenia.

Ważne, by centrala alarmowa, na której bazuje cała instalacja, mogła współpracować z wieloma urządzeniami różnego typu, ze szczególnym uwzględnieniem zaawansowanych czujek wielofunkcyjnych. Powinna także zapewniać monitorowanie ich stanu, powiadamiać o zdarzeniach w systemie, jak również umożliwiać obsługę wielu użytkowników o zróżnicowanych uprawnieniach dostępowych, w tym takich, którzy mają jedynie czasowy dostęp, np. pracownicy serwisu sprzątającego. W placówkach dozorowanych przez ochronę fizyczną sprawdzą się także funkcje wymuszające podjęcie określonych działań, np. cyklicznego obchodu wartownika w obiekcie.

Urządzenia tworzące instalację zabezpieczenia technicznego w tak wymagających obiektach powinny także posiadać zabezpieczenia przed próbami ich unieszkodliwienia przez intruza. Przykładem może być stosowany w czujkach ruchu aktywny antymasking IR alarmujący o zasłonięciu, zaklejeniu lub zamalowaniu. Ciągłość ochrony zapewniają również odpowiednie zasilacze, gwarantujące stabilną pracę instalacji nawet przez kilkadziesiąt godzin po dokonaniu sabotażu polegającego na odcięciu zasilania lub awarii wynikającej ze zdarzeń losowych, a po jego przywróceniu – szybkie naładowanie akumulatorów.

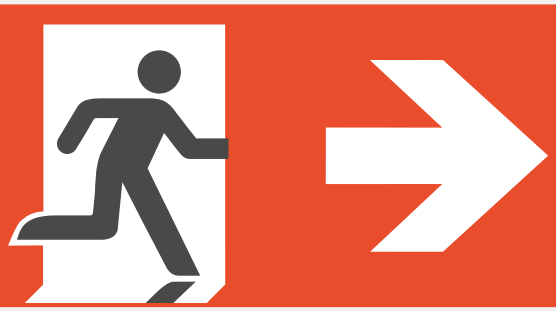
## Urządzenia o wysokim stopniu ochrony

Realizację tych funkcji oferują produkty firmy Satel spełniające rygorystyczne kryteria norm branżowych. W przypadku zarządzania rozproszonymi systemami zabezpieczeń sieci obiektów strategicznym rozwiązaniem może okazać się specjalizowane oprogramowanie integrujące, takie jak INTEGRUM. To narzędzie opracowane przez inżynierów firmy Satel umożliwia wygodne kierowanie ochroną grupy placówek połączonych w centralnie zarządzany system.

Więcej informacji na temat INTEGRUM na str. 31 tego wydania „a&s Polska”

# Bezpieczeństwo pożarowe w obiektach infrastruktury krytycznej

**Zapewnienie bezpieczeństwa w obiektach budowlanych należących do infrastruktury krytycznej państwa stanowi ogromne wyzwanie** i nakłada dużą odpowiedzialność na wszystkie strony zaangażowane w ten proces.



**Grzegorz Ćwiek**
Schrack Seconet Polska

Problematyka ta jest tym bardziej złożona, że dotyka wielu warstw działania i współdziałania ludzi zarówno w kraju, jak i wymiarze międzynarodowym, zaangażowania często znaczących środków finansowych i wyboru odpowiedniej technologii wspierającej nakreślone plany i wyznaczone zasady oraz budżety.
Infrastruktura krytyczna (IK) zgodnie z definicją Ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2013 r. poz. 1166 oraz z 2015 r. poz. 1485) *to systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców*[1].

[1] Zob. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2013 r. poz. 1166 oraz z 2015 r. poz. 1485).

Wykaz obiektów budowlanych ma charakter niejawny, w przypadku IK są to przede wszystkim te obiekty, których zniszczenie lub zakłócenie działania mogłoby spowodować sytuację kryzysową, mającą negatywny wpływ na poziom bezpieczeństwa ludzi lub środowiska. W ustawie wymieniono obiekty (jako część systemów) związane z zaopatrzeniem w energię, surowce energetyczne i paliwa, zapewnieniem łączności i sieci teleinformatycznych, odgrywające kluczową rolę w obszarze transportu, finansów itd. Jest ich w kraju ogromna liczba, a prawidłowe zabezpieczenie przeciwpożarowe stanowi jeden z ważniejszych sposobów ich ochrony. Wspomniana ustawa nie mówi wiele na ten temat, a zasad, wytycznych i wskazówek do zaplanowania i wykonania takich zabezpieczeń można szukać w innych aktach prawnych i dokumentach wspierających.

Z punktu widzenia sztuki zabezpieczenia przeciwpożarowego obiektów budowlanych IK obowiązują niemal identyczne zasady i praktyki jak w przypadku każdego zwykłego obiektu spoza katalogu IK. Podstawowymi aktami prawnymi, regulującymi bezpieczeństwo ppoż. w zakresie minimalnych wymagań, są:

- Rozporządzenie Ministra Infrastruktury z 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie (Dz.U. z 2015 r. poz. 1422);
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. nr 109, poz. 719);
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 24 lipca 2009 r. w sprawie przeciwpożarowego zaopatrzenia w wodę oraz dróg pożarowych (Dz.U. nr 124, poz.1030).

Najważniejsze dla zabezpieczeń przeciwpożarowych są jednak wspomniane wcześniej wskazówki dodatkowe oraz wytyczne pozwalające znacznie lepiej dobrać właściwe środki bezpieczeństwa. Szczególną uwagę należy zwrócić na najnowszy dokument przyjęty przez Radę Ministrów (Uchwała nr 210/2015 RM z 2 listopada 2015 r.), będący aktualizacją Narodowego Programu Ochrony Infrastruktury Krytycznej.

Publikacja NPOIK to doskonały krok w kierunku uświadomienia wielu interesariuszom konieczności szerszego spojrzenia na specyfikę zapewnienia bezpieczeństwa (pożarowego) obiektów infrastruktury krytycznej.

W odróżnieniu od ustaw i rozporządzeń, do których jesteśmy przyzwyczajeni od lat, a które są napisane mało zrozumiałym językiem i nie dają przejrzystych wskazówek nawet specjalistom, dokument NPOIK promuje nowoczesne zasady zarządzania procesem zapewnienia bezpieczeństwa. W dużej mierze jego konstrukcja opiera się na wykorzystaniu praktyk i integracji działań zaczerpniętych z systemów zarządzania jakością, bezpieczeństwem, środowiskiem, ciągłością działania oraz zarządzania ryzykiem. Dokument powołuje się na takie normy i wytyczne, jak PN-EN ISO 9001 (systemy zarządzania jakością), PN-EN ISO 14001 (system zarządzania środowiskowego), OSHA 1910.119 (zarządzanie bezpieczeństwem procesowym), PN ISO 31000 (zarządzanie ryzykiem), PN-EN ISO 22301 (bezpieczeństwo powszechne, systemy zarządzania ciągłością działania), ISO 22313:2012 (systemy zarządzania ciągłością działania – poradnik), BS 11200:2014 (zarządzanie kryzysowe – dobre praktyki), NIST SP 800-34 (wytyczne w zakresie utrzymania ciągłości działania dotyczące technologii informatycznych) i wiele innych.
Na tej podstawie można stwierdzić, że zapewnienie bezpieczeństwa ppoż. w obiektach budowlanych o szczególnym znaczeniu (jako elementu systemu IK) wymaga innego podejścia niż w przypadku obiektów spoza tego obszaru. Konieczne jest bowiem dokonanie bardziej szczegółowej analizy związków między zagrożeniami, podatnością obiektów na owe zagrożenia oraz skutkami, jakie zdarzenia o charakterze kryzysowym mogą wywołać dla bezpieczeństwa, np. ludności całego regionu. Ciężar strat wywołanych pożarem takiego obiektu jest nieporównywalnie większy niż np. niewielkiego obiektu niebędącego elementem IK, a więc standardowe podejście do projektowania, instalacji i konserwacji systemu sygnalizacji pożarowej nie wystarczy.
Przykładem nowoczesnego (tak potrzebnego dzisiaj także poza obszarem infrastruktury krytycznej) podejścia do tworzenia zabezpieczeń ppoż. są np. wytyczne dotyczące zapewnienia bezpieczeństwa technicznego. NPOIK promuje budowę systemów odpornych na zakłócenia (tzw. rezylientnych), a zatem nie tylko działających sprawnie na co dzień, ale także pozwalających na szybkie i sprawne odbudowanie swoich właściwości po wystąpieniu zdarzenia krytycznego, np. pożaru czy awarii.

Dobierając urządzenia do systemu np. sygnalizacji pożarowej, projektant lub wykonawca powinni kierować się następującymi wskazówkami doboru technologii i procesu ich wdrożenia:
- zapewnienie ciągłości usługi (wykrywania pożaru i sterowania urządzeniami przeciwpożarowymi) – dzięki wykorzystaniu takich cech technicznych, jak nadmiarowość czy organizacyjnych, jak strategia obsługi posprzedażowej;
- niezawodność – poprzez oszacowanie niezbędnej dostępności do zasobów systemu, wybór lub wymaganie spełnienia konkretnego (%) wskaźnika gotowości urządzeń ppoż.;
- zdolność serwisowa – rozumiana jako charakterystyki utrzymania ruchu, czasu napraw, niezbędnego czasu i nakładów na konserwację itd.;
- bezpieczeństwo – z punktu widzenia spełnienia wymagań podstawowych (prawnych i normatywnych), np. dla wykorzystanych urządzeń.

Wymienione punkty mogą się wydawać tożsame, gdyż w ostatecznym rozrachunku dotyczą konieczności utrzymania ciągłości działania wszelkich elementów tworzących dany system bezpieczeństwa (jako podsystem IK). Jednak po wnikliwej lekturze objawią się jako dziesiątki ważnych punktów na liście kontrolnej planowania bezpieczeństwa pożarowego – od fazy tworzenia koncepcji, poprzez projekty, proces przetargowy, aż po fazę odbiorów instalacji. Po głębszej analizie wymagań w zakresie ochrony przeciwpożarowej okaże się, że spośród kilkudziesięciu produktów zdolnych spełnić większość wymagań technicznych IK pozostanie do wyboru kilkanaście; wszystkie wymagania spełni już tylko kilka urządzeń czy systemów, a braki formalne w wielu przypadkach pozostawią do dyspozycji inwestora jednego lub dwu producentów systemów zabezpieczeń ppoż. Podobnie w przypadku firm projektowych lub wykonawczych – charakterystyka działalności, doświadczenie, zdolność do utrzymania procesów na wyznaczonym poziomie i wypełnienia procedur zgodnie z przyjętymi zasadami i przepisami ograniczy możliwość uczestnictwa w przetargu na wykonanie instalacji tylko do wąskiego grona najlepszych.

## PODSUMOWANIE

Artykuł nie wyczerpuje tematyki zapewnienia bezpieczeństwa pożarowego w obiektach infrastruktury krytycznej, stanowi wręcz przyczynek do dalszej, głębszej dyskusji na ten temat. Wskazuje na konieczność innego, szerszego rozumienia bezpieczeństwa (pożarowego) w przypadku obiektów o szczególnym przeznaczeniu. Temu celowi może służyć poznanie wielu innych, poza zwykle stosowanymi w branży, norm i regulacji, w tym związanych z zarządzaniem ryzykiem, utrzymaniem ciągłości czy zarządzaniem procesowym.
Problematyka doboru urządzeń i technologii nie jest bowiem tak ważna, jak podejście holistyczne, systemowe do całości procesu zapewnienia właściwej ochrony, np. w wyniku zastosowania cyklu PDCA przez wszystkich uczestników procesu w celu upowszechnienia myślenia krytycznego, wyeliminowania błędów projektowania, wykonawstwa czy używania urządzeń najtańszych i awaryjnych (brak kryterium cenowego przy wyborze ofert w procesie przetargowym).
Niezwykle istotne jest, by każdy, kto zamierza uczestniczyć w procesie zabezpieczenia ppoż. obiektów infrastruktury krytycznej, poznał nowoczesne zasady zarządzania wymienione w NPOIK. Podniesienie jakości działania wszystkich uczestników takich zadań z pewnością przyczyni się do poprawy bezpieczeństwa obywateli.
Może nadejdzie taki czas, kiedy podobne podejście będzie stosowane powszechnie, we wszystkich projektach niezwiązanych z infrastrukturą krytyczną.

**Bibliografia**

[1] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

[2] Materiały internetowe Rządowego Centrum Bezpieczeństwa www.rcb.gov.pl.

[3] Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity wraz z załącznikami.

Ela-compil sp. z o.o.
ul. Słoneczna 15a,
60-286 Poznań
https://ela.pl

# FPM+

Podczas projektowania obiektów szczególny nacisk jest kładziony na ochronę przeciwpożarową. **Niewłaściwie zaprojektowane sieci urządzeń przeciwpożarowych lub ich nienależyta organizacja mogą być przyczyną powstania niebezpiecznych dla życia sytuacji pożarowych.**

# Rola centrali sterującej urządzeniami ppoż. w realizacji scenariuszy pożarowych

Aby uniknąć takiego ryzyka, tworzy się ściśle określone procedury i standardy, które muszą być bezwzględnie przestrzegane.

## Elementy niezbędne w systemach przeciwpożarowych

Zaprojektowane systemy przeciwpożarowe muszą poprawnie funkcjonować. W przypadku zagrożenia pożarem muszą gwarantować sprawną ewakuację ludzi przebywających w budynku oraz zapewniać bezpieczeństwo służbom ratowniczym.
W tym celu opracowuje się zaawansowane scenariusze pożarowe (opis sekwencji zdarzeń na wypadek pożaru). Pierwszym etapem takiego projektu jest analiza i wskazanie koncepcji niezbędnych do jego wykonania. Następnie dobiera się urządzenia przeciwpożarowe, ze szczególnym uwzględnieniem ich funkcjonalności, oraz planuje ich umiejscowienie w zabezpieczanym obiekcie.

Kluczowym elementem realizacji scenariusza pożarowego jest nadzorowanie wszystkich urządzeń na co dzień i podczas sytuacji krytycznych. W tym celu tworzy się również procedury na wypadek awarii lub niewłaściwej pracy urządzeń oraz procedury powiadamiania służb, które są odpowiedzialne za sprawność systemu.

## Jak spełnić te wymagania?

Firma Ela-compil opracowała jedną z pierwszych na rynku central sterujących urządzeniami przeciwpożarowymi: FPM+. Jej zadaniem jest sprawowanie nadzoru nad urządzeniami przeciwpożarowymi zainstalowanymi w obiekcie, sygnalizowanie ich stanu, zgłaszanie alarmów pożarowych, a także sygnalizowanie uszkodzenia czy zablokowania konkretnego urządzenia lub grupy urządzeń. Zastosowanie centrali FPM+ rozwiązuje problem sterowania zarówno urządzeniami przeciwpożarowymi, jak i pozostałymi uwzględnionymi w scenariuszu pożarowym.
Centrala FPM+ realizuje wszystkie sterowania wynikające z założeń scenariusza pożarowego, z uwzględnieniem wymagań technologicznych, którym podlegają urządzenia. Pozwala również nadzorować wszystkie urządzenia i sterować tymi, które podczas pożaru powinny przejść w odpowiedni stan pracy. FPM+ jest neutralna wobec wszystkich urządzeń pożarowych, takich jak klapy przeciwpożarowe, wentylatory, automatyczne kurtyny dymowe, bramy przeciwpożarowe itp., niezależnie od producenta. Oznacza to, że projektant może dobrać urządzenie dowolnego producenta bez obawy o jego kompatybilność z centralą sterującą.
By ułatwić projektantom opracowanie matrycy sterowań, firma Ela-compil udostępnia nieodpłatnie intuicyjny program konfiguracyjny, który pozwala szybko i sprawnie implementować matrycę, dodatkowe parametry i funkcje specjalne w centrali FPM+. Dzięki jego zastosowaniu projektowanie przebiega szybciej i łatwiej.

## Stała kontrola i możliwość sterowania ręcznego

Centrala sterująca FPM+ jest odpowiedzią na zapotrzebowanie rynku. Możliwość współpracy z dowolnym systemem sygnalizacji pożarowej sprawia, że projektant bez problemu zastosuje preferowane przez siebie urządzenia przeciwpożarowe w obiekcie.
Wdrożenie centrali przeciwpożarowej FPM+ zapewnia nie tylko ciągły monitoring stanu urządzeń, ale także pozwala na wyłączenie automatycznego trybu sterowania w sytuacji, gdy z dowolnej przyczyny powstałby nieuzasadniony alarm. FPM+ umożliwia błyskawiczne przywrócenie stanu pracy urządzeń oraz ręczną zmianę lub uruchomienie scenariusza sterowań.

# CENTRALA STERUJĄCA
## urządzeniami przeciwpożarowymi

FPM+

Centrala przeznaczona do nadzorowania i sterowania urządzeniami ppoż. Ułatwia zarządzanie i kontrolę nad systemami uruchamianymi w sytuacji zagrożenia pożarem.


## Zalety centrali FPM+:

- szybkie i łatwe projektowanie
- jedna matryca sterowań
- opcja sterowania ręcznego
- integracja i monitoring urządzeń ppoż.
- współpraca z dowolnym systemem sygnalizacji pożaru
- współpraca z dowolnym systemem nadrzędnym

**Normy i certyfikaty:**

- deklaracja zgodności 001/2015
- certyfikat zgodności z aprobatą 2974/2014
- świadectwo dopuszczenia CNBOP nr 2237/2014

elacompil

Ela-compil sp. z o.o., ul. Słoneczna 15a, 60-286 Poznań, tel.: +48 61 869 38 50, -60, **www.ela.pl**

Minimax Polska
Kiełpin, ul. Ogrodowa 27/ 29
05-092 Łomianki
www.minimax.pl

# Ochrona ppoż. elektrociepłowni

Elektrociepłownie charakteryzują się wysokim stopniem zaawansowania technologicznego. **Duża liczba jednostek operacyjnych sprawia, że muszą spełniać najwyższe wymogi organizacyjne, szczególnie pod kątem niezawodności i bezpieczeństwa, w tym pożarowego.**

Optymalna ochrona przeciwpożarowa w elektrociepłowniach wymaga zastosowania specjalistycznych rozwiązań dla każdego obszaru, aby zapobiec zniszczeniu nieruchomości i wyposażenia oraz zapewnić ciągłość działań operacyjnych. Minimax, jako dostawca kompleksowych rozwiązań ochrony przeciwpożarowej, oferuje unikatową gamę innowacyjnych systemów ppoż. i instalacji gaśniczych. Spełniają one najwyższe standardy jakości i sprawdzają się jako wydajne i skuteczne rozwiązania przeciwpożarowe.

## Zbiorniki olejowe

W elektrociepłowniach wykorzystujących podwójne turbiny paliwowe, zasilane zarówno gazem, jak i parą, paliwo oraz olej paliwowy mogą być przechowywane w zbiornikach o dużych rozmiarach.
**Zagrożenie:** samozapłon gazów znajdujących się w zbiorniku olejowym, uderzenie pioruna lub zaiskrzenie powodowane ładunkiem elektrostatycznym.

## ROZWIĄZANIA PPOŻ. REKOMENDOWANE PRZEZ MINIMAX

| SYSTEMY PRZECIWPOŻAROWE | INSTALACJE TRYSKACZOWE | SYSTEMY GASZENIA WODNĄ MGŁĄ MINIFOG | INSTALACJE ZRASZACZOWE | SYSTEMY HYDRANTÓW | SYSTEMY GASZENIA PIANĄ | SYSTEMY GAŚNICZE OXEO (ARGON / AZOT) | SYSTEMY GAŚNICZE $CO_2$ | SYSTEMY GAŚNICZE (NOVEC™ 1230) MX 1230 | SYSTEMY WYKRYWANIA POŻARU |
|---|---|---|---|---|---|---|---|---|---|
| **Produkcja energii** | | | | | | | | | |
| Zbiorniki olejowe | | | ● | | ● | | | | ● |
| Kotłownie z odzyskiem ciepła | | ● | ● | ● | | | | | ● |
| Turbiny gazowe | | ● | | | | ■ | ● | | ● |
| Turbiny parowe – komory/przewody olej. | | ● | ● | | | | | | ● |
| Kanały/pomieszcz. kablowe, magistrale | ● | ● | | | | | | | ● |
| Pomieszczenia kontroli elektrycznej | | | | | | ■ | | ● | ● |
| Transformatory | | ● | ● | | | | | | ● |
| **Pomieszczenia dodatkowe** | | | | | | | | | |
| Budynki administracyjne | ● | ● | | ● | | | | | ● |
| Serwerownie | | | | | | ■ | | ● | ● |

**Ochrona przeciwpożarowa:** najlepszym rozwiązaniem jest instalacja pianowych systemów gaśniczych z zestawem MX TankFoam RTK. System wytwarza pianę o wolnym tempie rozprzestrzeniania (piana lekka). W momencie wybuchu pożaru zajęta ogniem powierzchnia jest zalewana pianą od góry. Piana powoduje natychmiastowy efekt chłodzenia, tłumi płomienie i chroni już ugaszony obszar przed ponownym wybuchem ognia. Jednocześnie, jeśli to wskazane, ściany boczne oraz dach zbiornika są chłodzone przez instalację zraszaczy wodnych.

## SYSTEM MX TankFoam RTK

Rura pianowa, garnek pianowy i wlew piany – te trzy powiązane ze sobą elementy tworzą zestaw systemu MX TankFoam RTK.
System służy do ochrony ppoż. szczególnie łatwopalnych cieczy przechowywanych w zamkniętych zbiornikach (łącznie ze zbiornikami z pływającym dachem lub górną warstwą azotu).
Mieszanka piany i wody, uwolniona z wielką siłą w momencie wybuchu pożaru, zasysa powietrze przez system otworów w rurze pianowej.
W efekcie wibracji i turbulencji tworzy się piana lekka. Podlega ona procesowi ujednolicenia w komorze pianowej, przechodząc dalsze jakościowe usprawnienie. Ciśnienie wywołane przez pianę powoduje pęknięcie dysku i piana zaczyna być uwalniana do zbiornika. W następstwie powstaje film pianowy, który odcina dopływ tlenu do płomieni i zapobiega ponownemu pojawieniu się ognia.
W systemie MX RankFoam RTK mogą zostać użyte wszystkie dostępne na rynku koncentraty pianowe. System może być również wypełniony specjalnie zaprojektowanymi składnikami aktywnymi.

## SYSTEM MGŁY WODNEJ Minifog ProCon

System Minifog ProCon zużywa do 70% mniej wody niż klasyczne instalacje zraszaczy. Wydajna ochrona ppoż. przy niskim zużyciu wody redukuje do minimum okresy przestojów produkcyjnych wynikłych z pożaru. Dodatkowo wykorzystanie mgły wodnej obniża temperaturę powietrza w otoczeniu, co jest szczególnie ważne z punktu widzenia ochrony ludzi.

Minifog ProCon może zostać połączony ze standardowym systemem gaszenia, np. instalacją tryskaczową, bez konieczności instalowania odrębnej pompy zaopatrującej w wodę.
W momencie wybuchu pożaru czujki pożarowe oraz centralny system kontroli inicjują proces gaśniczy na danym obszarze. Woda zostaje uwolniona ze specjalnych dysz ProCon, tworząc efekt mgły. Odpowiednie dysze ProCon są dostępne we wszystkich rozwiązaniach projektowych. Najczęściej instaluje się dysze impulsowe lub obrotowe dysze płasko-stożkowe. Dysze ProCon są rekomendowane do użycia w obszarach, w których notuje się wysoki poziom pyłu i zanieczyszczenia.

## Kotłownie z odzyskiem ciepła

Z perspektywy ochrony ppoż. kotłownie w elektrociepłowniach muszą zostać podzielone na dwie strefy. Pierwszy obszar to strefa, w której znajduje się osprzęt techniczny, tj. pompa zaopatrująca w wodę czy systemy kontroli elektrycznej. Drugi obszar obejmuje kocioł, w którym jest wytwarzana para. Ten obszar cechuje się brakiem zagrożenia pożarowego.
**Zagrożenia:** w obszarach, w których zlokalizowano elektryczny sprzęt kontrolno-monitorujący, spięcia i ogień mogą zostać wywołane przegrzaniem sprzętu. Możliwe są nieszczelności w systemie zaopatrywania w olej na poziomach wszystkich ciśnień (niskiego, średniego i wysokiego). Dotyczy to pomp kotła z wodą oraz systemu kondensacji.
W rezultacie na rozgrzanych powierzchniach może nastąpić samozapłon przeciekającego oleju silnikowego lub zapłon w wyniku zaiskrzenia. W tym momencie ogień może się rozprzestrzeniać na sąsiednie obszary.
**Ochrona przeciwpożarowa:** w obszarach, na których zlokalizowano sprzęt techniczny, używa się automatycznych czujek pożarowych, które skutecznie wykrywają wstępną fazę pożaru. Ponadto lokalizuje się w bliskiej odległości ręczne ostrzegacze pożarowe ROP, umożliwiające aktywowanie gaszenia.
Do szybkiego i skutecznego gaszenia pożaru zaleca się systemy mgły wodnej Minifog ProCon, które wyróżniają się znacznie mniejszym zużyciem wody niż klasyczne systemy zraszaczy. Są one również wyposażone w sygnalizatory świetlne i akustyczne. W bliskim sąsiedztwie kotła montuje się też hydranty i gaśnice.

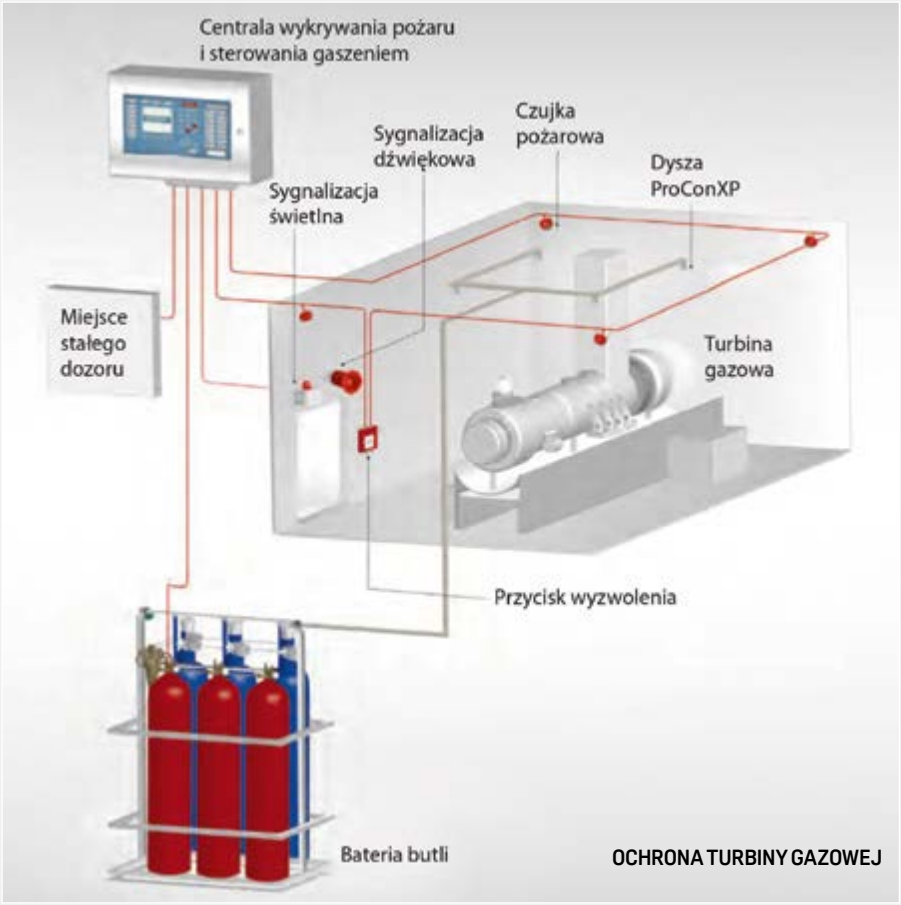
## Turbina gazowa

Sercem każdej elektrociepłowni jest turbina gazowa. Większość elementów jest instalowana pod pokrywą dźwiękoszczelną.
**Zagrożenia:** największe zagrożenie pożarem pochodzi ze strony systemu dostarczania paliwa do palnika oraz systemu olejowego, szczególnie łożyska turbiny znajdującego się w kanale ujściowym. Paliwo i olej mogą łatwo ulec zapłonowi na rozgrzanych powierzchniach.
**Ochrona przeciwpożarowa:** ochrona turbiny gazowej rozpoczyna się od instalacji odpowiedniego systemu detekcji pożaru. Ponieważ w otoczeniu turbiny może dojść do gwałtownego rozprzestrzeniania się otwartych płomieni i znacznego wzrostu temperatury. Najlepszym rozwiązaniem w tych warunkach jest montaż czujek płomienia i temperatury UniVario. Po wykryciu pożaru przez czujki UniVario szybki proces gaszenia bez pozostawiania osadów zapewni system gaszenia gazem $CO_2$. W przypadku największych turbin najczęściej używa się niskociśnieniowych systemów $CO_2$. Dzięki możliwości magazynowania środka gaśniczego w formie płynnej systemy te nie wymagają dużej przestrzeni do instalacji.
Alternatywnym systemem gaśniczym jest dla tego obszaru system wysokociśnieniowej mgły wodnej Minifog ProCon XP. Zużywa on ok. 95% mniej wody w porównaniu do klasycznych instalacji zraszaczowych, co do minimum obniża szkody wywołane akcją gaśniczą.

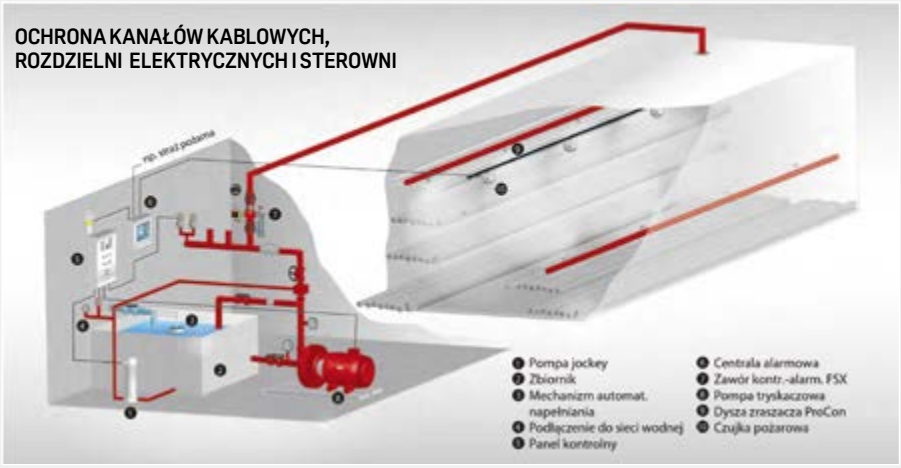
## Kanały kablowe, rozdzielnie elektryczne i sterownie

Do funkcjonowania elektrowni niezbędne są liczne sterownie i kanały kablowe wykorzystywane do dostarczania energii

Minimax Polska
Kiełpin, ul. Ogrodowa 27/ 29
05-092 Łomianki
www.minimax.pl




OCHRONA TURBINY GAZOWEJ




OCHRONA KANAŁÓW KABLOWYCH, ROZDZIELNI ELEKTRYCZNYCH I STEROWNI

## CZUJKI POŻAROWE UniVario

Inteligentne przemysłowe czujki pożarowe UniVario, dzięki solidnej obudowie i technologii produkcji, mogą skutecznie działać w ekstremalnie trudnych warunkach. Reagują na podczerwień i ultrafiolet oraz wysoką temperaturę.
Dzięki modułowej konstrukcji oraz użyciu najnowocześniejszej technologii przetwarzania sygnału spełniają specyficzne wymagania.
Mogą być używane zarówno w pomieszczeniach, jak i na otwartej przestrzeni. Mogą być również bezpośrednio zintegrowane w układzie pętlowym.

oraz przekazywania danych. Ze względów bezpieczeństwa przewody są prowadzone w kanałach kablowych oraz uporządkowane w rozdzielniach i sterowniach.
**Zagrożenia:** główną przyczyną pożaru w takich miejscach jest przegrzanie lub krótkotrwałe spięcie elektryczne zwykle wynikające z przeciążenia. W trosce o odpowiednią ochronę ppoż. należy uwzględnić ryzyko szybkiego rozprzestrzeniania się ognia z powodu ciągów powietrza i dużej liczby przewodów. Pożar, który po izolacji przewodów często się rozprzestrzenia na niedostępne kanały kablowe, może szybko wywołać zakłócenia pracy całej elektrowni.
**Ochrona przeciwpożarowa:** w miejscach, w których są instalowane przewody, stosuje się automatyczne czujki dymu lub systemy zasysające umożliwiające szybkie wykrycie pożaru. Jako system gaśniczy stosuje się MiniFog ProCon, którego niezawodność została potwierdzona w wielu testach pożarowych. Dla ochrony kanałów kablowych instaluje się dysze impulsowe, do ochrony rozdzielni i sterowni – dysze płasko-stożkowe.

## Pomieszczenia kontrolne

Pomieszczenia i systemy kontrolne w elektrociepłowniach są obszarami niezwykle wrażliwymi i kosztownymi.
**Zagrożenia:** pożary wybuchają głównie w następstwie spięć elektrycznych spowodowanych przegrzaniem przewodów lub elementów elektrycznych i elektronicznych.
**Ochrona przeciwpożarowa:** do wykrycia wczesnej fazy pożaru stosuje się punktowe czujki dymu lub system zasysający HELIOS AMX5000. Jako system gaśniczy Minimax zaleca systemy wykorzystujące gazy inertyzacyjne: argon i azot. Inną opcją jest zastosowanie systemu MX 1230 wykorzystującego jako środek gaśniczy Novec 1230. Oba systemy doskonale sprawdzają się w ochronie obszarów wrażliwych i spełniają wszystkie wymagania gaśnicze.

## Ochrona transformatorów

Transformatory działają jako przekaźniki pomiędzy turbinami a siecią energetyczną. Składają się z urządzenia chłodzącego, zbiornika wyrównawczego poziomu oleju oraz izolatorów wypełnionych olejem.
**Zagrożenia:** główną przyczyną pożaru jest możliwość krótkich spięć w transformatorach. Stwarza to ryzyko przegrzania, a olej może się szybko zapalić.

**Ochrona przeciwpożarowa:** w momencie wykrycia przegrzania transformator jest automatycznie wyłączany, co ma zapobiec powstaniu ognia. Podstawą ochrony przeciwpożarowej w przypadku transformatorów jest bezpiecznik Buchhzolza. Gwarantuje on właściwą ocenę potrzeb chłodzenia komponentów. W przypadku przegrzania zostaje uruchomiony automatyczny lub półautomatyczny system zraszaczy wodnych. System zraszaczy Minimax opracowano na podstawie najnowszych badań pod kątem celów ochrony i schematów testowych. Specjalne dysze Viking Model A oraz Model C-1 ułatwiają równomierną, ciągłą dystrybucję wody. Ilość zużywanej wody jest tu znacznie mniejsza niż w standardowych instalacjach zraszaczowych.

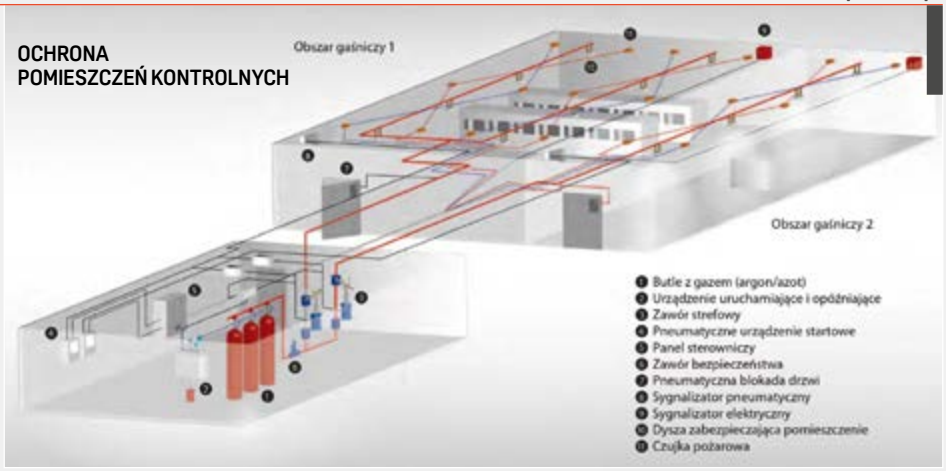
## Serwerownie

Pomieszczenia ze sprzętem IT monitorującym i kontrolującym procesy operacyjne są szczególnie narażone na wybuch pożaru.
**Zagrożenia:** niesprawne lub przegrzane urządzenia elektroniczne mogą być przyczyną wzniecenia ognia i powstania otwartych płomieni.
**Ochrona przeciwpożarowa:** do ochrony przeciwpożarowej w serwerowniach może być stosowany system MX 1230, charakteryzujący się szybkim uwolnieniem środka gaśniczego oraz bezosadowym procesem gaszenia. Dzięki technologii 50-barowej można zastosować instalację wielostrefową. Alternatywnym rozwiązaniem są systemy Oxeo wykorzystujące gazy inertyzacyjne. Zalecana jest również instalacja profesjonalnego systemu detekcji pożaru. Najlepiej w tym przypadku sprawdzają się punktowe czujki dymu lub system czujek zasysających HELIOS AMX5000.

## Pomieszczenia administracyjne

Pomieszczenia administracyjne są użytkowane przez pracowników zazwyczaj w ciągu dnia. Obszary te są puste w określonych przedziałach czasu.
**Zagrożenia:** przyczyną pożarów w pomieszczeniach administracyjnych może być przegrzany lub niesprawny sprzęt elektroniczny. Rozprzestrzeniający się ogień bardzo szybko dociera do innych obszarów budynku. Trudno zagwarantować, że o każdej porze w pomieszczeniach znajduje się personel odpowiedzialny za monitorowanie danego obszaru pod kątem bezpieczeństwa pożarowego, by rozpocząć szybką akcję gaśniczą.
**Ochrona przeciwpożarowa:** skuteczną ochronę zapewniają system wykrywania pożaru i sterowania gaszeniem oraz instalacja tryskaczowa. Poleca się oszczędny pod kątem zużycia wody system gaszenia mgłą wodną Minifog EconAqua, który można połączyć z istniejącą standardową instalacją tryskaczową. Dodatkowo, aby zapewnić szybką, manualną ochronę, instaluje się gaśnice i hydranty ścienne.
Oprogramowanie Inveron firmy Minimax umożliwia śledzenie na ekranie komputera statusu wszystkich systemów zabezpieczeń i ochrony ppoż. Szczególnie w obszernych i rozbudowanych obiektach, takich jak elektrociepłownie, osoby odpowiedzialne mogą szybko monitorować wszystkie istotne dane z systemów wykrywania pożaru oraz systemów gaśniczych i innych systemów wykrywania zagrożenia. Dzięki temu są w stanie podjąć właściwe decyzje w sytuacjach stresowych.
Inveron zapewnia wysokiej jakości informację, łącząc automatycznie wszystkie wiadomości i wydarzenia w przyjazny dla użytkownika interfejs z przejrzystymi grafikami. Bieżący stan punktów kontrolnych może być wyświetlany w formie graficznej, tekstowo lub jako animacja. Odnosi się to do komunikatów zarówno powyżej, jak i poniżej wartości progowych, które są wyświetlane w czasie rzeczywistym.

**Minimax Polska** należy do grupy **Minimax Viking GmbH**, która od ponad 110 lat jest jednym ze światowych liderów w zakresie ochrony ppoż. Jako pierwsza firma w Polsce uzyskała certyfikat VdS. Korzystając z komponentów produkowanych we własnej fabryce, projektuje i wykonuje instalacje w standardach: VdS, FM Global, NFPA, PN-EN.




### CZUJKA HELIOS AMX5000

**Czujka zasysająca Helios AMX5000 ma możliwość inicjowania sygnałów wstępnych, dokonywania oceny zanieczyszczenia, dopasowania poziomu wrażliwości. System charakteryzuje się najwyższym stopniem detekcji nawet najmniejszego zarzewia ognia.**

### CENTRALA FMZ 5000

**Podstawą aktywnej ochrony przeciwpożarowej w elektrociepłowniach jest centrala kontrolno-alarmowa. Minimax oferuje centralę wykrywania pożaru i sterowania gaszeniem FMZ 5000. Tu są zbierane i zapisywane wszystkie sygnały alarmowe (aktywowane ręcznie lub automatycznie) z czujek dymu, temperatury i płomieni oraz systemów gaszenia rozmieszczonych na terenie obiektu. Centrala FMZ 5000 może zostać dowolnie zaprogramowana i funkcjonalnie przystosowana wg potrzeb użytkownika. Jest również dostępna wersja działająca w układzie pętlowym, gdzie na jednym panelu może ze sobą współpracować nawet do 126 jednostek.**

# Problemy związane z bezpieczeństwem pożarowym infrastruktury krytycznej

Pojęcie infrastruktury krytycznej w skali mikro odnosi się przede wszystkim do obiektów przemysłowych, które mają **instalacje i urządzenia niezbędne do utrzymania ciągłości procesów produkcyjnych.**

**Janusz Sawicki**
IBP NODEX

Jednym z głównych zadań przedsiębiorstw jest zabezpieczenie instalacji, których działanie jest niezbędne do funkcjonowania firmy. Aby je zrealizować, trzeba określić zagrożenia oraz instalacje i urządzenia technologiczne, których one dotyczą, a następnie dobrać odpowiednie do zagrożeń rozwiązania zapobiegawcze. Nie sposób opisać rozwiązań i problemów występujących we wszystkich gałęziach przemysłu, ale można je przybliżyć na przykładzie instalacji funkcjonujących w elektrowniach czy w przemyśle chemicznym.

## Awarie

Awarie instalacji, urządzeń i systemów technologicznych są nieuniknione. Dlatego niektóre elementy infrastruktury krytycznej w postaci instalacji i urządzeń, których uszkodzenie lub wypadnięcie z cyklu produkcyjnego może powodować poważne straty materialne, powinny być dublowane lub należy wprowadzić pewną ich nadmiarowość. Przykładem mogą być np. transformatory rezerwowe w procesie wytwarzania i przesyłu energii elektrycznej, zdublowane ciągi nawęglania w elektrowniach, redundantne punkty zasilania zakładów petrochemicznych itp.

Oprócz wskazanych środków podnoszących poziom niezawodności procesu produkcyjnego jednym z ważniejszych środków zapobiegania awariom są bezsprzecznie procedury utrzymania ruchu, tzn. przeglądy, konserwacje, naprawy urządzeń oraz prace modernizacyjne. O koniecznych działaniach dotyczących niezawodności procesu i zastosowaniu odpowiednich środków zaradczych decyduje analiza stopnia ryzyka danej instalacji lub infrastruktury krytycznej na różne zagrożenia.

W procesach produkcyjnych dotyczących wytwarzania i rozdziału energii elektrycznej, przemysłu chemicznego i petrochemicznego, dystrybucji paliw, transportu kolejowego i lotniczego funkcję nadrzędną spełniają skomputeryzowane systemy sterujące i kontrolujące. W stosunku do nich powinny być m.in. wdrożone tzw. poziomy nienaruszalności bezpieczeństwa SIL *(Safety Integrity Level)*. Są one miarą bezpieczeństwa urządzeń elektrycznych, elektronicznych i mechanicznych odnoszącą się również do oprogramowania. Poziomy SIL definiuje norma PN-EN 61508-1.2010: *Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem – Część 1: Wymagania ogólne.* Zastosowanie poziomów SIL, tzn. jaki poziom powinien być przyjęty dla danej dziedziny, określają odpowiednie normy.

## Zdarzenia kryzysowe – wczesna detekcja

Jednym z najczęściej występujących zagrożeń mogących spowodować przerwanie procesu produkcyjnego jest pożar, którego faza rozwinięta ma właściwości niszczące urządzenia, systemy i instalacje technologiczne.

### NAJWAŻNIEJSZE ZAGROŻENIA, W CYKLU PRODUKCYJNYM

- awarie instalacji i urządzeń kluczowych dla procesów produkcyjnych;
- zdarzenia kryzysowe, takie jak pożar, zalania i inne klęski żywiołowe;
- działania o charakterze sabotażowym.

Całkowite zapobieżenie zagrożeniu pożarowemu nie jest możliwe. Każdy proces produkcyjny, zwłaszcza w wymienionych gałęziach przemysłu, niesie poważne ryzyko wystąpienia pożaru. Można je zminimalizować, stosując odpowiednie instalacje i urządzenia detekcji pożaru w jego jak najwcześniejszej fazie.

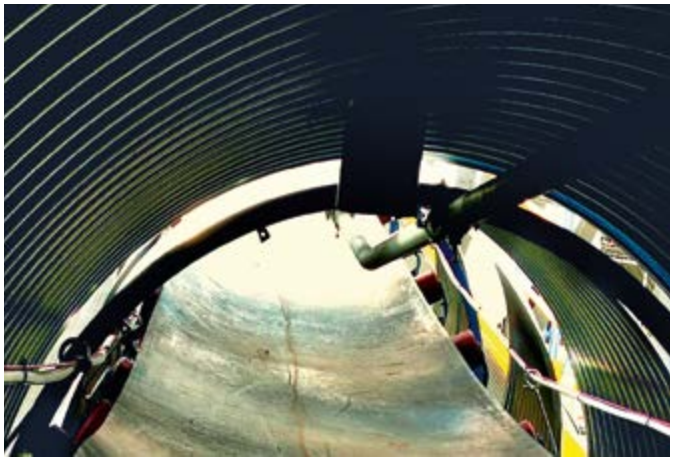
Zastosowanie systemów detekcyjnych w instalacjach przemysłowych jest trudne i powinno być przedmiotem dokładnej analizy oraz znajomości zagrożeń wynikających z charakteru procesów produkcyjnych. Systemy wczesnej detekcji kryteriów pożaru powinny charakteryzować się odpowiednią odpornością na specyficzne oddziaływanie środowiska, w którym pracują, i nie powodować fałszywych alarmów pożarowych.

Oprócz systemów detekcji pożaru niektóre instalacje infrastruktury krytycznej powinno się wyposażać w odpowiednie, dodatkowe urządzenia wykrywające czynniki świadczące o zagrożeniu pożarem. Są to np. czujki wykrywające tlenek i dwutlenek węgla, kamery termowizyjne i kamery wizyjne z możliwością wykrycia dymu oraz inne systemy monitorujące. Takie rozwiązania należy stosować np. w systemach nawęglania w elektrowniach węglowych.

Jeżeli chodzi o elektrownie węglowe, największe zagrożenie pożarem występuje m.in. w ciągach nawęglania, gdzie węgiel jest transportowany za pomocą taśmociągów. Zanieczyszczenie tam występujące może spowodować zablokowanie łożysk krążników, a co za tym idzie nadmierny wzrost ich temperatury i w konsekwencji zapalenie się transportowanego paliwa. Fragment taśmociągu pokazano na *fot. 1.*

## Zdarzenia kryzysowe – tłumienie pożaru

Systemy wczesnej detekcji pożaru – systemy sygnalizacji pożarowej (SSP), odpowiednio dobrane i prawidłowo zainstalowane, wykryją zagrożenie pożarowe w jego bardzo wczesnej fazie. W zależności od prędkości rozwoju pożaru (klasyfikowanej jako parametr $\alpha$ wyrażony w [kW/s$^2$] i przyjmowany do osiągnięcia mocy pożaru równej 1 MW) najbardziej krytyczne są pożary określane jako szybkie i bardzo szybkie. Z reguły cechują się one początkową fazą płomieniową i znaczną energią. Dla tego typu pożarów powinna być wdrożona procedura automatycznego gaszenia za pomocą stałych urządzeń gaśniczych. Wyzwolenie takich instalacji powinno następować niezwłocznie po otrzymaniu sygnału z SSP i przeprowadzeniu procedur bezpieczeństwa, ewakuacji osób z zagrożonego obszaru lub instalacji technologicznej.



**Rys. 1. Fragment taśmociągu nawęglania. Widoczne krążniki, na których przesuwa się taśma (materiały własne)**

**Fot. 2. Zabezpieczenie transformatora za pomocą systemu mgły wodnej (materiały własne)**

Dobór medium gaszącego będzie zależał od materiału palnego, gęstości obciążenia ogniowego oraz usytuowania gaszonej instalacji lub urządzeń (wnętrzowe lub zewnętrzne). Najczęściej stosowanymi instalacjami gaszeniowymi są stałe instalacje gazowe, wodne zraszaczowe i tryskaczowe. Coraz częściej wykorzystuje się instalacje mgły wodnej. Są także stosowane instalacje pianowe, proszkowe w ograniczonym zakresie inertyzujące. Z kolei do gaszenia instalacji technologicznych coraz częściej są stosowane gaśnicze urządzenia aerozolowe.

Niedrogimi i skutecznymi systemami gaśniczymi są instalacje gaśnicze na wysokociśnieniową mgłę wodną. Systemy te charakteryzują się niewielkim zużyciem wody i nieskomplikowanymi instalacjami (w porównaniu do instalacji tryskaczowych). W nowoczesnych rozwiązaniach gaszenia instalacji nawęglania, rozdziału energii czy kablowni coraz częściej wykorzystuje się wysokociśnieniowe systemy mgły wodnej. Przykładem może być sposób rozwiązania gaszenia zewnętrznego transformatora blokowego pokazany na *fot. 2.*

Małe zużycie wody predysponuje mgłę wodną także do gaszenia taśmociągów nawęglania elektrowni. W przypadku uruchomienia tego typu instalacji nie występują straty wtórne spowodowane zalaniem instalacji nawęglania dużą ilością wody, co jest możliwe przy zastosowaniu stałych instalacji gaśniczych wodnych tryskaczowych i zraszaczowych.

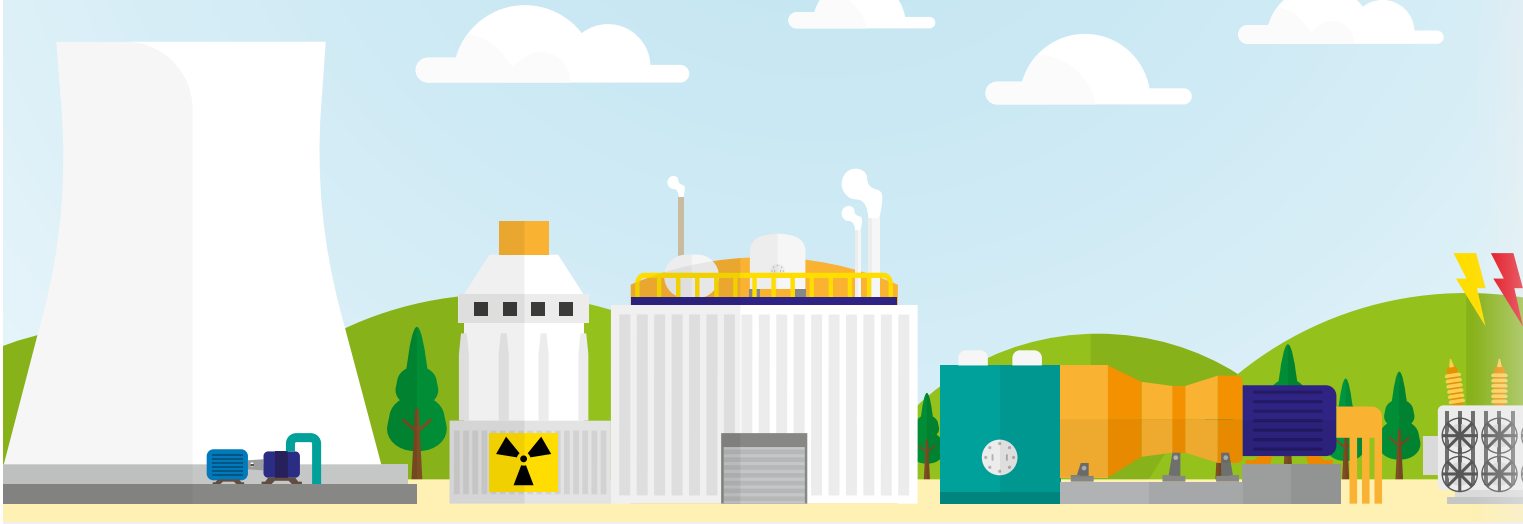
## Podsumowanie

Nie ma jednej recepty na takie zabezpieczenie instalacji i urządzeń infrastruktury krytycznej, która wskazywałaby metody i sposoby wykonania typowych, zunifikowanych systemów bezpieczeństwa w stosunku do danej dziedziny przemysłu.

**W każdym przypadku zabezpieczenie instalacji wskazanych jako infrastruktura krytyczna powinno być przedmiotem wnikliwej analizy i oceny dokonywanej przez specjalistów i ekspertów z danej dziedziny, technologii, zabezpieczeń przeciwpożarowych i ochrony mienia.**

# Głos branży

**Zabezpieczenia techniczne stosowane w obiektach infrastruktury krytycznej muszą spełniać najbardziej wymagające standardy bezpieczeństwa. Wymagają one specyficznych rozwiązań, które dla rynku security stanowią duże wyzwanie.** Istotnym i coraz częściej pojawiającym się problemem są cyberataki. W obliczu zawirowań politycznych i zagrożeń terrorystycznych bezpieczeństwo obiektów i systemów krytycznych dla funkcjonowania państwa jest tematem priorytetowym.



## Hikvision akcentuje specyficzne wymagania

**Łukasz Lik**
dyrektor ds. technicznych, Hikvision Poland

Bezpieczeństwo sektora energetycznego stanowi kluczowy element funkcjonowania państwa. Produkcja i przesyłanie energii elektrycznej jest niczym układ krążenia dla gospodarki. Dotyczy to takich obiektów, jak kopalnie, odwierty gazu i ropy, elektrociepłownie, elektrownie wiatrowe, słoneczne, wodne, sieci przesyłowe czy sieci rozdzielcze. Każdy ma swoją specyfikę, jest narażony na zagrożenia o różnym charakterze. W sektorze wydobywczym np. często znajdują się strefy zagrożone wybuchem. Ich monitorowanie nie tylko zapewnia ochronę przed ingerencją osób niepożądanych, ale też kontroluje procesy technologiczne. Sama kamera również nie może stwarzać zagrożenia. Mmusi być w wykonaniu iskrobezpiecznym Ex spełniającym rygorystyczne normy ATEX i IECEx. W ofercie Hikvision w tym roku pojawi się np. kamera termowizyjna, która umożliwi monitorowanie temperatury w strefach zagrożonych samozapłonem (podajniki węgla).

W przypadku każdego z takich obiektów, jak kopalnie czy elektrownie, bardzo ważną rolę spełnia ochrona obwodowa, często wielopoziomowa: wysoki płot, elementy systemu alarmowego (czujki i bariery) oraz kamery. Przy tego typu zadaniach wręcz niedoścignione są kamery bispektralne. Integracja w jednej obudowie kamery termowizyjnej i kamery wysokiej rozdzielczości pracującej w pasmie widzialnym pozwala na pełną identyfikację zdarzeń. Dzięki funkcjom VCA analizującym obraz termiczny

# Axis stawia na cyberbezpieczeństwo

**Jan T. Grusznic**
**Sales Engineer,**
**Axis Communications**

We właściwym zabezpieczeniu obiektów infrastruktury krytycznej – w skali zarówno mikro, jak i makro – pomaga przedstawienie ich w formie łańcucha wzajemnych powiązań. Sygnały niezależnie docierające z setek czujek liniowych, kamer, czujników temperatury, urządzeń kontroli dostępu lub kontrolujących procesy są trudne, wręcz niemożliwe do zarządzania bez odpowiednich scenariuszy. Wymiana informacji pomiędzy poszczególnymi punktami, automatyzacja i odpowiednio przyznane priorytety to kluczowe elementy zintegrowanego systemu zabezpieczeń w obiektach IK.

Otwarte standardy wymiany informacji między urządzeniami zapewniają wymaganą zarówno współoperacyjność na kolejnych etapach rozbudowy systemu, jak i kompatybilność wsteczną gwarantującą poprawne działanie najnowszych technologii z istniejącymi rozwiązaniami informatycznymi. Nie do przecenienia są również możliwości oprogramowania urządzeń brzegowych, np. kamer, w celu wymiany informacji z systemami do wizualizacji procesów technologicznych lub produkcyjnych (SCADA). Bezpośrednia wymiana danych między – wydawać by się mogło – niepowiązanymi systemami wpływa na zwiększenie bezpieczeństwa załogi i nierzadko efektywności produkcji.

Po wydarzeniach w Estonii w 2007 r., gdy przez trzy tygodnie kraj był nękany tzw. cyberwojną polegającą na blokowaniu dostępu do serwerów instytucji rządowych, świadomość wagi cyberbezpieczeństwa infrastruktury krytycznej zaczęła wzrastać. Oprócz odpowiedniego dostosowania kamer do warunków środowiskowych coraz częściej analizuje się jej zabezpieczenie przed nieautoryzowanym dostępem – fizycznie i programowo.

Z informatycznego czy sieciowego punktu widzenia urządzenie brzegowe jest takim samym końcowym punktem sieci, jak komputery przenośne, stacjonarne czy urządzenia mobilne. W odróżnieniu od nich kamerze IP nie grozi powszechne zagrożenie wynikające z odwiedzania przez użytkowników niebezpiecznych stron, otwierania wiadomości ze złośliwą zawartością czy instalowania niepewnych aplikacji.

Kamera jest jednak urządzeniem sieciowym z interfejsem, który może być narażony na ryzyko nieautoryzowanego dostępu. Dlatego jest separowana od sieci ogólnodostępnej, cały system zarządzania bezpieczeństwem zaś nie ma bezpośredniego dostępu do sieci zewnętrznych, w tym internetu. Wszystkie urządzenia powinny mieć kilkupoziomowy dostęp użytkowników chroniony silnymi hasłami. Ponadto stosuje się filtrację adresów, z których można dokonywać połączeń. Domyślne numery portów są zmienianie, a niewykorzystywane protokoły komunikacyjne – wyłączane.

W instalacjach szczególnie narażonych na ataki wymiana informacji między urządzeniami musi być szyfrowana, a wszystkie urządzenia wymagają dodatkowej autoryzacji za pomocą kluczy lub certyfikatów bezpieczeństwa. Oprogramowanie elementów systemu: kamer, serwerów oraz stacji roboczych jest na bieżąco aktualizowane o publikowane przez producentów poprawki.

Dzięki przynależności do *Building Security In Maturity Model* (BSIMM) zajmującego się rozwojem inicjatyw na rzecz bezpieczeństwa programistycznego Axis nieustannie pracuje nad stosowaniem najlepszych praktyk – weryfikacji projektów i architektury, weryfikacji kodu źródłowego oraz testowania pod kątem znanych problemów z podatnością na ataki. Minimalizuje to ryzyko związane z próbą przejęcia lub zablokowania systemu i powiązanych elementów.

## energetyki

można zredukować liczbę fałszywych alarmów docierających do operatorów.

Należy też uwagę zwracać na zagrożenia wewnętrzne, takie jak ignorancja personelu, sabotaż lub silny stres w wyniku różnych zdarzeń, np. przestępstwo czy atak terrorystyczny. Aby złagodzić skutki lub wręcz wyeliminować wymienione zdarzenia, personel powinien być odpowiednio przeszkolony, a jego kompetencje regularnie sprawdzane. Polityka bezpieczeństwa, standardy i procedury operacyjne, jasno określające zasady i zadania dla wszystkich pracowników i gości, powinny być rygorystycznie przestrzegane.

Sektor energetyczny jest też narażony na różnego rodzaju zjawiska naturalne, takie jak wichury, powodzie, pożary czy roślinność w pobliżu linii przesyłowych. Aby zabezpieczyć ciągłość dostaw energii, newralgiczne punkty systemu energetycznego 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 linii przesyłowych, oględzin słupów i izolatorów. Umożliwiają kontrolę rozkładu temperatury ogniw fotowoltaicznych, łopat wirników turbin wiatrowych czy też weryfikację stanu zadrzewienia w korytarzach linii średniego i wysokiego napięcia. Pomagają w natychmiastowej ocenie sytuacji i podjęciu niezbędnych działań, ograniczając w ten sposób koszty i ryzyko wyłączenia dostaw energii.

Pomysłów na zastosowanie dronów w systemach zabezpieczeń może być znacznie więcej. Jedynym 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. Hikvision umożliwia nie tylko scalenie ich w jeden system, ale także tworzenie redundantnych centrów zarządzania bezpieczeństwem w odniesieniu do dużych w skali kraju obszarów. Wielozadaniowość systemu oraz możliwość centralizacji procesu obserwacji i wykrywania zagrożeń zarówno podnosi standardy bezpieczeństwa, jak i skutecznie redukuje koszty związane z utrzymaniem IK.

# Linc Polska: odpowiednie rozwiązania to podstawa

**Jakub Sobek**
certyfikowany trener techniczny, Linc Polska

W dyskusjach dotyczących bezpieczeństwa infrastruktury krytycznej najczęściej pojawia się temat ochrony perymetrycznej, czyli właściwego zabezpieczenia obiektu przed wtargnięciem intruza z zewnątrz. Protest ekologów z 2007 r., którzy włamali się na teren Elektrowni Bełchatów, by wywiesić na kominie transparent „Stop $CO_2$" czy podobny sprzeciw rok później na terenie Elektrowni Konin pokazują, jak wiele jest do zrobienia. Bardzo niebezpieczną sytuacją są awarie urządzeń pracujących na terenie obiektów infrastruktury krytycznej. Mogą one nie tylko doprowadzić do wstrzymania działalności obiektu, ale także spowodować poważne konsekwencje, takie jak utrata życia lub zdrowia czy skażenie chemiczne, gdy awaria ma miejsce np. na terenie zakładów chemicznych.

Aby zapobiegać tego typu zdarzeniom, warto skorzystać z rozwiązań termowizyjnych. Coraz częściej są one stosowane w automatyce, utrzymaniu ruchu i weryfikacji działania poszczególnych elementów infrastruktury. Do takich zastosowań branża oferuje dwa rodzaje rozwiązań. Pierwsze to kamery stałopozycyjne, przez cały czas skierowane na pracujące urządzenia. W polu widzenia kamery definiuje się wówczas obszary lub punkty pomiarowe. Gdy zostaną przekroczone ustalone progi temperaturowe, generowane jest zdarzenie alarmowe. Takie działanie pozwala na bardzo wczesnym etapie wykryć wadliwie działające elementy automatyki i wykonać czynności serwisowe, nie dopuszczając do awarii. Dostrzeżenie przegrzewającego się elementu zapobiega także pożarowi.

Drugim rodzajem kamer pomiarowych są urządzenia umieszczone na głowicach obrotowych. Ich ruch programuje się w taki sposób, że kamera jest obracana na zdefiniowane punkty, wykonując pomiary temperaturowe w zadanych odstępach czasu. To rozwiązanie z kolei pozwala na wykonywanie pomiarów na znacznie większym obszarze. Wszystkie dane są gromadzone w bazach danych i dzięki oprogramowaniu analitycznemu można wykrywać np. trendy temperaturowe. Jeśli temperatura na badanym elemencie stale rośnie w wybranym czasie, można zakładać, że wkrótce przekroczy zdefiniowany próg alarmowy.

Kamera pomiarowa na głowicy obrotowej może być także wsparciem systemu perymetrycznego. Przykład: w obiekcie znajduje się światłowodowy system napłotowy wykrywający intruza. Informacja o detekcji wtargnięcia do obiektu jest przesyłana do kamery, która ustawia się na odpowiedni fragment ogrodzenia. Dzięki temu operator systemu monitoringu może szybko zweryfikować zdarzenia alarmowe i na podstawie obrazu wideo podjąć decyzję, jakie działania należy podjąć. Wykorzystanie w takim przypadku kamer termowizyjnych pozwala znacznie zredukować liczbę kamer CCTV. Jedna kamera termowizyjna daje wiele korzyści i może być źródłem dużych oszczędności.

Wyposażenie obiektów IK w odpowiednie rozwiązania techniczne oraz podjęcie w kolejnych latach działań edukacyjnych i uświadamiających pozwoli zwiększyć poziom bezpieczeństwa tych obiektów. Wdrażanie zasad ochrony nie jest procesem krótkim i łatwym, dlatego wysiłki na rzecz podnoszenia bezpieczeństwa powinny być podejmowane każdego dnia.

# Grupa Żywiec: o bezpieczeństwie w zakładzie przemysłowym

**Jacek Tobiasz**
Security Manager, Grupa Żywiec (Heineken)

Nowoczesny model zapewnienia bezpiecznego środowiska dla rozwoju zakładu przemysłowego nie może się ograniczać do nawet najbardziej sumiennie wykonywanej pracy ochrony fizycznej. Aby zapewnić przyjazne i bezpieczne środowisko działania zakładu, nie można budować go „obok" działalności operacyjnej i oczekiwać, że ryzyko zostanie zminimalizowane. Bezpieczeństwo w zakładzie przemysłowym to nie tylko zasady BHP, których stosowanie powinno zapewniać pracownikom bezpieczne warunki pracy. Bezpieczeństwo ma także wymiar biznesowy. Przy opracowaniu audytu modelu bezpieczeństwa działającego już podmiotu, np. dużej fabryki, należy wskazać możliwe i ekonomicznie uzasadnione propozycje poprawy tego modelu we wszystkich obszarach ryzyka. Efektem takich działań powinno być zmniejszenie sumy wszystkich strat będących następstwem świadomego działania (oszustwo) lub braku działania (niedbalstwo). Przy czym oba te przypadki mogą mieć źródło wewnątrz przed-

# Sztuka zabezpiezpieczenia ppoż. według Schrack Seconet

**Grzegorz Ćwiek**
prezes,
Schrack Seconet Polska

Z punktu widzenia sztuki zabezpieczenia przeciwpożarowego obiektów budowlanych infrastruktury krytycznej obowiązują niemal identyczne zasady i praktyki jak w przypadku każdego zwykłego obiektu. Bezpieczeństwo pożarowe regulują podstawowe akty prawne – rozporządzenia Ministra Infrastruktury oraz Ministra Spraw Wewnętrznych i Administracji. Najważniejsze dla zabezpieczeń przeciwpożarowych są jednak wskazówki dodatkowe i wytyczne pozwalające znacznie lepiej dobrać właściwe środki bezpieczeństwa. Szczególną uwagę należy zwrócić na najnowszy dokument będący aktualizacją Narodowego Programu Ochrony Infrastruktury Krytycznej.

Publikacja NPOIK to doskonały krok w kierunku uświadomienia wielu interesariuszom konieczności szerszego spojrzenia na specyfikę zapewnienia bezpieczeństwa (pożarowego) obiektów infrastruktury krytycznej. W odróżnieniu od ustaw i rozporządzeń, do których jesteśmy przyzwyczajeni od lat, a które są napisane mało zrozumiałym językiem i nie dają przejrzystych wskazówek nawet specjalistom, dokument NPOIK promuje nowoczesne zasady zarządzania procesem zapewnienia bezpieczeństwa. Jego konstrukcja w dużej mierze opiera się na wykorzystaniu praktyk i integracji działań zaczerpniętych z systemów zarządzania jakością, bezpieczeństwem, środowiskiem, ciągłością działania oraz zarządzania ryzykiem.

Zapewnienie bezpieczeństwa ppoż. w obiektach budowlanych o szczególnym znaczeniu (jako elementu infrastruktury krytycznej) wymaga innego podejścia niż w przypadku obiektów spoza tego obszaru. Trzeba dokonać bardziej szczegółowej analizy związków między zagrożeniami, podatnością obiektów na owe zagrożenia oraz skutkami, jakie zdarzenia o charakterze kryzysowym mogą wywołać dla bezpieczeństwa np. ludności całego regionu. Ciężar strat wywołanych pożarem takiego obiektu jest nieporównywalnie większy niż np. niewielkiego obiektu niebędącego elementem IK. Standardowe podejście do projektowania, instalowania i konserwacji systemu sygnalizacji pożarowej nie wystarczy.

Przykładem nowoczesnego (tak potrzebnego dzisiaj także poza obszarem infrastruktury krytycznej) podejścia do tworzenia zabezpieczeń ppoż. są np. wytyczne dotyczące zapewnienia bezpieczeństwa technicznego. NPOIK promuje budowę systemów odpornych na zakłócenia (tzw. rezylientnych), a zatem nie tylko działających sprawnie na co dzień, ale także pozwalających na szybkie i sprawne odbudowanie swoich właściwości po wystąpieniu zdarzenia krytycznego, np. pożaru czy awarii.

## GŁOS UŻYTKOWNIKA

siębiorstwa, jak też nie być w żaden sposób powiązane z jego pracownikami i współpracownikami.

Jak pokazuje praktyka, różne profile i modele organizacji produkcji oraz całego łańcucha dostaw i funkcjonowania magazynów wyrobu gotowego dowodzą, że to, co nęka jeden zakład, w innym w ogóle nie występuje. Należy więc przygotować optymalny model zapewniający maksymalny poziom bezpieczeństwa i minimalne rodzaje ryzyka, uwzględniając indywidualne cechy konkretnego przypadku.

Na pewno nie wystarczy zapewnienie szczegółowej kontroli wejść i wjazdów ani restrykcyjne kontrolowanie osób, dokumentacji i transportów opuszczających zakład. Taki model będzie po pierwsze kosztowny, bo wymaga zatrudnienia wielu pracowników ochrony, po drugie zaś nie wyeliminuje problemów ani strat, ponieważ nie zagwarantuje ujawnienia nieprawidłowości.

Początek procesu zapewnienia bezpieczeństwa musi mieć zatem źródło w dogłębnej analizie dostępnych, a czasem rozproszonych danych.

Analizie podlegają takie informacje, jak wyniki inwentaryzacji magazynów gotowego wyrobu, magazynów półproduktów, strat produkcyjnych (efektywności), metody rozliczania stanów produkcyjnych i tworzenia stanów magazynowych, a także stosowane systemy rozliczeń, odpowiedzialność dostawców, przewoźników, podwykonawców, systemy autoryzacji i potwierdzeń wykonania usług przez podmioty zewnętrzne, co zbuduje świadomość pracowników w obszarze możliwych fraudów zdarzających się w podobnych organizacjach.

Wszystko to będzie stanowiło punkt wyjścia do wypracowania skutecznego modelu dla efektywnego i nowoczesnego zarządzania bezpieczeństwem.

GŁOS UŻYTKOWNIKA

# innogy Polska o cyberatakach

**Janusz Syrówka**
Dział Bezpieczeństwa
innogy Polska (dawniej RWE)

Ostatnio coraz częściej mówi się o cyberatakach na szeroko rozumiany sektor energetyczny, chociażby za sprawą udanego ataku na jedną z elektrowni ukraińskich, lecz przestępczość cyfrowa to niejedyne zagrożenie dla bezpiecznego funkcjonowania firm energetycznych. Ich najważniejszym zadaniem jest zapewnienie ciągłości dostaw energii, a to wymaga dużego zaangażowania logistycznego na wypadek potencjalnych sytuacji kryzysowych. Pozwala zminimalizować skutki tradycyjnych zagrożeń, takich jak awarie infrastruktury, działania sił natury, a także skutecznie zwalczać nowe formy zagrożeń.

W tym aspekcie można uznać, że nowe zagrożenia, takie jak cyberprzestępczość, stanowią wyzwanie dla firm z sektora energetycznego i są bodźcem mobilizującym do udoskonalania dotychczasowych mechanizmów obronnych. Rola technicznego budowania systemów zabezpieczeń wydaje się oczywista w kontekście tego typu zagrożeń. Wart omówienia, ze względu na jego częste bagatelizowanie pomimo znaczącej roli w procesie bezpieczeństwa, jest czynnik ludzki. Świadomość niebezpieczeństw oraz umiejętne i odpowiednio wczesne rozpoznanie sygnałów świadczących o nadchodzącym zagrożeniu należy uznać za istotny czynnik zapobiegania tego typu sytuacjom.

Oprócz działań systemowych firma innogy Polska podejmuje liczne inicjatywy, których celem jest podniesienie świadomości pracowników w zakresie zagrożeń związanych z cyberprzestępczością. Obecnie w firmie trwa kampania *Human Firewall*, której tytuł podkreśla ważną rolę człowieka w przeciwdziałaniu cyberatakom w sektorze energetycznym. Obejmuje ona m.in. prezentację zagrożeń na żywo, wykorzystanie modułów e-learningowych czy konkursy. Co istotne, nie ogranicza się do zachowań ściśle związanych z miejscem pracy, ale porusza też problematykę bezpieczeństwa w sieci podczas korzystania z niej w środowisku prywatnym.

Budowanie świadomości bezpieczeństwa cyfrowego w sferze prywatnej przekłada się wprost na podniesienie jego standardów w miejscu pracy, i odwrotnie.

# Dahua: specyficzne rozwiązania dla infrastruktury krytycznej

**Marian Maroszek**
Sales Support Engineer,
Dahua Technology Poland

W dzisiejszym świecie jesteśmy otoczeni coraz większą liczbą różnych systemów zabezpieczeń. Technologia mająca zapewnić poczucie bezpieczeństwa pojawia się w miejscach, o których jeszcze kilka lat temu nikt nawet by nie pomyślał. Nie inaczej jest w przypadku infrastruktury krytycznej.

Mnogość rozwiązań stosowanych w priorytetowych obiektach jak dworce kolejowe czy lotniska jest całkiem duża, skupię się tylko na niewielkim ich fragmencie dotyczącym telewizji dozorowej.

Podstawowym ogniwem w systemach CCTV od lat są kamery dozorowe, przeżywające w ostatnim czasie dynamiczny rozwój. Przetworniki obrazu w połączeniu z wyspecjalizowanymi procesorami obróbki sygnałów pozwalają na rejestrację materiału w niesprzyjających warunkach, przy znikomym poziomie oświetlenia. Dzięki takim technologiom, jak Starlight stało się możliwe generowanie użytecznego i często kolorowego obrazu w warunkach, które jeszcze kilka lat temu wymagały używania dodatkowych źródeł światła czy promieniowania IR.

Nieco mniej rozpowszechnioną grupą urządzeń stosowaną w systemach monitoringu wizyjnego są kamery termowizyjne. Ich cena dotychczas stanowiła sporą barierę, jednakże i tutaj następuje ogromny progres. Na rynku pojawiają się coraz doskonalsze niechłodzone matryce bolometryczne, których cena systematycznie spada, co powoduje powszechne stosowanie termowizji.

Sprawdzającym się rozwiązaniem są kamery integrujące w jednej obudowie dwa moduły: termowizyjny i optyczny. Wszechstronność takiego urządzenia sprawia, iż monitoring dużych przestrzeni zewnętrznych staje się nie tylko możliwy i wygodny, ale także bardzo precyzyjny i skuteczny. W przypadku infrastruktury krytycznej, np. lotnisk, ma to kluczowe znaczenie.

Maksimum możliwości dwóch wymienionych rozwiązań zapewnia funkcja inteligentnej analizy obrazu. Percepcja operatorów jest ograniczona, z pomocą przychodzą im zautomatyzowane systemy analizy obrazu z kamer. O ile kiedyś możliwości oprogramowania kończyły się na prostej detekcji ruchu, o tyle dziś nie jest rzadkością wykrywanie i rozpoznawanie twarzy, tworzenie linii perymetrycznych czy wykrywanie pożarów. Niewątpliwie branża CCTV jeszcze nieraz zaskoczy, dostarczając wiele ciekawych i nowatorskich rozwiązań.

a&S POLSKA

# ŚNIADANIE EKSPERTÓW

# Bezpieczeństwo infrastruktury krytycznej i obiektów przemysłowych

## dyskusja o bezpieczeństwie w luźnej atmosferze

**ZAPRASZAMY PRZEDSTAWICIELI:**

- security managerów obiektów infrastruktury krytycznej
- security managerów obiektów przemysłowych
- przedstawicieli firm i instytucji o strategicznym znaczeniu dla funkcjonowania państwa:
  m.in. zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowych, ochrony zdrowia, transportowych, ratowniczych oraz produkcji, składowania i stosowania substancji niebezpiecznych

**12 maja 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 · BOSCH · alhua TECHNOLOGY · Hanwha Techwin · HIKVISION · Linc Polska Sp. z o.o. · OPTEX · SASMA · SCHRACK SECONET


# BEZPIECZEŃSTWO CYBERNETYCZNE SYSTEMÓW STEROWANIA PRZEMYSŁOWEGO

Incydenty komputerowe i działanie hakerów kojarzą się zazwyczaj z atakami na komputery osobiste, strony internetowe i ewentualnie na systemy niektórych przedsiębiorstw: banków, sklepów internetowych czy firm medycznych. **Mają one na celu przede wszystkim skompromitowanie danej instytucji** (podmiana zawartości strony www lub jej wyłączenie), **kradzież danych bądź wymuszenie wpłaty okupu w zamian za odzyskanie dostępu do własnych danych** (*ransomware*).

**Marek Sajdak**
prezes Aurora Intelligence

Takie rozumienie celu działań przestępców komputerowych jest zrozumiałe, gdyż opiera się na codziennym doświadczeniu wzmacnianym bieżącymi doniesieniami medialnymi. Mówimy tu o tzw. obszarze IT, czyli technologii informacyjnej (*information technology*).

W życiu codziennym bardzo często spotykamy się z rozwiązaniami IT, wykonując chociażby przelewy bankowe przez internet, przygotowując prezentację w PowerPoincie czy tworząc sprawozdania w arkuszu Excel.
To tylko jedna strona nowoczesnego świata technologii. Obok IT codzienne życie wspiera obszar technologii OT, czyli technologii operacyjnej (*operational technology*). OT obejmuje rozwiązania (*systemy*) przeznaczone do sterowania procesami fizycznymi. Należą do nich systemy sterowania dla elektrowni, sieci energetycznej czy infrastruktury kolejowej. Systemy OT kontrolują zwrotnice, pompy czy zawory. Bez technologii OT nie mielibyśmy w domu prądu, wody, nie funkcjonowałyby stacje benzynowe, nie jeździłyby pociągi, nie latałyby samoloty.

## Ataki na systemy OT/ICS

Zagrożenie atakami hakerskimi dotyczy nie tylko obszaru IT, ale także obszaru OT. Dla przestępców motywowanych finansowo głównym celem ataku są oczywiście systemy IT, gdyż atak jest tańszy i łatwiejszy do przeprowadzenia, a przy tym można się szybko wzbogacić, kradnąc dane czy wymuszając okup. Dla przestępców motywowanych ideologicznie bądź wspieranych przez rządy celem są także systemy OT. Skuteczny atak na system sterowania przemysłowego może oznaczać wyłączenie dostaw energii elektrycznej, wody i gazu, katastrofy komunikacyjne (kolejowe i lotnicze), awarie oczyszczalni ścieków, zaburzenie procesów produkcyjnych czy katastrofy przemysłowe, np. w rafineriach. Ataki na infrastrukturę OT są istotnym elementem w tzw. wojnie hybrydowej, czyli strategii wojennej łączącej działania konwencjonalne (atak wojsk regularnych), nieregularne (tzw. zielone ludziki) oraz cybernetyczne (ataki przez internet, dezinformacja). W nowoczesnej wojnie atak cybernetyczny na sieci komputerowe przeciwnika, połączony z atakiem na infrastrukturę sterowania w przemyśle, będzie pierwszym etapem poprzedzającym atak militarny.

## Dyrektywa NIS

Zagrożenia dotyczące systemów przemysłowych stanowiących istotny element infrastruktury krytycznej państw zostały dostrzeżone przez ustawodawcę europejskiego. W 2016 r. została przyjęta dyrektywa NIS (Dyrektywa Parlamentu i Rady UE dot. środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii). Zakłada ona poszerzenie współpracy państw członkowskich UE w kwestii cyberbezpieczeństwa. Dokument definiuje obowiązki, jakim będą podlegać operatorzy kluczowych usług (przedsiębiorcy z sektorów energetyki, transportu, bankowości i infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę pitną, infrastruktury cyfrowej) oraz dostawcy usług cyfrowych (internetowe platformy handlowe, wyszukiwarki, usługi przetwarzania w chmurze).
Na wybrane podmioty dostarczające kluczowe usługi będą nałożone dwa obowiązki. Pierwszy nakazuje wprowadzenie środków ochrony (technicznych i organizacyjnych) zależnych od poziomu ryzyka, drugim jest konieczność raportowania incydentów. Państwa członkowskie muszą powołać zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), zespoły krajowe CSIRT natomiast będą tworzyły sieć współpracy wspieraną organizacyjnie (sekretariat) i merytorycznie przez ENISA (Europejska Agencja Bezpieczeństwa Sieci i Informacji).
CSIRT, CERT oraz zespół reagowania na incydenty komputerowe oznacza grupę osób składającą się z analityków bezpieczeństwa, zorganizowaną w celu opracowywania, rekomendowania i koordynowania działań, których zadaniem jest wykrywanie, powstrzymywanie i zwalczanie skutków wynikających z incydentów, a także pozyskanie informacji na temat istoty tych incydentów.
Zespoły narodowe CSIRT zajmą się transgranicznymi problemami bezpieczeństwa i sposobami skoordynowanego reagowania na zagrożenia. Swoje zadania uzyskała także Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA), która będzie koordynować współpracę między państwami w ramach sieci CSIRT, a także wspierać państwa członkowskie i Komisję Europejską poprzez udostępnianie specjalistycznej wiedzy, doradztwo i ułatwianie wymiany najlepszych praktyk.
W ramach sieci CSIRT będą wymieniane informacje o incydentach i to ten obszar można uznać za priorytetowy. Incydenty cybernetyczne bardzo często mają charakter międzynarodowy, a technologie stosowane przez przestępców są wykorzystywane bezpośrednio do ataków na infrastrukturę wielu państw. Zapewnienie wymiany informacji o incydentach między krajowymi CSIRT pozwoli na skuteczniejszą reakcję na tego typu działania.

W nowoczesnej wojnie atak cybernetyczny na sieci komputerowe przeciwnika, połączony z atakiem na infrastrukturę sterowania w przemyśle, będzie pierwszym etapem poprzedzającym atak militarny.

### PRZYKŁADY UJAWNIONYCH ATAKÓW NA SYSTEMY STEROWANIA PRZEMYSŁOWEGO W OSTATNICH LATACH

- **2010 r.** **Iran**, atak robaka Stuxnet powodujący zmianę parametrów wirówek do wzbogacania uranu, w efekcie ich uszkodzenie
- **2014 r.** **Niemcy**, atak na systemy sterowania w hucie stali, który zakończył się znacznymi stratami finansowymi
- **2015 r.** **Ukraina**, atak na dostawcę energii elektrycznej Ukrenergo, w którego wyniku 250 000 gospodarstw nie miało prądu elektrycznego
- **2016 r.** **Ukraina**, atak na infrastrukturę energetyczną, skutkujący odcięciem 200 MW energii dla Kijowa (co stanowiło 1/5 zapotrzebowania na energię stolicy Ukrainy)

## STRATEGIA CYBERBEZPIECZEŃSTWA RZECZYPOSPOLITEJ POLSKIEJ NA LATA 2017–2022

**Cel główny**

Zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych.

**Cele szczegółowe**

1. Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa.
2. Wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom.
3. Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni.
4. Zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa.

### Strategia cyberbezpieczeństwa RP

Wymiana informacji pomiędzy krajami na temat incydentów będzie możliwa, pod warunkiem że sieć wymiany zostanie utworzona w każdym kraju członkowskim. Zgodnie ze „Strategią Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022", przyjętą w marcu 2017 r. przez Ministerstwo Cyfryzacji, konieczne jest utworzenie lub rozbudowa krajowej sieci CSIRT (CSIRT narodowy, CSIRT sektorowe, komercyjne i przedsiębiorców), które wymieniałyby kluczowe informacje o zagrożeniach bezpieczeństwa i incydentach w danym sektorze bądź dziale administracji rządowej. Idąc od poziomu międzynarodowego, poprzez poziom krajowy (CSIRT krajowy), poziom sektorowy (sektorowe zespoły CSIRT), dochodzimy do zespołów na poziomie przedsiębiorców, czyli zespoły CSIRT funkcjonujące w przedsiębiorstwach. Zespół CSIRT w przedsiębiorstwie musi być wyposażony w narzędzia zbierania i raportowania informacji o incydentach. Takim miejscem powinien być SOC, czyli Operacyjne Centrum Bezpieczeństwa (*Security Operations Center*). Dla podkreślenia funkcji związanej z bezpieczeństwem informacji często wykorzystuje się także określenie CSOC (*Cyber Security Operations Center*).

Obok IT codzienne życie wspiera OT, czyli technologia operacyjna. To rozwiązania przeznaczone do sterowania procesami fizycznymi, np. w elektrowniach czy infrastrukturze kolejowej.

### Operacyjne Centrum Bezpieczeństwa

CSOC jest wyposażony w narzędzia do zbierania informacji o zdarzeniach (logów) z urządzeń sieciowych, systemów IT (CRM, ERP, billing itd.), systemów bezpieczeństwa (firewall, IPS, IDS, antywirusy, systemów ATP), a także z systemów przemysłowych (ICS/SCADA). Tradycyjne metody ochrony infrastruktury IT polegające na rozmieszczeniu rozwiązań firewall, IPS, IDS czy antywirusy obecnie nie zapewniają skutecznej ochrony infrastruktury. Dlatego też kilka lat temu zaczęto stosować zaawansowane rozwiązania przeciwdziałania atakom APT (*Advanced Persistent Threats*) wyposażone w mechanizmy tzw. *sandboxingu*, czyli zdolność do uruchamiania w wydzielonym, kontrolowanym środowisku pobieranych z internetu załączników w poszukiwaniu *malware*, czy od niedawna sondy sieciowe wyposażone w mechanizmy AI (*Artificial Intelligence*). Takie rozwiązania nadal nie zapewnią pełnego bezpieczeństwa, gdyż każdy system może uznać dane zachowanie użytkownika czy ruch sieciowy za legalny. Dopiero korelowanie informacji o zdarzeniach pochodzących z różnych systemów i weryfikacja uzyskiwanych informacji ze źródłami zewnętrznymi, tzw. *Threat Intelligence*, pozwala na wykrycie skomplikowanych zaawansowanych ataków.

Kluczowym elementem takiego podejścia jest właśnie CSOC stanowiący miejsce dowodzenia cyberbezpieczeństwem w przedsiębiorstwie. Gdy przedsiębiorca w swojej infrastrukturze posiada nie tylko systemy IT, ale także OT/ICS, sprawa zaczyna się komplikować. Infrastruktura OT/ICS powinna zostać wydzielona z sieci IT, co kilkadziesiąt lat temu było normą. Dzisiaj następuje szybka konwergencja sieci IT/OT, co powoduje, że przestępca może łatwiej dostać się do sieci OT, włamując się najpierw do sieci IT z poziomu internetu. Jednym z rozwiązań problemu jest zastosowanie odpowiednich rozwiązań firewall pozwalających na wymianę ruchu między sieciami w ściśle zdefiniowanych ramach bądź zastosowanie tzw. *data diode*, czyli rozwiązań firewall pozwalających na przepływ danych tylko w jedną stronę, np. danych pomiarowych z sieci ICS do sieci IT. Na właściwą separację przepływu danych między sieciami IT i OT należy nałożyć wspomniane mechanizmy logowania zdarzeń, czyli CSOC. Ograniczenie się do korelacji zdarzeń jedynie z sieci IT powoduje, że nie będziemy świadomi nieautoryzowanych operacji w sieciach OT. Wybór dostawcy rozwiązań CSOC powinien uwzględniać zdolność rozwiązań CSOC do analizy zdarzeń z protokołów infrastruktury OT.

Posiadanie standardowych zabezpieczeń infrastruktury jest nadal warunkiem niezbędnym do ochrony przed atakami, niemniej Operacyjne Centrum Bezpieczeństwa Cybernetycznego CSOC pozwala na skoordynowane zarządzanie bezpieczeństwem, pozyskiwanie i wykorzystywanie informacji ze źródeł zewnętrznych (np. sieć CSIRT w ramach dyrektywy NIS). Jest też warunkiem koniecznym dla przedsiębiorców infrastruktury krytycznej przy wypełnianiu dyrektywy NIS na poziomie krajowym.

CYBERBEZPIECZEŃSTWO SYSTEMÓW KONTROLI DOSTĘPU

# Skutki finansowe dla przedsiębiorstw i instytucji

Anna Twardowska

## Cyberzagrożenia na świecie

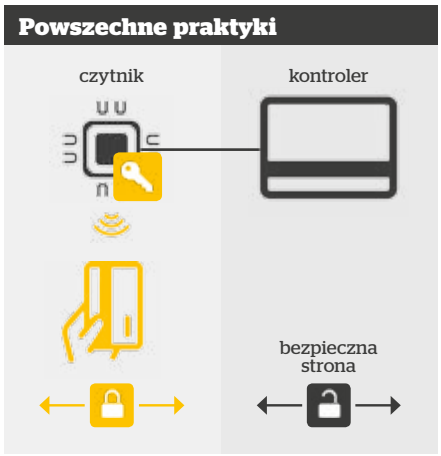
Rok 2016 uświadomił, że cyberzagrożenia przestały być zjawiskiem odległym, które bezpośrednio nas nie dotyczy. Był pełen doniesień dotyczących cyberataków. Serwis Yahoo w grudniu 2016 r. przyznał się do wycieku danych miliarda użytkowników, ataki DDoS spowodowały awarię serwisów Twitter i Spotify, a w maju z banku centralnego w Bangladeszu ukradziono 81 mln dolarów. Jednego z najbardziej spektakularnych ataków dokonał malware Mirai, który zainfekował prawie 500 tys. urządzeń. Na polskim podwórku też zanotowano wiele zdarzeń, z atakiem na stronę internetową KNF na czele. Od pewnego czasu można zauważyć tendencję polegającą na wykorzystywaniu do ataków urządzeń podpiętych do internetu, np. kamer czy innych urządzeń Internetu Rzeczy (IoT). Zagrożone są wszystkie systemy sieciowe, a zatem także systemy kontroli dostępu (SKD), systemy VMS, systemy automatyki budynkowej (BMS) czy systemy sterowania procesami produkcyjnymi (SCADA/ICS).

## Systemy kontroli dostępu a zagrożenia współczesne

Świadomość potrzeby zabezpieczania systemów IT przed cyberatakami jest obecnie dość powszechna. Działy IT w coraz większej liczbie organizacji mają już opracowane zasady postępowania i narzędzia chroniące przed tego typu zagrożeniami. Z kolei branża security jeszcze nie wypracowała procedur ani nie wdrożyła metod przeciwdziałania im. Wraz z rozwojem systemów kontroli dostępu (SKD) i rozpowszechnieniem technologii IP bezpieczeństwo tych systemów nabrało nowego wymiaru. Większość podstawowych urządzeń KD wykorzystuje standardową architekturę IT: serwery, systemy operacyjne, sieci LAN/WAN. Są więc narażone nie tylko na próbę podrobienia karty służącej do otwarcia drzwi, ale także na ataki z poziomu protokołu TCP/IP. Systemy kontroli dostępu, podobnie jak wszystkie elementy architektury IT, powinny być zabezpieczane tymi samymi metodami. Czy jest to praktyka powszechna? Kontrolery stosowane obecnie w SKD są urządzeniami bardzo wydajnymi, wyposażonymi w system operacyjny, procesor, pamięć i podłączenie do sieci LAN, są również bliskie środowisku IT. Kamera IP, drukarka, a nawet cały system kontroli dostępu mogą być, tak jak komputer, pierwszym punktem podatnym na atak hakerski.

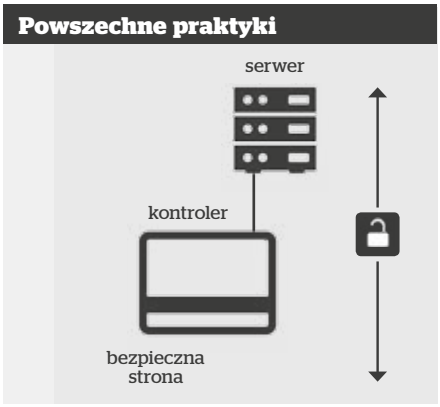
## Pierwsze słabe ogniwo – karta

Słabym punktem SKD jest często standard stosowanych kart. Rodzina standardów ISO/IEC 14443 reguluje zasady dotyczące budowy kart zbliżeniowych.

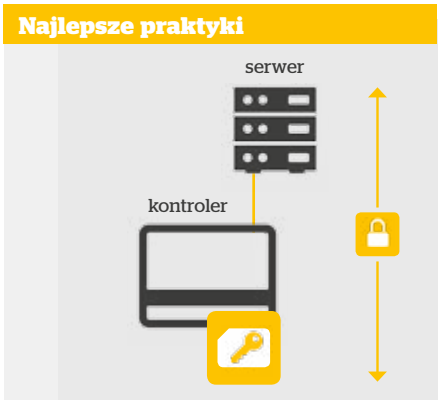



Rys 1. Klucz DESfire jest przechowywany w czytniku


Rys. 2. Przechowywanie klucza DESfire po bezpiecznej stronie drzwi, na kontrolerze




Rys. 3. Styk kontrolera z serwerem, bez użycia certyfikatów do uwierzytelnienia połączenia




Rys. 4. Połączenie uwierzytelnione za pomocą certyfikatu znajdującego się fizycznie na kontrolerze

Jednym z pierwszych był standard Unique o częstotliwości pracy 125 KHz. Charakteryzuje się zapisanym w pamięci jawnym numerem seryjnym, który bardzo łatwo skopiować. Z tego powodu karty Unique są zastępowane przez Mifare, czyli karty bezdotykowe o częstotliwości pracy 13,56 MHz. Najbardziej popularną kartą jest Mifare Classic, nagminnie stosowana w polskich systemach KD. Pierwsze doniesienia o procederze ich klonowania sięgają 2007 r. Proceder kopiowania karty może się odbyć bez wiedzy jej posiadacza, wystarczy bowiem zbliżyć ją na odległość od kilku do kilkunastu centymetrów. Zupełnie inaczej sprawa bezpieczeństwa przedstawia się w przypadku kart Mifare Desfire. Standard ten charakteryzuje się dużą szybkością transmisji danych oraz najwyższym obecnie poziomem bezpieczeństwa danych opartym na sprzętowych mechanizmach kryptograficznych DES, 3DES, AES, 3KDES (tylko w wersji DESFire EV1), co ogranicza ryzyko nadużyć. Karty Unique i Mifare Classic wciąż są bardzo popularne w Polsce w przedsiębiorstwach z sektorów energetycznego i finansowego – dwóch najbardziej narażonych na cyberataki. Projektowanie systemów, ich wdrożenie i realia finansowe sprawiają, że często rezygnuje się z określonego poziomu zabezpieczeń. W rezultacie uzyskuje się system, który tylko pozornie chroni przed dostępem osób niepowołanych. Oprócz prostego klonowania kart organizacje, szczególnie z sektora infrastruktury krytycznej, są narażone także na zaawansowane próby przechwycenia dostępu do chronionych obiektów. Powszechnie stosowaną praktyką jest przechowywanie klucza DESfire na czytniku, zatem wrażliwe dane są dostępne na zewnątrz i tam jest on deszyfrowany (*rys. 1*). W Europie coraz częściej zaleca się stosowanie kluczy DESFire, które muszą być składowane po bezpiecznej stronie – fizycznie na kontrolerze (*rys. 2*).

Cyberatakami są zagrożone wszystkie systemy sieciowe, a zatem także systemy kontroli dostępu (SKD), systemy VMS, systemy automatyki budynkowej (BMS) czy systemy sterowania procesami produkcyjnymi (SCADA/ICS).

Jeśli SKD stosowany w firmie nie ma możliwości przechowywania kluczy DESfire na kontrolerze, a przy tym do transmisji pomiędzy czytnikiem a kontrolerem używa się protokołu Wieganda, to pojawiają się w systemie kolejne otwarte drzwi dla potencjalnych hakerów.

## Dobre praktyki ze świata IT

Punktem zagrożenia jest również styk kontroler–serwer. Powszechną praktyką w nowoczesnych SKD jest połączenie kontrolerów z serwerem po protokole TCP/IP (*rys. 3*). W profesjonalnych SKD jest ono szyfrowane za pomocą AES (*Advanced Encryption Standard*), ale zasady bezpieczeństwa IT wymagają wzmocnionej autoryzacji. Zakładają budowanie zaufania pomiędzy urządzeniami. Łatwo sobie wyobrazić sytuację, że nieuczciwa firma serwisująca wymienia kontroler, podłącza do sieci nowe urządzenie o takim samym adresie IP, adresie MAC i tej sami wersji fabrycznie wbudowanego oprogramowania (*firmware*). Różnica polega na tym, że nowe urządzenie zostało zainfekowane szkodliwym oprogramowaniem. W efekcie po wpięciu do SKD haker uzyskuje dostęp do wybranych przejść, nadaje innym uprawnienia, wymazuje logi, a także ma dostęp do systemów zintegrowanych odpowiedzialnych np. za sterowanie windami, temperaturą czy oświetleniem. Jeśli SKD współdzieli sieć korporacyjna LAN, wspomniane szkodliwe oprogramowanie może przedostać się do komputerów i serwerów przedsiębiorstwa. Ten czarny scenariusz niestety może się ziścić.

W systemach IT tę autoryzację uzyskuje się poprzez użycie certyfikatów (w tym przypadku powinny się one pojawić po stronie zarówno serwera, jak i kontrolera). Przed nawiązaniem połączenia urządzenia powinny się sobie przedstawić, czyli wymienić certyfikatami. Taka praktyka zapewnia, że nawet po podmianie urządzenia na obcy produkt dostęp do SKD będzie niemożliwy (*rys. 4*). Tylko konkretne przedsiębiorstwo jest w posiadaniu certyfikatu przypisanego właśnie jemu. Zazwyczaj mają do niego dostęp nie więcej niż trzy osoby, obowiązuje też surowa procedura ich stosowania. Producenci systemu kontroli dostępu oraz kart nie mają do nich wglądu.

Przedsiębiorstwa często nie mają strategii dotyczącej zagrożeń, które przenoszą się ze środowiska IT do branży security. Dodatkowym problemem jest brak komunikacji między działem security a działem IT. Rozwiązanie chroniące przed migracją cyberzagrożeń do SKD należy więc zaprojektować z perspektywy obu zespołów. Z punktu widzenia cyberbezpieczeństwa powinny zostać zabezpieczone połączenia pomiędzy wszystkimi elementami systemu kontroli dostępu (*rys. 5*).

## Wpływ cyberataków na finanse przedsiębiorstw

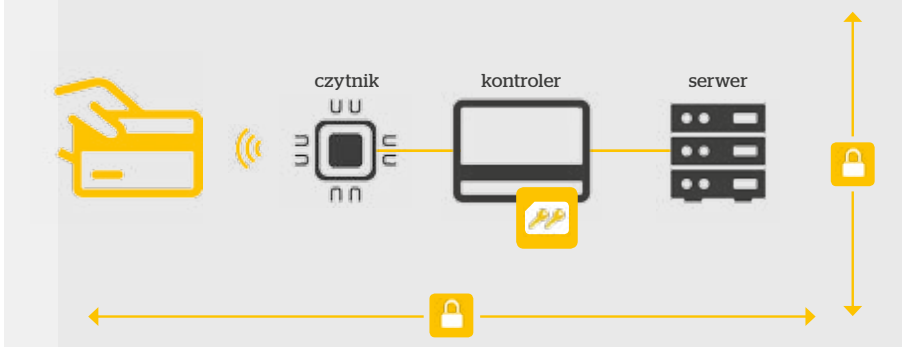
Ataki na systemy informatyczne, produkcyjne czy zabezpieczeń nie są już problemem specjalistów ds. bezpieczeństwa w organizacji. Ich konsekwencje są odczuwalne przez zarząd, akcjonariuszy i klientów. Jedna z międzynarodowych firm audytorsko-doradczych przeprowadziła badanie wśród 1200 osób zarządzających firmami o złożonej strukturze. Dotyczyło ono obaw, z jakimi mierzą się menedżerowie. Wśród odpowiedzi na temat produktów i usług oraz obaw dotyczących tego, że z trudem nadążają za rozwojem nowych technologii, aż 20% z nich wskazało cyberbezpieczeństwo jako budzące ich największy niepokój. Świadczy to o dużej świadomości cyberzagrożeń już na najwyższym szczeblu zarządzania firmami. To samo badanie wykazało, że 86% prezesów martwi się o lojalność swoich klientów. Wbrew pozorom są to tematy ściśle ze sobą powiązane. Niezapewnienie bezpieczeństwa informacji może bowiem mieć wpływ na utratę zaufania klientów. Z kolei niezabezpieczenie poufności informacji tajnych (np. dostęp do strzeżonych receptur firmy) może się przełożyć na osłabienie innowacyjności przedsiębiorstwa. Wzrost świadomości klientów i wnikliwość mediów na szczęście sprawiają, że cyberataki coraz rzadziej pozostają niezauważone i anonimowe.

Cyberataki powodują ogromne straty dla firm, materialne i wizerunkowe. Jak wynika z raportu PWC (*rys. 6*), zanotowane w Polsce w 2015 r. incydenty naruszenia informacji w 33% przełożyły się na straty finansowe, w 31% – na ujawnienie lub modyfikację danych, w 16% – na utratę reputacji. W minionym roku 4% firm polskich w wyniku cyberataków straciło ponad 1 mln zł, a 5% odnotowało przestój w działalności przekraczający pięć dni.

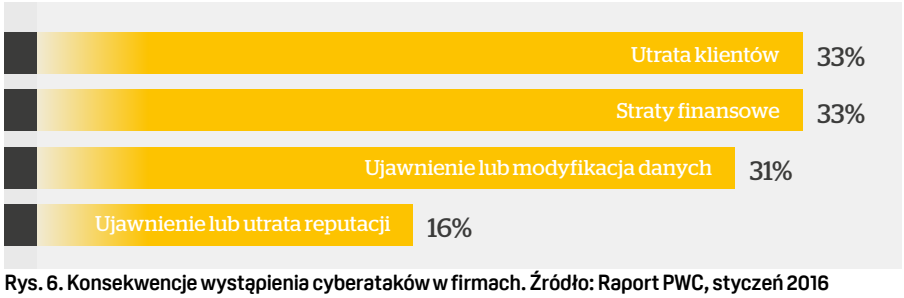
Atak może nadejść z różnych stron, dlatego na cyberbezpieczeństwo organizacji należy spojrzeć holistycznie, dostrzegając – oprócz zabezpieczeń teleinformatycznych – wszystkie systemy, które korzystają z połączeń sieciowych, zatem również SKD, SSWiN, CCTV czy BMS. Wybierając system kontroli dostępu lub planując inwestycję w tym zakresie, warto zwrócić uwagę, czy ma on mechanizmy zabezpieczeń przed cyberatakami lub czy można na nim uruchomić taką funkcjonalność w najbliższych latach. Jest to szczególnie ważne dla firm i instytucji z sektora infrastruktury krytycznej. Temat ochrony SKD przed cyberatakami powinien również być przedmiotem planowanych modernizacji w instytucjach rządowych, firmach przemysłowych, energetycznych, transporcie, telekomunikacji czy sektorze finansowym. Należy traktować go nie mniej poważnie niż inwestycje w cyberbezpieczeństwo systemów informatycznych w organizacji.

Tylko współpraca między działami IT a zabezpieczeń technicznych w zakresie określenia ryzyka oraz opracowanie odpowiednich procedur obowiązujących w infrastrukturze zarówno IT, jak i teletechnicznej pozwoli przygotować organizację na współczesne zagrożenia.

**Najlepsze praktyki**




**Rys. 5. System kontroli dostępu w z zapewnioną bezpieczną komunikacją pomiędzy wszystkimi urządzeniami**




**Rys. 6. Konsekwencje wystąpienia cyberataków w firmach. Źródło: Raport PWC, styczeń 2016**

EY
Rondo ONZ 1
00-124 Warszawa
www.ey.com

# CYBERPRZESTĘPCY SĄ JUŻ W INNEJ EPOCE

**Firmy nie radzą sobie z wykrywaniem incydentów bezpieczeństwa, a przedsiębiorcy identyfikują niewiele cyberataków. Ponad 80% badanych przedsiębiorstw w ciągu roku wykryło do pięciu incydentów.** Dwie trzecie ankietowanych firm uważa, że najsłabszym ogniwem organizacji pod względem podatności na cyberataki są pracownicy, ale jednocześnie zbyt mało uwagi przykładają do szkoleń – wynika z badania EY, Chubb i CubeResearch „Cyberbezpieczeństwo firm".

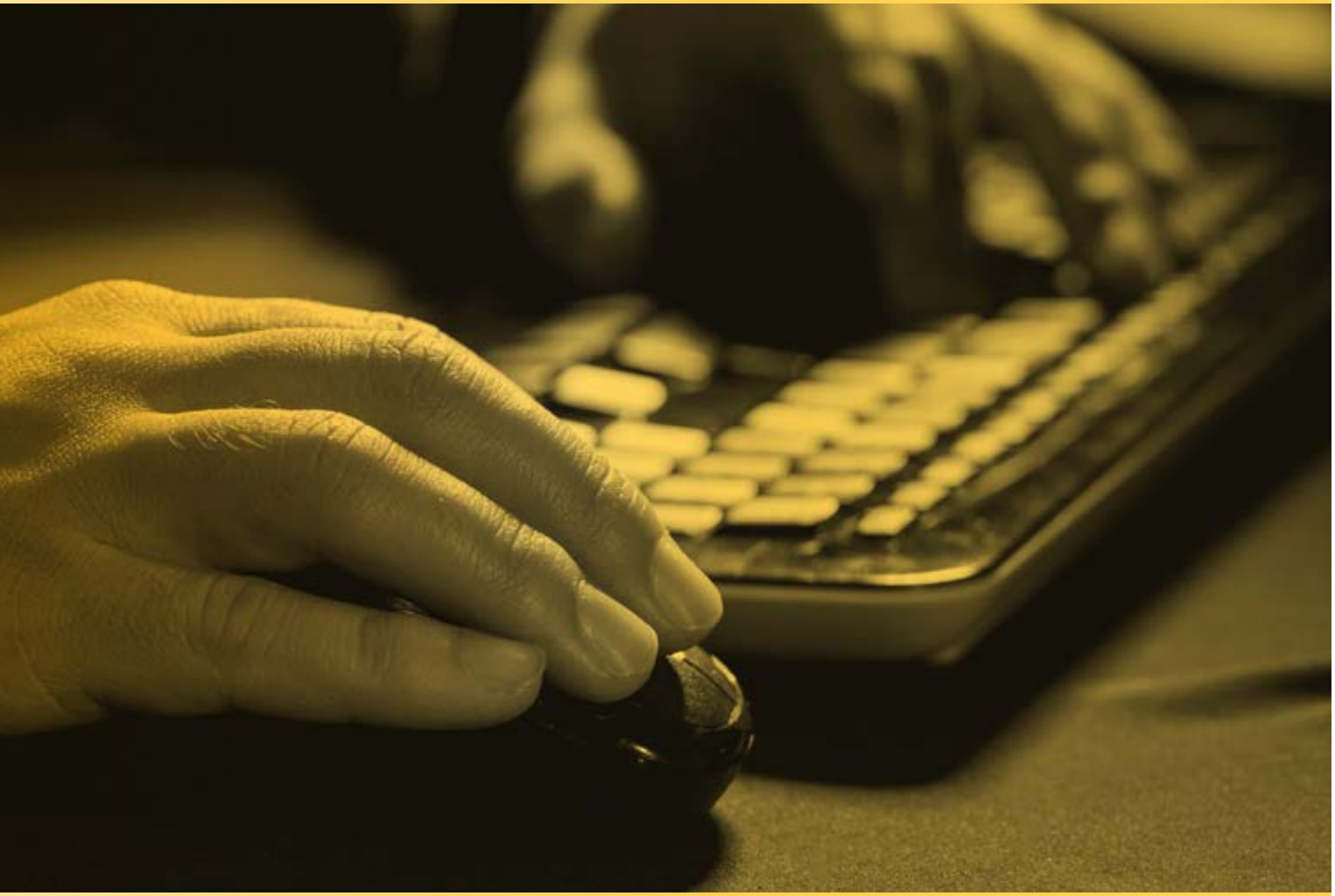
W minionych 12 miesiącach osiem na dziesięć firm zanotowało od zera do pięciu znaczących incydentów naruszenia bezpieczeństwa. Jedna na dziewięć firm padła ofiarą cyberataków od pięciu do dziesięciu razy. 6% badanych doświadczyło więcej niż 10 incydentów. Najczęściej wskazywano ataki malware'owe (68% badanych), działania pracowników (44%) oraz utratę danych z powodu awarii sprzętu (39%). Te incydenty są zdaniem respondentów także największymi zagrożeniami dla ich firm.

*Wyniki wskazują, że firmy nie radzą sobie z wykrywaniem ataków. Organizacje identyfikują bardzo mało incydentów, a wśród tych wykrytych dominują łatwe do zaobserwowania takie jak infekcja ransomware czy utrata danych w wyniku awarii. Pojawia się obawa, czy brak poczucia zagrożenia nie wynika właśnie z braku możliwości zaobserwowania incydentów bezpieczeństwa* – mówi Aleksander Ludynia, menedżer w Zespole Zarządzania Ryzykiem Informatycznym EY.

*Wciąż zdarza się, że słyszymy, że danej firmy „cyberataki nie dotyczą". Warto się wtedy zastanowić, czy tak faktycznie jest, czy też może dana firma jest już ofiarą cyberprzestępców, ale jeszcze o tym nie wie* – dodaje Tomasz Dyrda, dyrektor w Dziale Zarządzania Ryzykiem Nadużyć EY.

## Człowiek najsłabszym ogniwem

Dla większości badanych przedsiębiorstw najsłabszym ogniwem w kontekście bezpieczeństwa organizacji jest nie sprzęt, oprogramowanie czy procedury, lecz człowiek – pracownik firmy. Takiego zdania jest aż 64% respondentów. – *Badanie pokazuje, że przeszkolenie z zakresu*



*bezpieczeństwa IT, przyjęcia na siebie odpowiedzialności za przestrzeganie zasad (przecież podpisaliśmy procedurę bezpieczeństwa) i odświeżanie wiedzy nie wystarcza. Listy trywialnych haseł, pokazujące ignorowanie podstawowych zasad ich tworzenia, lekceważenie zaleceń i procedur szyfrowania danych, otwieranie e-maili phishingowych – to tylko ułamek błędów, które popełniają ludzie, a jednocześnie użytkownicy urządzeń i systemów IT* – ostrzega Tomasz Dyrda.

*– Pracownicy firm ciągle są obdarzani sporym zaufaniem pracodawców. Dodatkowo wiele ataków prowadzonych jest za pomocą przejętych kont administratorów, dlatego także ich działania powinny podlegać szczególnej kontroli i monitorowaniu* – uważa Aleksander Ludynia.

Na kolejnych miejscach wśród przyczyn cyberzagrożeń znaleźli się przestępcy komputerowi - wymieniani przez ponad połowę respondentów (57%), a także przestarzałe oprogramowanie (40%).

## Zabezpieczenia z XX wieku

Mimo nasilającego się zagrożenia ze strony cyberprzestępców i coraz większej liczby udanych ataków firmy opierają swoją obronę na technologiach stworzonych w latach 80. ubiegłego wieku. Jak wynika z badania EY, Chubb i CubeResearch „Cyberbezpieczeństwo firm", są to przede wszystkim programy antywirusowe (93%) i zapory ogniowe (89%). Popularność innych sposobów zabezpieczenia w badanych firmach nie przekroczyła jednej trzeciej. – *Wiele firm wskazuje, że boryka się z incydentami polegającymi na utracie danych, co może prowadzić do wniosku, że firmy nie radzą sobie również z tworzeniem kopii zapasowych kluczowych zasobów informatycznych. Patrząc na wyniki badania, wydaje się, że konieczne są intensywne zmiany w podejściu polskich firm do kwestii bezpieczeństwa systemów informatycznych* – mówi Aleksander Ludynia, menedżer w Zespole Zarządzania Ryzykiem Informatycznym EY.

> Dla większości badanych przedsiębiorstw najsłabszym ogniwem w kontekście bezpieczeństwa organizacji jest nie sprzęt, oprogramowanie czy procedury, lecz człowiek – pracownik.

## Kiedy już zaatakują...

Zaledwie 7% firm posiada system informowania o incydentach działający w trybie 24/7/365, do którego podłączone są wszystkie istotne systemy teleinformatyczne. Aż 43% firm nie posiada żadnego systemu ostrzegania. Bodźcem do bardziej intensywnych działań w obsza-

EY
Rondo ONZ 1
00-124 Warszawa
www.ey.com



rze bezpieczeństwa IT jest atak hakerski. W sytuacji kryzysowej zarząd firmy widzi na bieżąco, jak skuteczne są plany reakcji i struktury odpowiedzialne za bezpieczeństwo IT. Badania w tym obszarze nie nastrajają optymistycznie. – *Niestety, w wielu przypadkach ataki są skuteczne: czy to działania socjotechniczne (ostatnio popularna fala ataków „na prezesa"), wymuszenia okupu (ransomware), czy też ukierunkowane działania hakerów. Firmy ponoszą realne straty i dopiero po takim „zimnym prysznicu" następuje refleksja i próba zrozumienia, w jaki sposób i z kim działać, żeby w przyszłości uniknąć podobnych sytuacji* – twierdzi Grzegorz Idzikowski, menedżer w Dziale Zarządzania Ryzykiem Nadużyć EY. – *Jedynie co ósma firma ma odpowiedni plan oraz zespół i może sprawnie koordynować działania w obliczu zagrożenia* – dodaje.

## Lepiej zapobiegać, niż leczyć

Chociaż firmy zdają sobie sprawę ze znaczenia ludzi dla bezpieczeństwa całego systemu, niewiele z tą wiedzą robią. Okazuje się, że aż 41% pracowników nie uczestniczyło w żadnym szkoleniu na temat bezpieczeństwa w sieci, a w prawie jednej trzeciej badanych firm nie ma procedury postępowania w sytuacji zagrożenia cybernetycznego.

Aż trzy czwarte respondentów badania EY, Chubb i CubeResearch „Cyberbezpieczeństwo firm" stwierdziło, że przeprowadziło w firmie testy bezpieczeństwa, wprawdzie jedynie co piąta firma (21%) zrobiła to w ciągu ostatniego roku, ale wynik ten można uznać za wysoki. Jednak samo wykonanie to tylko pierwszy etap, na którym większość badanych się zatrzymuje. Tylko 15% firm twierdzi, że wnioski z audytu zostały wdrożone w życie.

Innym sposobem zapobiegania konsekwencjom finansowym incydentów bezpieczeństwa jest transfer części ryzyka na ubezpieczyciela. – *W procesie transferu ryzyka sprawdzane są zasady bezpieczeństwa informatycznego, zarzadzania ryzykiem i tzw. higiena informatyczna firmy* – twierdzi Marta Paruch z CHUBB.

– *Mimo że polisa ubezpieczeniowa nie jest remedium na wszelkie problemy, ma możliwość zmniejszenia ponoszonych przez firmę konsekwencji. Ubezpieczyciel może bowiem przejąć część ryzyka poprzez pokrywanie kosztów prawników w przypadku roszczeń pokrzywdzonych w związku z ujawnieniem ich danych niezgodnie z przepisami prawa wraz z zapłatą kar administracyjnych nałożonych przez organy regulacyjne, kosztów doradców PR i informatyków śledczych* – dodaje.

## Z JAKIEGO TYPU INCYDENTAMI MIELI PAŃSTWO DO CZYNIENIA?

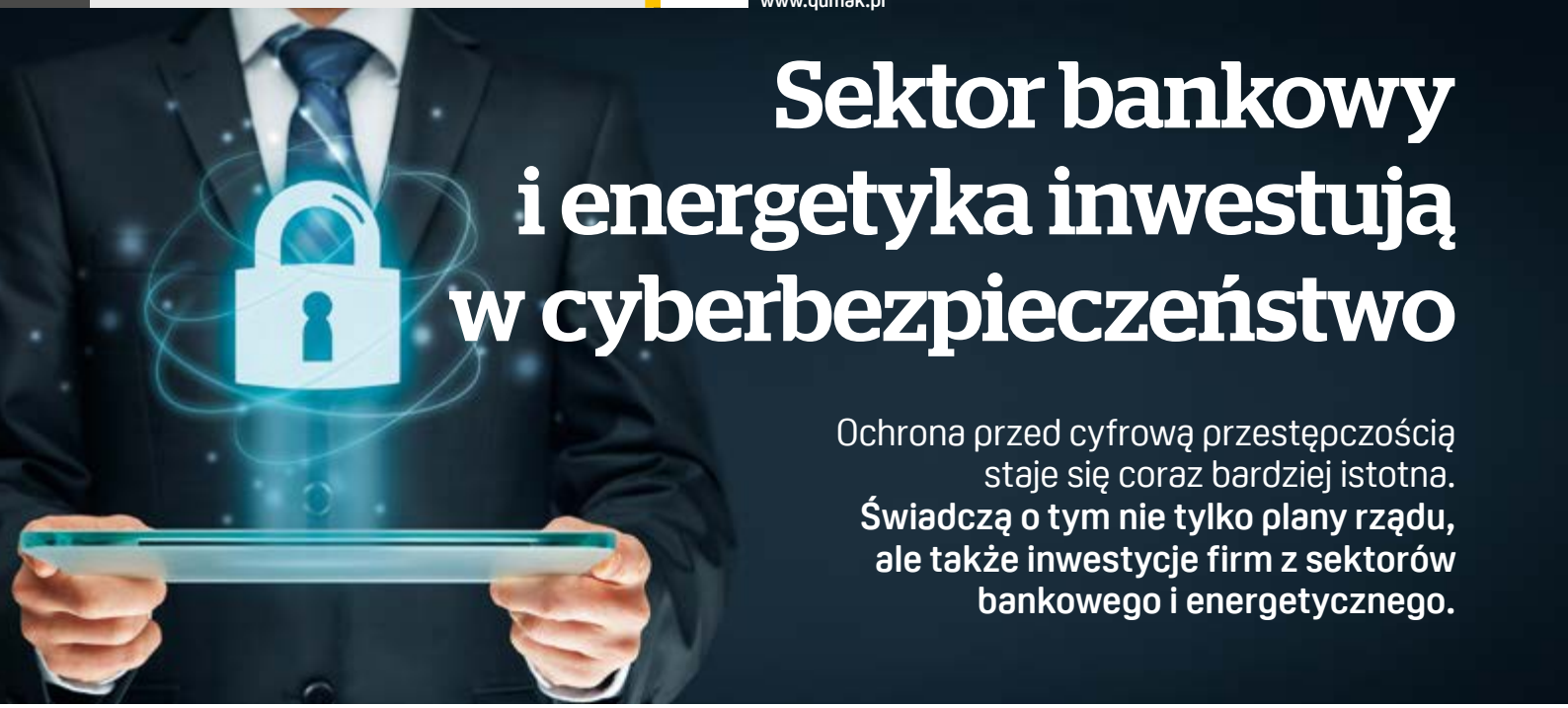

## KTO/CO JEST NAJCZĘSTSZĄ PRZYCZYNĄ INCYDENTÓW?


## O badaniu

Autorami badania „Cyberbezpieczeństwo firm" są konsultanci CubeResearch, EY oraz Chubb. Prace badawcze składały się z dwóch części: badania zasadniczego, gdzie na zadane pytania odpowiadały osoby na co dzień zajmujące się problematyką cyberbezpieczeństwa firm, oraz badania dodatkowego przeprowadzonego wśród pracowników firm. Badanie zasadnicze wykonano na próbie 350 firm, badanie dodatkowe – na próbie 500 pracowników zatrudnionych w firmach polskich.

**Firma EY**
Światowy lider rynku usług profesjonalnych obejmujących usługi audytorskie, doradztwo podatkowe, doradztwo biznesowe i doradztwo transakcyjne. Na całym świecie EY zatrudnia ponad 230 tys. pracowników.

Qumak S.A.
Al. Jerozolimskie 134
02-305 Warszawa
www.qumak.pl



# Sektor bankowy i energetyka inwestują w cyberbezpieczeństwo

Ochrona przed cyfrową przestępczością staje się coraz bardziej istotna. **Świadczą o tym nie tylko plany rządu, ale także inwestycje firm z sektorów bankowego i energetycznego.**

**Krzysztof Tyl**
dyrektor Centrum Kompetencyjnego Business Continuity & Data Security, Qumak SA

Tworzenie rozwiązań mających na celu obronę przed atakami oraz wykrywaniem przestępczości w sieci stało się już priorytetem wielu organizacji, w tym również administracji rządowej. Wpływa na to zarówno rozwój technologiczny, jak i zmieniający się układ geopolitycznych sił, w których Polska odgrywa znaczącą rolę.
Niedawno Ministerstwo Obrony Narodowej zapowiedziało inwestycje w rozbudowę zdolności w cyberprzestrzeni, na którą przeznaczy 1 mld zł. Mogą one objąć budowę laboratorium służącego do prowadzenia badań oraz rozwoju systemów i sieci teleinformatycznych czy zakup systemu do analizy ruchu sieciowego.
W cyberobronność inwestuje również MSWiA. Pod koniec ub.r. ministerstwo uruchomiło w Komendzie Głównej Policji Biuro ds. Walki z Cyberprzestępczością, które ma wprowadzać najnowsze rozwiązania technologiczne w tym zakresie. Chęć zwiększenia udziału technologii w zwalczaniu i wykrywaniu cyberprzestępczości potwierdza również ostatni kontrakt firmy Qumak z Komendą Główną Policji na outsourcing specjalistów IT z różnych dziedzin, którzy będą realizować ogólnopolskie projekty informatyczne. To dopiero początek działań mających na celu wzmocnienie bezpieczeństwa, ale już widać, że będzie to strategiczny obszar inwestycyjny.

## Inwestycje sektora bankowego i energetyki

Instytucje bankowe od dłuższego czasu inwestowały w takie rozwiązania i wyraźnie widać, że nie zwalniają tempa, a doskonalenie zabezpieczeń jest dla nich kwestią priorytetową. W cyberbezpieczeństwo zaczęła także inwestować branża energetyczna.
W ub.r. dla firm z obu tych branż Qumak zrealizował projekty zarządzania cyberbezpieczeństwem o łącznej wartości przekraczającej 7,7 mln zł netto. Tego rodzaju inwestycje będą z pewnością kontynuowane ze względu na realnie występujące zagrożenie. Obszar ten jest również jednym z kluczowych, na którym koncentruje się obecnie Qumak w swojej nowej strategii rozwoju na lata 2017-2020.

## Systemy SIEM – zakres wdrożeń

Zapewnienie odpowiedniej ochrony wymaga konkretnych inwestycji. W przypadku kontraktów zrealizowanych przez Qumak kluczowe było wdrożenie systemów klasy SIEM (ang. *Security Information and Event Management*), opartych na rozwiązaniu IBM Qradar. Zaimplementowane systemy stanowią kluczowy element powstających w tych instytucjach centrów zarządzania bezpieczeństwa tzw. *Security Operations Center* (SOC) oraz są centralnym miejscem do zarządzania bezpieczeństwem całej firmy.
Dzięki nim możliwe jest m.in. rozliczanie zasad bezpieczeństwa pracowników, reagowanie na incydenty zewnętrzne i wewnętrzne, wykrywanie anomalii sieciowych oraz stała automatyczna analiza setek milionów zdarzeń dla różnych scenariuszy cyberataków. Dodatkowo prace przy budowie zabezpieczeń obejmowały również dostawę i konfigurację systemu, projekt architektury, integrację ze środowiskiem IT klienta, projekt mechanizmów korelacji i raportowania. Konieczna była również integracja źródeł logów i źródeł kontekstowych oraz wdrożenie mechanizmów korelacji (UC) i raportowania.

## Systemy cyberbezpieczeństwa przynoszą dodatkowe korzyści

Zrealizowane przez Qumak wdrożenia pozwoliły m.in. na usystematyzowanie informacji o zabezpieczeniach stosowanych w firmie, rozpowszechnianie wiedzy o bezpieczeństwie wśród administratorów, odpowiadanie na zalecenia audytowe oraz przyspieszenie rozwiązywania problemów w działaniu systemów IT.
W cyberbezpieczeństwo będą inwestować kolejne sektory. Dziś nie ma już od tego odwrotu. Jeśli firmy chcą bezpiecznie prowadzić biznes, wykorzystując technologie i internet, będą musiały wdrożyć takie rozwiązania, aby zabezpieczyć się przed działaniami cyberprzestępców.

Marzy mi się dzień, gdy ochrona komercyjna nie będzie zastępowała służb państwowych, będzie dla ludzi pomocą i wsparciem, a dla przedsiębiorców jednym ze zwykłych procesów funkcjonowania ich firm. **Wymaga to głębokiej zmiany (przede wszystkim mentalności) w całym społeczeństwie.**

## AGENCJE OCHRONY W XXI WIEKU CZ. 2.

# PERSPEKTYWY I KIERUNKI ROZWOJU

**Krzysztof Moszyński**
Konsalnet

Marzy mi się dzień, gdy (tak jak w Szwecji) w fabrykach nie będą zabezpieczane elektronarzędzia, ponieważ świadczy to o braku zaufania do pracowników, albo (tak jak w Danii) załogi interwencyjne po incydencie zabezpieczą mienie do momentu przyjazdu policji lub właściciela, ale nie po to, by schwytać włamywacza. Kiedy (jak w Danii) pracownik ochrony za pracę na etacie utrzyma rodzinę na godnym poziomie,

a mówiąc, że pracuje w agencji ochrony, nie będzie musiał tłumaczyć, że w żadnym obiekcie nie pilnuje szlabanu.

## Ochrona komercyjna w Polsce – kierunki rozwoju

Przedsiębiorcy zostali zmuszeni do modernizacji firm i świadczonych usług. Wprowadzenie minimalnej stawki godzinowej do umów zleceń, wzrost płacy minimalnej do 2000 zł oraz zmiany w dodatku do wynagrodzenia za pracę w godzinach nocnych spowodowało, że ochrona fizyczna przestała być tania. A skoro już taka nie jest, przedsiębiorcy zaczęli zastanawiać się, co zrobić, żeby klient zgodził się na podwyżkę. I to znaczną, sięgającą nawet 35% kwoty jednostkowej (roboczogodziny) w porównaniu do roku 2016. Klienci zrobią wszystko, żeby nie płacić więcej niż w roku 2016. Od stycznia 2016 r. opłaty za usługi i tak wzrosły o kilkanaście procent wraz z wprowadzeniem nowych zasad naliczania składek na ubezpieczenie społeczne od umów cywilnoprawnych. Co zatem proponują w odpowiedzi na wnioski agencji ochrony o kolejną podwyżkę?

1. Rozpisanie konkursu ofert opartego 1:1 na dotychczasowym systemie ochrony.
2. Rozpisanie konkursu ofert na podstawie nowo opracowanego (w znacznej mierze przez niezależne od agencji ochrony podmioty) systemu ochrony opartego zazwyczaj na rozbudowywanych i modernizowanych systemach zabezpieczeń technicznych.
3. Postawienie agencji ochrony przed wyborem – świadczenie usług na starych zasadach, przy minimalnym wzroście budżetu przez dotychczasową agencję ochrony, albo zmiana agencji na taką, która zgodzi się świadczyć usług na niezmienionych warunkach.

Poza punktem 1, który nic nie zmienia, pozostałe reakcje wyzwoliły w agencjach ochrony niespodziewane pokłady innowacyjności[1]. Okazało się, że bez widocznego obniżenia jakości ochrony można w niektórych obiektach zmniejszyć nawet o 20–30% posterunki/roboczogodziny przy odpowiednio skonfigurowanym systemie ochrony, dobranych funkcjonalnie narzędziach i odpowiednim zadaniowaniu służb ochrony.

Co zatem z kierunkami rozwoju? Otóż po raz pierwszy rynek wymusił na przedsiębiorcach i odbiorcach zmiany polegające na konstruowaniu systemów ochrony na potrzeby konkretnego obiektu, opartych na interakcjach pracowników ochrony z systemami zabezpieczeń i procesami przebiegającymi w obiektach odbiorców. Nie wszyscy jeszcze, nawet nie większość, są skłonni do zmian „tego, co było zawsze" na nowe i nieznane, ale tendencja jest już wyraźna. Pojawia się coraz więcej pytań o rozbudowy, modernizacje i adaptacje istniejących systemów zabezpieczeń, i to pod kątem ich ścisłego współdziałania z ochroną fizyczną. Odbiorcy usług ochronnych zaczynają rozumieć, że ochrona jest takim samym procesem wewnętrznym ich organizacji, jak logistyka. Jak każdy proces powinna być elastyczna – tzn. zmienna w czasie, konfiguracji i funkcjonalności.

Po drugiej stronie barykady można dostrzec – choć nie wszędzie i nie u wszystkich graczy rynkowych – początki zmian w postrzeganiu tego, co i jak zrobić w chronionym obiekcie. Można stosować np. system ochrony oparty na połączeniu posterunków stacjonarnych i patroli mobilnych skierowanych do ochrony konkretnych osiedli. Osiedla znajdują się zazwyczaj w niedużej od siebie odległości, co przy nowej usłudze i zachowaniu jakości ochrony pozwala uzyskać oszczędności na poziomie ok. 30% w stosunku do kosztów ochrony ponoszonych obecnie, bez inwestycji w nowe systemy zabezpieczeń technicznych.

Reasumując, zrówno polski rynek firm ochrony, jak i odbiorców usług ochronnych zaczyna dostrzegać mnogość dostępnych kierunków rozwoju procesu zabezpieczenia i ochrony. Na początku wymaga to pracy analitycznej i koncepcyjnej, której efektem będzie opracowanie właściwego dla danego odbiorcy i jego obiektu/obiektów systemu ochrony i zabezpieczenia. W Polsce rozpoczął się proces ewolucji ochrony.

## Ochrona komercyjna w Polsce – ewolucja

Na czym owa ewolucja ochrony może polegać, jest to przecież proces nieprzewidywalny. Jesteśmy w o tyle wygodnej sytuacji, że możemy czerpać wzorce z rynków bardziej zaawansowanych, dostosowywać je do naszych realiów i prognozować rozwój rynku polskiego.

Lata 2017–2018 będą przełomowe dla ochrony komercyjnej. Wychodząc prawie

> Lata 2017–2018 będą przełomowe dla ochrony komercyjnej w Polsce. Jesteśmy w wygodnej sytuacji, mogąc czerpać wzorce z rynków bardziej zaawansowanych, dostosowywać je do naszych realiów i prognozować rozwój rynku polskiego.

> Wprowadzenie minimalnej stawki godzinowej, wzrost płacy minimalnej i zmiany w wynagrodzeniach za pracę w godzinach nocnych wyzwoliły w agencjach ochrony niespodziewane pokłady innowacyjności.

[1] Nieliczne, głównie duże podmioty rynku ochrony od początku 2016 r. opracowywały nowe usługi, inwestowały w zaawansowane systemy zarządzania ochroną, technologie mobilne, analitykę, oprogramowanie, modernizacje stacji monitorowania przygotowywanych pod nowe usługi itp.

30 lat temu (1989 r.) z pozycji nieregulowanego rynku – ani od strony przepisów, norm jakościowych i ilościowych, ani praktyk branżowych – w Polsce został osiągnięty etap, kiedy handlowiec czy konsultant, a już na pewno analityk reprezentujący agencję ochrony coraz częściej pyta klienta, w jakim celu pracownik ochrony ma cały czas przebywać we wskazanym miejscu. Czy nie szkoda na to pieniędzy? Nic dziwnego, że dotychczas czerpały one dochody ze sprzedaży „masy", czyli roboczogodzin. Im więcej wszak, tym lepiej.

Ewolucja w jej ogólnym zarysie będzie polegać na tym, że zadowolony klient, zamiast płacić za np. 10 tys. roboczogodzin w miesiącu po 10 zł za godzinę, chętnie zapłaci 25 zł za każdą z np. 3000 roboczogodzin w miesiącu. Dlaczego? Ponieważ będzie miał profesjonalną ochronę pracownika zaangażowanego, utożsamiającego się z dobrem przedsiębiorstwa, ambitnego, widzącego przyszłość w tej branży, a nie pracownika sezonowego. Co ważne, będzie miał w swojej organizacji dopasowany do potrzeb oraz istniejącego ryzyka i zagrożenia efektywny proces zunifikowany z całą organizacją i jej specyfiką. Proces ten zapewne będzie oparty na zaawansowanych rozwiązaniach technicznych, zinformatyzowanych i mobilnych usługach, czyli na rozwiązaniach zdalnych i sieciowych.

Branżę ochrony czeka długa droga, z której nie ma już powrotu. Będzie ona ciekawa, pełna wyzwań, nauki i pracy. Będziemy tworzyć nową jakość, nowe standardy i rozwiązania.

## Ochrona komercyjna w Polsce – co dalej?

Wypadkową naszkicowanej ewolucji będą kolejne kroki w rozwoju i modernizacji procesów ochronnych.

### 1. AGENCJE OCHRONY

Usługi świadczone przez agencje ochrony jako elastyczne i mobilne[2)] zostaną dopasowane na bieżąco do potrzeb klienta. Proces odchodzenia od stałej „twardej" ochrony fizycznej na rzecz usług zdalnych i sieciowych będzie stały i bardziej dynamiczny. Będą to firmy, dla których słowo „profesjonalizm" to nie tylko pusty frazes, a ich pracownicy, dbający o swoje kwalifikacje i kompetencje, będą dumni z wykonywania tego zawodu. Agencje ochrony dostrzegą zaniedbywany dotychczas ogromny obszar safety, który jest rozwinięciem security.

Szeroko rozumiane techniki zabezpieczeń będą miały coraz większy udział w rynku ochrony. I nie będą to wyłącznie urządzenia, lecz także obróbka danych, analityka, rozwiązania software'owe i sieciowe.

Branżę ochrony czeka długa droga, z której nie ma powrotu. Będzie ciekawa, pełna wyzwań, nauki i pracy. Będziemy tworzyć nową jakość, nowe standardy i rozwiązania.

### 2. PROCESY OCHRONNE

Czeka nas skok jakościowy związany z robotyzacją i automatyzacją początkowo nielicznych, później coraz większej liczby procesów ochronnych. Już dzisiaj coraz częściej stosuje się systemy rejestrujące osoby i pojazdy, tworzące z danych pobieranych z kadrów i zdjęć dane osobowe lub dane pojazdów (np. tablice rejestracyjne). W większości firm logistycznych służby ochrony korzystają ze skanerów kodów kreskowych do kontroli ładowanych i/lub rozładowywanych pojazdów czy towarów w magazynach.

Wszędzie tam, gdzie procesy są w pełni powtarzalne i liczy się niezawodność, wydajność i niskie koszty pracy, wcześniej czy później zostanie wprowadzona automatyzacja procesów. Pracę ręczną przy taśmach produkcyjnych zastąpi robotyzacja.

Rozwiązania wojskowe, jeszcze bardzo drogie, opierają się na bezzałogowych pojazdach, dronach, a nawet łodziach patrolowych, które w trybie standardowym są kierowane przez komputer. Dopiero sytuacja niestandardowa powoduje przełączenie na kierowanie ręczne, choć nie w każdym przypadku.

Za kilka, kilkanaście lat rynek ochrony komercyjnej nie powinien odbiegać strukturą od rynków zachodnich. Będzie kilku graczy posiadających łącznie 80% rynku (lub więcej) oraz grupa niezależnych, lokalnych agencji ochrony.

Łatwo sobie wyobrazić, że perymetr ochronny jest chroniony przez samobieżny i kierowany przez komputer pojazd gąsienicowy, wyposażony w zestaw kamer i mikrofonów, przekazujący wszystkie sygnały wychodzące poza zadany poziom tła do stacji monitorowania, powodując alarm na stanowisku operatorskim. Na jednym z portali internetowych ukazał się artykuł „K5 – strażniczy robot do pilnowania obiektów" opisujący przyszłość naszej branży. Pracownicy zapewne zostaną rozlokowani w miejscach bezpośredniego i koniecznego kontaktu z innymi osobami i będą reagowali wyłącznie na sygnały alarmowe generowane przez zautomatyzowane systemy bezpieczeństwa.

Agencje ochrony również będą mogły korzystać z nowych usług, np. Falck w Estonii odwozi i odprowadza dzieci do szkół i przedszkoli. Z kolei w Danii jeździ do domów na wezwania do niewielkich awarii domowych, które wymagają interwencji tzw. złotej rączki.

### 3. GLOBALIZACJA

Czy tego chcemy, czy nie, prekursorów na rynku polskim jest wielu, i to od lat. Zarówno Securitas czy nieobecne już w Polsce Group4 oraz Falck (z których powstała korporacja Group4Securicor, w Polsce zakupiona przez Konsalnet), jak i nieudane wejście na rynek polski czeskiej firmy M2C – to były próby włączenia polskiego rynku ochrony w sieć globalnych korpo-

[2)] Agencje ochrony powinny się specjalizować. Skoro usługi powinny być dostosowane do klienta, należy skupić się na tym, w czym dana agencja jest najlepsza.

racji ochronnych. Na razie tylko Securitas działa w Polsce jako zachodnia korporacja ochronna, choć po ostatnich zmianach coraz bardziej przypomina rodzime firmy. Globalne korporacje wrócą jednak do Polski.

Właśnie jesteśmy świadkami największego przejęcia na polskim rynku ochrony – Konsalnet został kupiony przez China Security & Fire. Można przypuszczać, że chińscy inwestorzy nie poprzestaną na tej jednej akwizycji, a ich strategia przewiduje w perspektywie dalszą globalną ekspansję.



Za kilka, kilkanaście lat polski rynek ochrony nie powinien odbiegać strukturą od zachodnich. Będzie kilku graczy posiadających łącznie nawet 80% rynku (lub więcej) oraz grupa niezależnych lokalnych agencji ochrony świadczących lokalne usługi na rzecz przedsiębiorców ceniących sobie firmy rodzime, czyli okrojoną ochronę fizyczną, lokalny monitoring z własnymi załogami interwencyjnymi (które będą podwykonawcami dla dużych graczy) i niewielki zakres usług komplementarnych.

BIO

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

VIVUS Finance
ul. 17 Stycznia 56
02-146 Warszawa
www.vivus.pl

# DANE W PREWENCJI, DETEKCJI I ANALIZIE NADUŻYĆ

O tym, że organizacja nie może funkcjonować bez danych, wiedzą właściwie wszyscy. Dane wprowadzone do krwiobiegu firmy zasilają ją informacyjnie, wpadając w przepastne bazy danych, a po nich w turbiny raportów i analiz; **przekierowane, przetworzone i uporządkowane przyjmują formę zestawów słupków, tabel i wykresów. Wyznaczają kierunek dalszego działania przedsięwzięć, kampanii czy strategii.**

Adam Trzeciak

Nie inaczej jest w przypadku funkcji odpowiedzialnej w przedsiębiorstwie za działania antyfraudowe. To układ odpornościowy organizacji – poprzez identyfikację i ograniczanie zagrożeń zapobiega on rozprzestrzenianiu się, nasilaniu czy wręcz występowaniu zjawisk niepożądanych, jakimi są nadużycia. Szczególnie w materii nadużyć związanych z wyłudzeniami środków czy produktów dane mają określone zadania. Aby mogły się z roli „komórek pamięci immunologicznej" należycie wywiązać, jednostka zarządzająca ryzykiem nadużyć musi odpowiednio je rozumieć, traktować i wykorzystywać.

Pierwszą okazją do pozyskania danych jest identyfikacja klienta. To moment krytyczny z oczywistego powodu – im skuteczniejsze potwierdzenie tożsamości klienta, tym sprawniejsze dochodzenie roszczeń w przypadku, gdy klient nie zechce wywiązać się z zobowiązań, a z perspektywy zapobiegania nadużyciom tym mniejsze ryzyko straty. Na tym etapie istotną rolę odgrywają trzy podstawowe aspekty: zakres danych, za pomocą których odbywa się indentyfikacja klienta, sposób ich pozyskiwania oraz jakość pozyskanych danych.

Pierwszy aspekt, czyli zakres danych, dotyczy zestawu informacji, poprzez które klient jest rozpoznawany, rejestrowany, otrzymuje profil czy konto. Są to zwykle dane osobowe i teleadresowe związane z dokumentami tożsamości, dotyczące banku, w którym ma rachunek, czy wreszcie szeroko pojęte informacje związane z pracodawcą klienta.

W przypadku sprzedaży online zakres danych powinien zostać poszerzony o wszelkie informacje, które można pozyskać z elektronicznych form sprzedaży, takie jak identyfikacja sieci, wskazanie operatora sieci, urządzenie, z którego klient korzysta, ustawień do tego urządzenia. W przypadku sprzedaży przez placówki czy sieć partnerów nieocenione – nie tylko pod kątem rozliczalności, ale także ze względu na przyszłe analizy – będą informacje związane z partnerem, identyfikatorem pracownika partnera czy punktu sprzedaży.

By lista danych wykorzystywanych do identyfikacji klienta była pełna, należy ją poszerzyć o kategorię danych, które może nie dają pewności przy

**Wyznacznikiem sprawności jednostki przeciwdziałającej nadużyciom jest trafność wniosków opartych na analizie i szybkość wdrożenia adekwatnych działań prewencyjnych.**

## WYKORZYSTANIE DANYCH W MECHANIZMACH ZAPOBIEGAJĄCYCH NADUŻYCIOM

- Pozyskanie możliwie najszerszego ich zakresu już przy pierwszej transakcji, pierwszym kontakcie z klientem oraz przy kolejnych kontaktach
- Skłanianie się do automatycznego pozyskiwania danych związanych z klientem
- Identyfikacja ich pochodzenia, czyli rozumienie, jak zostały pozyskane.
- Normalizacja pozyskanych danych.

pierwszym kontakcie z klientem, ale przy ponownym mogą okazać się nieocenione. Chodzi o dane biometryczne. Coraz częściej na rynku są dostępne rozwiązania oparte na potwierdzaniu tożsamości osoby poprzez odcisk palca, odręczne pismo, głos czy fizjonomię. Nie są już nowością metody weryfikacji na podstawie tych niepowtarzalnych, nierozerwalnie związanych z osobą, spersonalizowanych danych biometrycznych. Sprawą dyskusyjną i do indywidualnej oceny pozostaje ich przydatność, np. pod kątem kosztów wdrożenia, możliwości zbierania tego typu danych, opłacalności wykorzystania czy w ogóle konieczności ich pozyskiwania.

Ważnym aspektem jest sposób pozyskania tych danych – czy są deklarowane, czy otrzymywane automatycznie, czy uzyskane osobiście, czy poprzez sieć partnerów sprzedających w imieniu konkretnej firmy usługę czy produkt. Determinuje to wagę zebranych danych oznaczającą poziom zaufania podczas ich analizowania i weryfikacji.

Jakość danych, czyli trzeci z wymienionych aspektów, to poziom ich **dokładności, adekwatności i znormalizowania.** Jako wyjaśnienie warto przytoczyć następujące przykłady: kod pocztowy nie może mieć czterech cyfr, numer PESEL – dziesięciu, Rzeszów to z pewnością nie nazwa ulicy w Podkowie Leśnej, a podany przez klienta adres poczty e-mail nie obędzie się bez znaku @ oraz nazwy domeny. Już na etapie rejestracji należy zadbać o to, by dane podawane przez klienta, pośrednika bądź partnera były poddane normalizacji, czyli ujęte i wpisywane w dopuszczalnych dla nich formatach. Ma to istotne znaczenie przy późniejszym budowaniu mechanizmów antyfraudowych, analizie, szukaniu i identyfikowaniu zależności na bazie danych historycznych. Dopiero na takiej podstawie można oprzeć proces tworzenia mechanizmów prewencji i detekcji nadużyć w organizacji: analizowanie scenariuszy wyłudzeń, które dotknęły firmę, budowanie zróżnicowanych modeli, silników reguł czy systemów ocen określających prawdopodobieństwo wystąpienia wyłudzenia.

Identyfikacja nadużyć i zapobieganie im to niekończący się, zapętlony, stale doskonalony proces. Na jego wejściu występują dane związane z identyfikacją i historią klienta, które przechodzą przez sito porównań, weryfikacji, reguł, analiz, wspierających decyzję o zaakceptowaniu lub odrzuceniu transakcji. Na wyjściu natomiast uzyskuje się efekt w postaci skuteczności wdrożonych zabezpieczeń – dana transakcja może być kolejną cegiełką do dodatniego wyniku finansowego firmy lub uszczupleniem tego wyniku, czyli stratą. Strat zapewne nigdy nie da się uniknąć, jednak zadaniem jednostki przeciwdziałającej nadużyciom, wyznacznikiem sprawności jej działania jest trafność wniosków opartych na analizie zidentyfikowanego, potwierdzonego nadużycia i szybkość wdrożenia adekwatnych działań prewencyjnych. Bez „odżywiania" właściwymi i odpowiednio dobranymi danymi układ odpornościowy organizmu firmy nie będzie w stanie skutecznie się bronić przed szkodliwymi zarazkami.

BIO

**Adam Trzeciak** Od 15 lat pracuje na rynku usług telefonii komórkowej oraz w sektorze usług finansowych na rzecz prewencji i detekcji nadużyć.

# PLANOWANIE CIĄGŁOŚCI DZIAŁANIA

## MODA CZY KONIECZNOŚĆ W NIESPOKOJNYCH CZASACH

Co sprawia, że jedne przedsiębiorstwa przechodzą przez kryzysy i klęski żywiołowe niemal nietknięte, podczas gdy **inne w tych samych warunkach walczą o przetrwanie?**

**Marcin Marczewski**

Katastrofy się zdarzają. W ostatni weekend sierpnia 2011 r. huragan Irene uderzył we Wschodnie Wybrzeże Stanów Zjednoczonych. Silny wiatr był przyczyną wielu awarii sieci energetycznej, natomiast obfite deszcze i spiętrzone wody Oceanu Atlantyckiego spowodowały liczne podtopienia i lokalne powodzie, m.in. w Wirginii, Karolinie Północnej, Massachusetts i New Jersey. Straty dla całej gospodarki USA oszacowano na 10 mld dolarów. Wśród wielu firm poszkodowanych przez żywioły były elektrownie, lotniska i transport publiczny, a także zakłady przemysłowe i wiele mniejszych firm.

Ponad dwa tysiące osób zatrudnionych w siedzibie głównej Johnson & Johnson's utraciło dostęp do biura po tym, jak woda odcięła drogi dojazdowe. GlaxoSmithKline zamknęło podtopioną fabrykę. Awarie zasilania przyczyniły się do zamknięcia biur Teva Pharmaceuticals, Bayer HealthCare oraz Cephalon Inc. Nietrudno wyobrazić sobie zamieszanie wywołane przez huragan w tych firmach. Część z nich odpowiedziała na zdarzenia w sposób reaktywny, dostosowując działalność do zmieniających się warunków. Były jednak wśród nich również takie, które Irene potraktowały jako trochę gorszą pogodę.

Jaką wartość dla firmy farmaceutycznej, jej klientów i organów nadzoru może mieć wdrożenie planów i systemu zarządzania ciągłością działania? Czy wdrożenia takich planów muszą być długotrwałe i kosztowne?

### Ciągłość działania

Firmy,myśląc o ciągłości działania, opracowują przede wszystkim formalne plany czy procedury odtwarzania infrastruktury IT po awarii (*Disaster Recovery Plan* – DRP). Oznacza to, że przede wszystkim są przygotowane na awarie związane z niedostępnością danych, systemów IT i infrastruktury telekomunikacyjnej. Zarządzanie ciągłością działania jest jednak obszarem znacznie szerszym, a odtwarzanie usług IT – tylko jednym z jego aspektów. Ciągłość działania obejmuje również inne obszary zarządzania firmą: bezpieczeństwo i dostępność pracowników, ochronę wizerunku, komunikację kryzysową, zapewnienie dostępności kluczowych dostawców i partnerów outsourcingowych oraz inne działania umożliwiające odtworzenie kluczowych procesów w sytuacji kryzysowej w z góry zaplanowanym czasie.

Kilka lat temu w Stanach Zjednoczonych przeprowadzono badanie stanu rozwiązań w obszarze ciągłości działania w firmach farmaceutycznych[1]. Jego wyniki wskazują, że znacznie lepiej rozwinięte w tym obszarze są duże korporacje farmaceutyczne. Mniejsze firmy z branży, o dochodach nieprzekraczających 1 mld dolarów, podchodzą do tej tematyki z większym dystansem. Jeśli chodzi o kluczowe dla tej branży obszary w kontekście wymagań dostępności, przedstawiciele firm zgodnie wskazywali procesy biznesowe związane z zarządzaniem finansami, procesy produkcyjne, ochronę danych i kapitału intelektualnego (badania i rozwój nowych produktów). Zarządy tych firm stwierdzały, że głównymi czynnikami wpływającymi na priorytet prac nad wdrożeniem planów ciągłości działania były branżowe regulacje prawne wprowadzane przez FDA, Sarbanes-Oxley Act (wymuszający na organizacjach przygotowanie rozwiązań w zakresie kontroli zarządczej, w tym zarządzania ryzykiem), a także zestawy dobrych praktyk dotyczących wytwarzania i badań nad nowymi produktami. Brak zgodności z ww. wymaganiami może skutkować nałożeniem znaczących kar finansowych (100 mln dolarów lub większych). Badania potwierdziły również, że znaczna część osób zarządzających spółkami z tej branży obawiała się, że w sytuacji realnego zagrożenia ciągłości działania ich organizacje mogłyby nie spełnić wymagań regulacyjnych. Jednym z takich wymagań jest ciągłe monitorowanie bezpieczeństwa oferowanych produktów, co oznacza utrzymanie pełnej dostępności centrów telefonicznych dla pacjentów,

[1] Raport Business Continuity in the Pharmaceutical Industry opracowany przez Stevens Institute of Technology.

**Najczęściej powtarzanymi argumentami przeciwko wdrażaniu planów jest brak czasu i fałszywe poczucie bezpieczeństwa.**

aby całą dobę mogli zgłaszać problemy i powikłania związane z produktami. W Polsce już dawno powstały podobne wymagania dostępności dla wybranych procesów realizowanych przez firmy z branży farmaceutycznej. Jest w nich mowa o tym, że każdy podmiot w łańcuchu dystrybucji leków musi zapewnić niemal natychmiastowe wycofanie z rynku produktów, których sprzedaż została formalnie wstrzymana, np. przez Główny Inspektorat Farmaceutyczny. Wydaje się jednak, że podmioty regulujące i nadzorujące rynek farmaceutyczny nie doceniają jeszcze narzędzi, jakimi są zarządzanie ryzykiem i planowanie ciągłości działania. Z drugiej strony większość firm działających na rynku polskim musiała zapewnić realizację tych wymagań prawnych i wdrożyła przynajmniej w wąskim zakresie rozwiązania organizacyjne, zapewniające możliwość zarządzania sytuacjami kryzysowymi i ciągłość wybranych procesów. Pozostaje pytanie, czy firmy te są pewne, że ich procedury zadziałają w sytuacji kryzysowej?

## Przygotować się na najgorsze

Rozwiązania w obszarze ciągłości działania do tej pory kojarzono jedynie z wielkimi korporacjami działającymi w branży finansowej, które było stać na poświęcenie czasu i pieniędzy na przygotowanie i wdrożenie planów. Okazuje się jednak, że to zwłaszcza małe i średnie przedsiębiorstwa są bardziej narażone na różnego typu incydenty i sytuacje kryzysowe, które mogą negatywnie wpłynąć na realizację ich krytycznych zobowiązań, procesów i usług. Praktyka dowodzi, że z jednej strony przygotowanie skutecznej reakcji na podobne zdarzenia nie wymaga poświęcenia dużych zasobów, z drugiej – takie działania przynoszą znaczące korzyści. W badaniach przeprowadzonych na Oksfordzie udowodniono 5-procentowy wzrost cen akcji spółek, które były dobrze przygotowane do zarządzania sytuacjami kryzysowymi. Spółki przygotowane gorzej lub nieprzygotowane w ogóle traciły średnio po 15% wartości.

W zarządzaniu ciągłością działania bardzo ważne jest poznanie otoczenia, w którym firma prowadzi działalność, jej najważniejszych procesów biznesowych oraz realnych zagrożeń i ich wpływu na prowadzenie biznesu. Podstawowymi zdarzeniami, na które przygotowuje planowanie ciągłości działania, są np. długotrwała awaria zasilania, niedostępność siedziby, absencja dużej grupy pracowników, awaria systemów i infrastruktury IT, problemy z dystrybucją, transportem i logistyką produktów czy też awaria u jedynego zewnętrznego dostawcy usług lub półproduktów. W wielu przypadkach to, że zrobiliśmy cokolwiek w celu zabezpieczenia ciągłości naszej firmy, umożliwi jej przetrwanie i minimalizację strat w wymiarze finansowym i wizerunkowym. Brak przygotowania i jakichkolwiek planów może zagrozić istnieniu firmy.

Najczęściej powtarzanymi argumentami przeciwko wdrażaniu planów jest brak czasu, niezrozumienie wartości dodanej, inne ważniejsze zadania, fałszywe poczucie bezpieczeństwa, wiara w to, że firma poradzi sobie, kiedy wystąpi kryzys, zbyt duże koszty, poczucie, że IT nas uratuje oraz przeświadczenie, że nie grozi nam żadne ryzyko.

Pełne wdrożenie planu składa się z kilku etapów. Pierwszym i podstawowym krokiem jest zrozumienie własnej organizacji, sposobu jej działania, a także czasu, w jakim należy realizować najważniejsze usługi lub inne zobowiązania (np. nałożone przez organy nadzoru). Drugim krokiem jest identyfikacja i ocena głównych zagrożeń, przed którymi stoi firma w ramach działalności operacyjnej. Powinna ona bazować na najprostszym podejściu, czyli odpowiedzi na następujące pytania: „Co może się zdarzyć?", „Gdzie, kiedy i dlaczego (jakie są czynniki ryzyka i podatności)?", „Jak firma jest obecnie zabezpieczona?" oraz „Co można poprawić?". Ponadto należy zidentyfikować najbardziej krytyczne zasoby niezbędne do przetrwania firmy i zbadać, jak są

zabezpieczone. Trzeba np. zweryfikować, czy kompetencje i zakresy odpowiedzialności pracowników są delegowane w taki sposób, aby niedostępność jednej osoby nie przerwała żadnego z kluczowych procesów biznesowych.

Następnym etapem budowy odporności firmy na zdarzenia kryzysowe jest opracowanie strategii zabezpieczenia i utrzymania kluczowych zasobów, takich jak ludzie, lokalizacje, technologie (produkcja, IT), dostawcy. To na tym etapie firmy stają przed dużym wyzwaniem, analizując, ile pieniędzy są skłonne wydać na zabezpieczenie systemów krytycznych i innych zasobów. Podczas projektowania rozwiązań zapasowych należy kierować się wymaganym przez biznes czasem dostępności systemu oraz wielkością strat, jakie mogą powstać w razie opóźnienia w jego uruchomieniu. Doświadczenie pokazuje, że przeważnie dochodzi wtedy do eskalacji oczekiwań przedstawicieli jednostek biznesowych odnośnie do wymagań krótkich czasów dostępności zasobów IT. Należy mieć jednak na względzie, że ostatecznie to właśnie biznes zostanie obciążony wydatkami poniesionymi w celu zwiększenia dostępności niezbędnych dla niego zasobów. Należy zawsze starać się minimalizować koszty związane z inwestycjami w infrastrukturę IT. Jeśli coś da się zrobić ręcznie w określonym czasie i jest to akceptowalne przez biznes, trzeba rozważyć takie rozwiązanie. Wydłużenie czasu na odtworzenie narzędzi IT oraz zewnętrznych usług znacznie zmniejszy koszty. Niestety nie ma jednej odpowiedzi, ile kosztują zabezpieczenia. Wydatki powinny być adekwatne do potencjału i prawdopodobieństwa zidentyfikowanego ryzyka. Górnym limitem w obszarze *Disaster Recovery* powinna być kwota 20–30% wartości potencjalnych strat.

Ważnym elementem tego etapu jest także przygotowanie założeń do pracy w trybie kryzysowym. W zakresie opracowania strategii działania należy zweryfikować, czy można zapewnić i wyposażyć zapasową lokalizację dla firmy na czas po wystąpieniu zdarzenia. Rozwiązanie to wydaje się najbardziej odpowiednie dla firm dysponujących większą liczbą lokalizacji biznesowych. Jeśli wybrani pracownicy mają być przenoszeni do lokalizacji zapasowych, muszą one być na tyle blisko, żeby udało się do nich dotrzeć w czasie w miarę krótkim i z góry zaplanowanym (biorąc pod uwagę ewentualne trudności spowodowane wystąpieniem incydentu). Jednocześnie lokalizacja zapasowa powinna być wystarczająco oddalona, aby nie znalazła się w zasięgu tego samego zdarzenia. W praktyce stosuje się lokalizacje zapasowe położone w odległości od kilku do kilkunastu kilometrów od lokalizacji podstawowej, ale w granicach tej samej aglomeracji. Alternatywą dla tego rozwiązania może być udostępnienie pracownikom zdalnego dostępu do narzędzi i systemów IT oraz zezwolenie na pracę z domu lub zaplanowanie wynajęcia zapasowego biura. Jeśli chodzi o zapasowe centra danych, duże firmy lokalizują je nawet w innych miastach lub regionach.

> Brak jakichkolwiek planów ciągłości działania może zagrozić istnieniu firmy.

Kolejnym działaniem jest weryfikacja, w jaki sposób zamierzają się przygotować na podobne zdarzenie kluczowi usługodawcy czy dostawcy firmy. W tym przypadku niezbędnym minimum jest ustalenie, w jaki sposób zabezpieczono świadczenie usług na rzecz firmy. Pomocne mogą być wszelkie dowody na testowanie, przeglądy oraz aktualizacje tych rozwiązań – czyli potwierdzenie, że były weryfikowane w praktyce.

Wszystkie planowane działania powinny zostać udokumentowane w formie głównego planu lub ogólnych założeń do pracy w sytuacji kryzysowej, które określą zakres zadań poszczególnych osób ze wskazaniem ich zastępców. Ważne, aby wytypować osoby, które będą podejmowały strategiczne decyzje biznesowe i finansowe. W ramach opracowania dokumentacji powinny zostać przygotowane: procedura zarządzania incydentami (nawet w formie listy kontrolnej), lista priorytetowych działań mających na celu odtworzenie krytycznych procesów biznesowych, zasady komunikacji kryzysowej z pracownikami, prasą, klientami, dostawcami, udziałowcami, ubezpieczycielem, urzędem nadzoru, a także listy kontaktowe do wszystkich zainteresowanych stron oraz listy zasobów niezbędnych do pracy w trybie awaryjnym.

Dobrą praktyką jest przeprowadzenie szkoleń dla pracowników firmy. Mają one na celu wyjaśnienie przyczyn powstania planu ciągłości działania, podstawowych zasad powiadamiania o różnego typu zdarzeniach (inne ścieżki eskalacji), miejsca zbiórek po ewakuacji oraz lokalizacji zapasowej, zakresu zadań poszczególnych osób i zespołów w strukturze zarządzania kryzysowego, miejsca, w którym zostaną ulokowanie zasoby niezbędne do odtworzenia działalności w trybie awaryjnym.

Warto, by firma zweryfikowała wdrożone rozwiązania m.in. poprzez wykonanie serii prostych testów, np. testów powiadamiania (weryfikacja list kontaktowych), przeprowadzenie warsztatów typu *walk through* polegających na wspólnym przeglądzie i weryfikacji procedur awaryjnych czy założeń do pracy w sytuacji kryzysowej. Bardzo dobrym rozwiązaniem jest przygotowanie testu symulacyjnego opartego na prostym i realnym scenariuszu, zakładającym np. pożar lub zalanie pomieszczeń firmy. W obrębie takich ćwiczeń pracownicy łatwo zweryfikują, czy założone w procedurach działania i przygotowane rozwiązania zapasowe są wystarczające, czy też należy je poprawić.

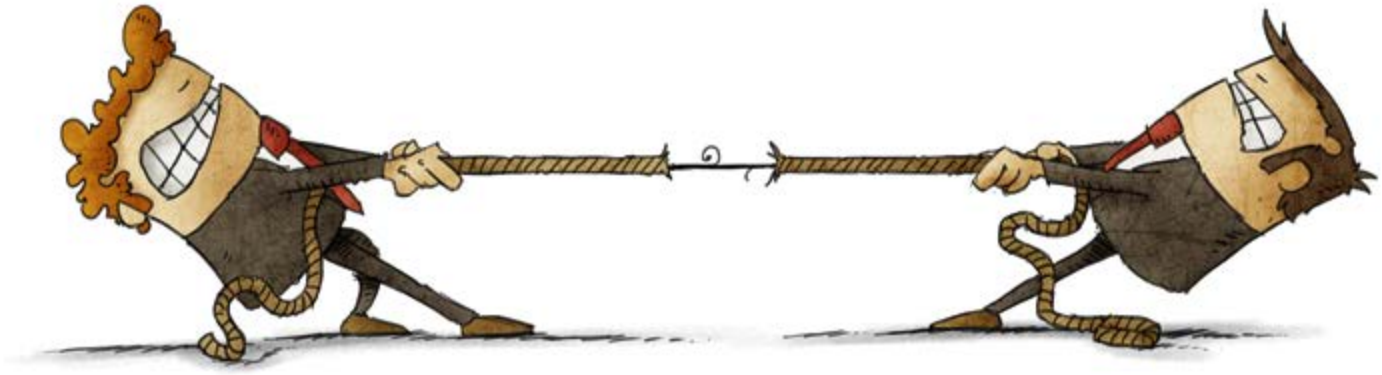
## Oczekiwanie na kolejny kryzys

Huragan Irene nie był ostatni w USA. Mieszkańcy i właściciele firm z niepokojem obserwowali rozwój kolejnych huraganów i burz tropikalnych, które potencjalnie mogły okazać się równie niebezpieczne i kosztowne. Wiele osób uspokajała myśl: „Przeżyliśmy, w przyszłości też jakoś damy radę". Inni wiedzieli, że w trudnej sytuacji mogą polegać na własnych planach i rozwiązaniach awaryjnych. W której grupie warto się znaleźć?

BIO

**Marcin Marczewski**
Prezes zarządu i architekt odporności biznesu w Resilia. Konsultant w dziedzinie zarządzania ryzykiem i bezpieczeństwem biznesu z ponad 14-letnim doświadczeniem.

# KŁÓTNIA W RODZINIE



**Nie tylko w relacjach rodzinnych dochodzi do spięć – czasami z błahych, czasami z poważnych powodów.** Również firmy doświadczają nieporozumień, które w wyniku kłótni właścicieli czy osób zarządzających przekształcają się w kryzys. **Co więcej, każda firma może znaleźć się w takiej sytuacji.**

**Michał Czuma**

Historia jednego z głośnych skandali, która jest ilustracją przedstawionego problemu, mogła wyglądać tak, jak prezentowano ją na początku konfliktu, czyli w lutym 2015 r. Tygodnik „Computerworld" na swoich łamach podał następującą informację: *Carly Fiorina przestaje pełnić funkcje prezesa i dyrektora generalnego koncernu Hewlett-Packard. Taką sensacyjną wiadomość przekazała oficjalnie rada nadzorcza koncernu. Firma wyznaczyła już jej tymczasowych następców. Przyczyną rozstania Fioriny z HP najprawdopodobniej stały się... komputery. Ich produkcja wciąż nie przynosiła firmie oczekiwanych dochodów.* W tygodniku informatycznym napisano również o różnicach w koncepcji rozwoju koncernu, szczególnie o błędnej ocenie strategii wynikającej z fuzji HP z innym koncernem z branży IT, Compaqiem. Z informacji można było wyczytać, że funkcje dyrektora generalnego (tymczasowym dyrektorem HP został wtedy szef finansowy Robert P. Wayman, związany z koncernem od ponad 36 lat) oraz prezesa zarządu (została nią Patricia Dunn) będą w firmie rozdzielone. R.P. Waymana wkrótce zastąpił Mark Hurd, który w poprzedniej firmie NCR dał się poznać jako twardy gracz, „strażnik marż i kosztów", głęboko zaangażowany w zarządzanie operacyjne.
Różnica zdań pomiędzy członkami zarządu a radą nadzorczą musiała być znaczna, gdyż C. Fiorina pożegnała się ze stanowiskiem ze skutkiem natychmiastowym, co wywołało falę spekulacji. Przyczyn nagłego jej pożegnania z firmą analitycy poszukiwali w finansach spółki. Jak donosił „Computerworld": *Największą bolączką HP są wyniki działu produkującego komputery.* Takie informacje uspokajały rynek, tym bardziej że podobne problemy przeżywali też konkurenci spółki, m.in. Dell i IBM. Ciekawscy chcieli jednak znać prawdę. Kryzysy to codzienność, większość właścicieli firm potrafi im zaradzić. Takie problemy jednak rozwiązuje się w zaciszu gabinetów, z dala od prasy i wścibskich, szczególnie w czasach, gdy informacja często zapewnia przewagę konkurencyjną. W tym przypadku było widać gołym okiem, że z HP wyciekały szczegółowe informacje i to szybkim strumieniem, czego dowodem był m.in. cytowany artykuł w prasie branżowej ujawniający szczegóły funkcjonowania HP w tamtym okresie. Spekulacje analityków rynkowych nie zapowiadały afery z podsłuchami i szpiegostwem w tle, ale mnożenie przecieków o kłótniach w zarządzie przyczyniało się obniżki akcji HP.

Jack Welch, najsłynniejszy menedżer świata, przez 20 lat kierujący amerykańskim koncernem General Electric (za jego

kadencji wartość GE wzrosła z 12 mld do 280 mld dol.), od dawna doradza niektórym firmom z listy „Fortune 500". *Kryzysy w firmach często skłaniają rozsądnych i inteligentnych ludzi do popełniania głupstw, takich jak wpadanie w panikę i szukanie winnych* – podkreślał niejednokrotnie w swoich felietonach. Wskazuje on przypadek HP jako działanie pod wpływem emocji przy braku spokojnego rozważania błędów będących skutkami pewnych decyzji i dokonywania działań naprawczych. Gdy kurz bitewny wokół tego skandalu opadł, pokuszono się o wskazanie przyczyny skandalu i wyciągnięto pierwsze wnioski. Jack Welch orzekł, że eksperci zajmujący się zarządzaniem firmą nie mają racji, twierdząc, iż rozdzielenie funkcji dyrektora generalnego (CEO) i prezesa zarządu jest korzystne dla firmy. Choć niektóre grupy monitorujące rynek przyznają firmom oceny bonusowe, warto pamiętać, iż wbrew opiniom uzasadniającym rozdzielanie tych dwóch funkcji przypadek HP udowodnił, że może ono wpływać destrukcyjnie na firmę. Dlaczego?
Wszystkie firmy, niezależnie od branży i wielkości, będą osiągały zyski, pod warunkiem że działania kierownictwa będą klarowne, zostanie określony jasny podział ról oraz zasady funkcjonowania. W przypadku HP problem polegał na tym, że firmą powinien kierować jeden dyrektor generalny, czyli Mark Hurd. Była to osoba znana i ceniona w branży, mająca wizję i strategię, dysponująca zespołem zdolnym realizować jego pomysły. Ale był też drugi decydent w osobie prezes zarządu Patricii Dunn, która próbowała na własną rękę docierać do pracowników i korzystać z potencjału firmy w celu realizacji swojego programu. Oznaczało to, że HP miało dwóch liderów, a to wcześniej czy później musiało doprowadzić do zamieszania, a później do sytuacji, kiedy to pracownicy sami wybierali opcję, która im odpowiadała. Konflikt w zarządzie firmy był więc nieunikniony. Nie wchodząc w szczegóły, Patricia Dunn zlecała prywatnym detektywom zakładanie nielegalnych podsłuchów telefonicznych, śledzenie dziennikarzy, przeszukiwanie koszy na śmieci, szpiegowanie poczty elektronicznej i umieszczanie informatorów wśród załogi. Działania te doprowadziły do złamania prawa, a wiele przypadków opartych na tamtych wydarzeniach jest przykładem, czego nie wolno robić, gdy klient prosi o wsparcie, wymuszając łamanie prawa. M. Hurd musiał znać poczynania P. Dunn, ale chyba udawał, że sprawa ta jego nie dotyczy, licząc zapewne, że ustali źródło przecieków, a w razie wpadki (lub później) wykorzysta sytuację do pozbycia się P. Dunn.
W wyniku afery, która od nazwiska zlecającej zadania prywatnym detektywom została nazwana „aferą Dunn", Dunn została zdymisjonowana, a prokurator generalny stanu Kalifornia oskarżył ją, byłego prawnika HP oraz trzech wynajętych detektywów o defraudację, kradzież tożsamości i spisek. W ramach postępowania prokuratorskiego ujawniono informacje dotyczące członków zarządu spółki, nawet niezaangażowanych w sprawę. Warto przytoczyć jedną z nich.

## Przypadek HP pokazał, że rozdzielenie funkcji dyrektora generalnego (CEO) i prezesa zarządu może destrukcyjnie wpływać na firmę.

Patricia Dunn broniła się przed Komisją ds. Energii i Handlu zajmującą się wyjaśnieniem tej sprawy, twierdząc, że nie miała nic wspólnego z nielegalnymi działaniami detektywów, którzy powinni tylko „ustalić źródło przecieków" w zarządzanej przez nich firmie. Zadania, jakie im wyznaczono, były „legalne", a ona nie „wyrażała zgody na bezprawne pozyskiwanie" np. billingów osób podejrzewanych i powiązanych ze sprawą. Bardziej skruszony prezes M. Hurd złożył m.in. oświadczenie, w którym przeprosił dziewięciu dziennikarzy, dwóch obecnych pracowników HP i siedmiu byłych lub obecnych członków zarządu HP oraz ich rodziny, których zapisy telefoniczne zostały w różnym stopniu uzyskane pod fałszywym pretekstem, określanym jako *pretexting* (wyłudzenie polegające na tym, że przestępca dzwoni do osoby, starając się pozyskać przez telefon dane umożliwiające później uzyskanie dostępu do rachunku bankowego, telekomunikacyjnego czy innego dostawcy usług).
I chociaż działania podejmowane tylko przez część zarządu miały szczytny cel, którym było ustalenie, kto był źródłem przecieków, i okazały się w pewnej mierze skuteczne (wykryto i oskarżono członka zarządu George'a Keywortha; 12 września 2006 r. zrezygnował on z pełnionej funkcji), to jednak konsekwencje nieprzemyślanych decyzji doprowadziły Hewletta-Packarda do długoletniej zapaści, utraty wartości rynkowej, reputacji i kolejnych kryzysów. Można powiedzieć, że problem, który profesjonaliści rozwiązaliby spokojnie i zgodnie z zasadami, ze względu na emocje oraz brak rozsądku i planowania pogłębił kłopoty firmy, wywołał kryzys i doprowadził do olbrzymich strat.

Bill Lockyer, prokurator generalny stanu Kalifornia, 4 października 2006 r. wniósł oskarżenie i nakazy aresztowania P. Dunn, byłego szefa etyki HP Kevina Hunsakera oraz trzech doradców zewnętrznych (detektywów). Po procesie 14 marca 2007 r. sędzia w sprawie karnej Patricii Dunn oddalił wszystkie zarzuty. K. Hunsaker i jego współpracownicy zostali skazani na kary pieniężne oraz obowiązkowe prace społeczne. Sprawy wobec osób, które były mniej lub bardziej zamieszane, toczyły się aż do roku 2012. Wpłynęły one na uchwalenie nowych regulacji, które przewidywały kary za wyłudzenia typu *pretexting*. Mark Hurd po rezygnacji z funkcji szefa koncernu nie narzekał na brak propozycji pracy. Rozstał się z firmą 6 sierpnia 2010 r. z powodu oskarżenia o… molestowanie seksualne byłej aktorki TV reality show Jodie Fisher, prywatnie jego przyjaciółki. Było to tylko parawanem, prawdopodobnie mającym na celu „zmiękczenie" go, gdyż jak czas pokazał, Hurd, żegnając się z HP (za jego odwołaniem opowiedziało się sześciu członków RN, przeciwko czterech), w zamian za „uwolnienie HP z przyszłych sporów prawnych", otrzymał „skromną" odprawę w wysokości 12,2 mln dol. oraz opcje nabytych akcji szacowanych w 2010 oku na 34,6 mln dol. Już w dniu, w którym M. Hurd złożył rezygnację, otrzymał propozycje pracy w spółkach IT i instytucjach finansowych. Został ostatecznie członkiem rady nadzorczej znanej korporacji Oracle.
Warto dodać, iż w sierpniu 2010 r. akcjonariusze HP złożyli pozew będący skutkiem odejścia Marka Hurda z korporacji. Pozew dotyczył nieokreślonych strat i zmian w ładzie korporacyjnym firmy. Poszkodowani akcjonariusze twierdzili, że HP straciło „znaczącą wiarygodność" ze względu na kontrowersje oraz zanotowało straty w wysokości 9 mld dol. w kapitalizacji ryn-

kowej po rezygnacji Hurda. Uznano też, że jego odprawa powinna być znacznie mniejsza, jeśli zwolniono go z przyczyn, jakie ujawniono opinii publicznej. Fundusz Brockton w imieniu akcjonariuszy złożył powyższy pozew przeciwko Hurdowi oraz członkom zarządu HP. Najgorzej zakończyła się sprawa Patricii Dunn. W wyniku stresu podupadła na zdrowiu, zdiagnozowano u niej chorobę nowotworową. Zmarła 4 grudnia 2011 r. w wieku 58 lat.

Z tej historii można wyciągnąć kilka wniosków. Pierwszy nasuwa się sam: zarządzając firmą, należy przewidywać konsekwencje każdej podejmowanej decyzji. Nie wolno się śpieszyć, ale jednocześnie trzeba pamiętać, że oczekiwanie, aż sprawa przyschnie, może narazić firmę na ryzyko i przynieść negatywne skutki. Nikt nie powinien oceniać właścicieli firm, którzy czasem muszą podejmować niezbyt popularne, ale na pewno ryzykowne decyzje. Warto patrzeć na własną działalność, pamiętając, że nie zawsze i nie wszystko przebiega zgodnie z planem, opinia publiczna zaś jest sędzią subiektywnym, często pochopnie i błędnie wydającym opinię. Nie wolno zapomnieć, że oceny krążące w przestrzeni publicznej mogą narazić firmę na ryzyko, którego nie da się przewidzieć. Trzeba też pamiętać, że biznes to odpowiedzialność za innych – udziałowców, pracowników, kooperantów, klientów i ich rodziny. Ich dobro wymaga decyzji czasami ryzykownych, czasami wymagających dużego wysiłku. Dlatego każda forma działalności powinna być chroniona przed zagrożeniami zarówno zewnętrznymi, jak i wewnętrznymi. Nie można jednak zlecić tego zadania amatorom, warto czasami spojrzeć na tę kwestię z pokorą.

Przy wyborze specjalistów należy zachować ostrożność. Wiele firm na rynku ma świetny PR i to jest ich największym sukcesem. Niestety są sprawy, którymi powinni się zajmować wyłącznie profesjonaliści. Jak takich wychwycić w morzu ofert? W pierwszej kolejności trzeba przetestować ich umiejętności, zlecając im najprostsze zadania. Emocje i pośpiech są złym doradcą – profesjonalista nie tylko podzieli się wiedzą, ale także pozwoli klientowi dokonać właściwego wyboru.

Zdarza się, że ocena sytuacji jest nieprawdziwa. Jeśli dostrzegamy tylko jedną stronę problemu lub jego część, z decyzją należy się wstrzymać. Największym błędem jest podejmowanie decyzji na podstawie szczątkowego, fragmentarycznego obrazu sytuacji.

Drugim istotnym zagadnieniem pozwalającym na wyeliminowanie kryzysów i nieprzewidzianych, niezbyt przyjemnych zdarzeń jest ochrona tajemnic firmy. Przedstawiona wcześniej sytuacja dotyka sporej grupy biznesmenów borykających się z problemem nieuczciwej konkurencji, a także wykorzystywaniem wewnętrznych sporów lub bezprawnych działań do własnych partykularnych celów, niespójnych z interesem spółki. Warto o tym pamiętać podczas tworzenia systemu zarządzania i podejmowania decyzji w firmie. Ktoś, kto dzisiaj jest najbardziej zaufanym pracownikiem, partnerem, jutro może stać się wrogiem z błahego, a nawet niezrozumiałego powodu. Ktoś, komu zaufaliśmy, może z przyjaciela stać się wrogiem i np. zniżyć się do szantażu, którego przedmiotem wcale nie musi być słabość czy niezgodne z przepisami działanie. To może być błąd popełniony przy okazji stworzonej przez zaufanego pracownika, który chce się zabezpieczyć na przyszłość. **Na takie sytuacje warto się przygotować, pamiętając, że żyjemy w dżungli interesów tysięcy ludzi.**

Ktoś, kto dzisiaj jest najbardziej zaufanym pracownikiem, jutro może stać się wrogiem z błahego nawet powodu. Warto o tym pamiętać podczas tworzenia systemu zarządzania i podejmowania decyzji w firmie.

Każda sytuacja kryzysowa ma swoje przyczyny – zwykle jest skutkiem zaniedbań i bagatelizowania zagrożeń. Na szczęście można je rozpoznać, gdyż każdy kryzys ma tendencję rozwojową. Nie wolno bagatelizować symptomów poprzedzających konflikt. Trzeba podejmować decyzje przeciwdziałające rozwojowi „stanów chorobowych" na wczesnym etapie diagnozowania zagrożeń. Uniknąć wielu problemów, skandali korporacyjnych czy niebezpieczeństwa pozwala m.in. przestrzeganie procedur obiegu informacji w firmie, kontrolowanie procesów i mocne przywództwo. Należy dbać o wzmocnienie firmy i wsparcie, także u wyspecjalizowanych doradców zewnętrznych. W przeciwnym razie to, co budujemy latami, może runąć. Trzeba o tym pamiętać.

BIO

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

# POLSKIE FIRMY ZA GRANICĄ
# KOSZTOWNY GRZECH ZANIECHANIA

Cieszą informacje o firmach polskich, które biznesową aktywność przenoszą do innych krajów, często odległych prawnie i kulturowo od standartów europejskich. **Inwestują tam dziesiątki, a nawet setki milionów złotych, często zapominając jednak o podstawowych zasadach zapewnienia choćby minimalnego bezpieczeństwa własnej działalności.**

**Sebastian Błażkiewicz**
prezes SASMA


Za przykład może posłużyć firma, która duże środki zainwestowała na Wschodzie, a po kilku latach wycofała się z inwestycji, tracąc know-how, które zostało skradzione wraz z dokumentacją i rynkiem zbytu. Kolejny przykład – nie tak dawny – to pucz w Turcji... Czy firmy polskie świadczące w tym kraju swoje usługi były przygotowane na taki rozwój sytuacji? Prewencja zawsze kosztuje mniej niż reagowanie po fakcie, i o tym należy pamiętać. Na co w aspekcie bezpieczeństwa biznesu powinny zwracać uwagę firmy planujące ekspansję na rynki zagraniczne?

## SIEDEM PODSTAWOWYCH ZASAD POSTĘPOWANIA

**1.** Rozpoznanie uwarunkowań politycznych i geograficznych – niepokoje społeczne, polityczne bądź częste kataklizmy naturalne mają duży wpływ na bezpieczeństwo biznesu. Kluczową rolę odgrywa tu tzw. *business intelligence*.

**2.** Weryfikacja kontrahentów – wszystkich osób i firm, z którymi są prowadzone rozmowy biznesowe, a także osób, które mają objąć stanowiska kierownicze.

**3.** Bezpieczeństwo informacji – należy zapewnić ochronę know-how, ponieważ obecnie informacja jest cenniejsza niż złoto.

**4.** Bezpieczeństwo podróży – aby nie czytać w prasie i nie oglądać w telewizji np. zdjęć pracowników firmy porwanych przez terrorystów lub zastanawiać się, gdzie się schronić w przypadku rozruchów, nie wolno zaniedbywać tego punktu.

**5.** Bezpieczeństwo łańcucha dostaw – duży problem występuje zwłaszcza w krajach afrykańskich i wschodnich; brak dostaw jest równoznaczny z kosztownymi przerwami w produkcji.

**6.** Bezpieczeństwo fizyczne plus zabezpieczenia techniczne.

**7.** Inne – w zależności od regionu czy kraju.

Należy pamiętać o podstawowych zasadach postępowania.
Tych kilka punktów z wielkiego katalogu należy przygotować, zanim firma ruszy na podbój rynków zagranicznych. Oczywiście można je bagatelizować, wierząc, że w przypadku kłopotów pomoże ambasada... i modlitwa.
Z własnego doświadczenia mogę jednak powiedzieć, że nie ma nic bardziej mylnego i kosztownego, jak wiara w szczęście (założenie, że „mnie się nic nie stanie") oraz pomoc dyplomatyczna. Ponadto koszty „gaszenia pożaru" są gigantyczne i zazwyczaj doprowadzają firmę do upadku.
Warto również pamiętać o zasadzie ograniczonego zaufania. Bez względu na to, gdzie zostaną zainwestowane fundusze, nawet jeśli w powszechnej opinii dane miejsce jest bezpieczne, pod żadnym pozorem nie wolno rezygnować z tworzenia równoległego systemu bezpieczeństwa.

> Prewencja zawsze kosztuje mniej niż reagowanie po fakcie, i o tym należy pamiętać.

Jak zatem zbudować system bezpieczeństwa?
Kluczowa jest tu współpraca ze specjalistami w zakresie bezpieczeństwa biznesu mającymi doświadczenie międzynarodowe. Nawet wysokiej klasy eksperci niczego nie zrobią w obcym kraju bez nawiązania lokalnych dobrych relacji. Działając po omacku, tylko zwiększają ryzyko. Przykład: wynajęcie niesprawdzonych lokalnych podwykonawców (ich pomoc jest zawsze niezbędna). Istnieje duże ryzyko, że staną się źródłem wycieku informacji, gdyż bardzo często konkurencja stosuje taktykę podesłania „bezpieczników" działających na dwa fronty.
Przed powierzeniem biznesu w ręce doradców należy przeprowadzić ich dokładną weryfikację. W tym celu warto posłużyć się prostymi narzędziami, takimi jak:
– weryfikacja CV osób z zarządu (doświadczenie itp.),
– referencje (w tym przypadku międzynarodowe),
– weryfikacja referencji (kontakt ze wskazanymi osobami czy firmami),
– rozmowa na temat kraju będącego celem prowadzenia biznesu (ważne są konkrety).

Przedsiębiorcy polscy – wzorem dojrzałych firm zachodnich – nie mogą popełniać kosztownego grzechu zaniechania. Bezpieczeństwo swoich firm muszą powierzać jedynie profesjonalistom.

BIO

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

# BRAND PROTECTION

## TRENDY I WYZWANIA

**Firmy borykające się z problemami podrabiania swoich produktów spotykają się z zadziwiającą pomysłowością osób po drugiej stronie barykady.** Czasem elementy, które dla konsumenta są oczywistym wyznacznikiem oryginalności i jakości produktu, to starannie wykonany falsyfikat lub produkt prawdziwy, lecz niepełnej wartości, który nigdy nie powinien trafić na rynek.

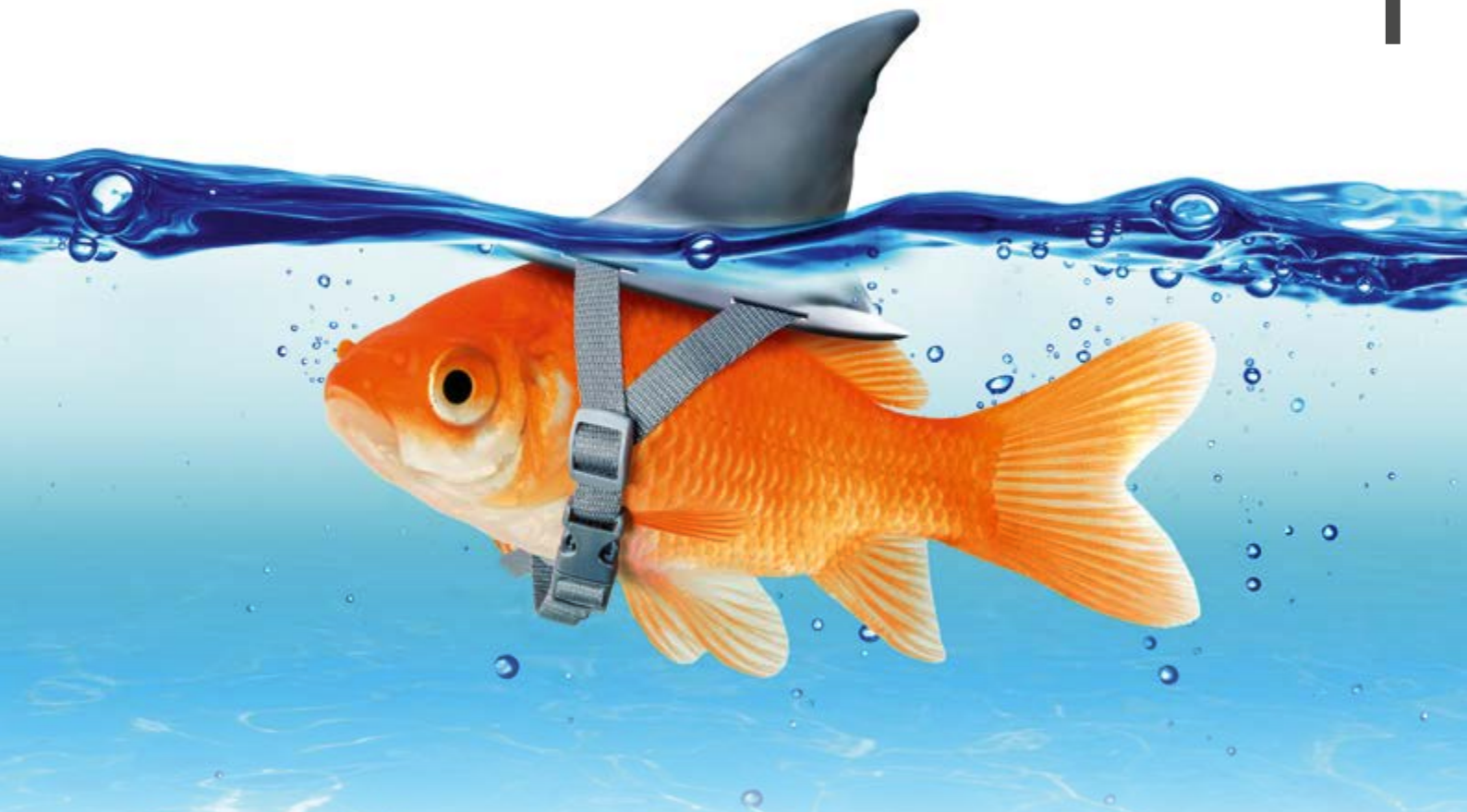
**Agnieszka Socha**
SASMA

Działania z zakresu ochrony marki i walki z podróbkami to istotny aspekt bezpieczeństwa biznesu. Kupowanie podrobionych towarów jest groźne nie tylko dla wizerunku i finansów firmy, ale także może zagrażać życiu i zdrowiu klientów. O skali i złożoności problemu pisaliśmy już w „a&s Polska" (1/2017). W tej części omówimy nowe trendy w procederze fałszerstwa oraz wyzwania, z jakimi muszą się mierzyć security managerowie.

### METODY PODRABIANIA...

**Oryginalny towar umieszczany w podrobionym opakowaniu – takie działania mogą wskazywać, że ktoś dysponuje dostępem do legalnego źródła produktu i nieupoważniony wynosi go z miejsca produkcji. Być może są to produkty, które z jakiegoś powodu (np. wady fabrycznej lub błędu w wykonaniu) zostały przeznaczone do zniszczenia lub (w przypadku żywności czy leków) zostały zanieczyszczone bądź upłynął ich termin ważności. Opakowania do złudzenia przypominające oryginały mają świadczyć, że towar jest w 100% wartościowy.**

- Oryginalne opakowanie z podróbką w środku – może wskazywać na fakt, że ktoś ma dostęp do oficjalnego procesu pakowania lub już gotowych opakowań. Wynosi je w dużych ilościach, po czym umieszcza w nich podrobiony towar (spreparowane przedmioty lub produkty niepełnowartościowe).
- Podrobione opakowanie i podrobiony towar – to najczęściej spotykana metoda fałszowania towarów. Często wskazuje na fakt, że ktoś dysponuje linią produkcyjną i prowadzi zorganizowaną nielegalną działalność na większą skalę.
- Wykorzystanie prawdziwej dokumentacji – znane są przypadki przedstawiania prawdziwej dokumentacji oryginalnych partii produktów, które po dostaniu się w niepowołane ręce są wykorzystywane do uwierzytelniania podrobionych towarów. Mogą to być dokumenty oryginalnych towarów, które już trafiły do obrotu. Taki dokument jest używany do uwierzytelnienia kilku lub nawet kilkunastu nielegalnych partii podróbek.



## Kanały i drogi dystrybucji

### Chiny wielką fabryką podróbek

Podrabiane produkty mogą pochodzić z każdego miejsca na świecie, ale to właśnie Chiny są uznawane za największy rynek produkcji podrobionych przedmiotów. Ku rozpaczy specjalistów od ochrony marki Chińczycy opanowali sztukę kopiowania do perfekcji. Teoretycznie prawo własności intelektualnej w Państwie Środka odpowiada światowym standardowym, jednak w praktyce właściwie nie jest egzekwowane.

### Transport morski i lądowy przoduje

Podrobione towary są najczęściej transportowane drogą morską i lądową. Kontenerowce przewożą ogromne ilości materiału, a nierzadko kontrola, ze względu na ilość i sposób załadunku, nie jest dokładna. Transport lądowy nie zawsze jest łatwy z powodu odległości i nie tak szybki jak drogą lotniczą, lecz z pewnością należy do najtańszych. Podróbki zalewają Stary Kontynent poprzez europejskie porty morskie, często w krajach wschodnich takich jak Bułgaria, Rumunia czy Ukraina, a także są transportowane tirami. Coraz częstszym sposobem rozprowadzania podrobionych towarów są przesyłki pocztowe, co wynika ze wzrostu popularności zakupów przez internet.

> „Podróbkowi przestępcy" zawsze będą krok przed security managerami, wymyślając coraz nowsze sposoby na zarobienie pieniędzy.

### Handel równoległy

Nielegalne działania związane z rozprowadzaniem leków, ich podrabianiem i handlem internetowym można śmiało nazwać przestępczością zorganizowaną. Zyski z takiej działalności niejednokrotnie przekraczają uzyskane np. z handlu narkotykami. Jest to tak dochodowy biznes, że zajmują się nim na całym świecie świetnie funkcjonujące i zorganizowane mafie farmaceutyczne. W ich działania często są zaangażowani wysoko postawieni urzędnicy państwowi.

Legalną formą obrotu towarami farmaceutycznymi na terenie Europejskiego Obszaru Gospodarczego (EOG) jest import równoległy leków. Polega on na zakupie oryginalnych towarów wyłącznie w uprawnionych hurtowniach farmaceutycznych w kraju, gdzie są one tańsze, a następnie sprzedaży w kraju, w którym ich cena jest wyższa. Różnicę stanowi jednak opakowanie, co niestety otwiera drzwi pomysłowym przestępcom.

Parający się tym procederem często produkują podrabiane leki i sprzedają je w innym opakowaniu, twierdząc, iż to oryginalny lek, lecz pochodzący z importu równoległego.

### Polska również krajem produkcyjnym

Trzeba mieć świadomość, że Polska nie jest jedynie krajem tranzytowym podróbek. Jest rynkiem zarówno nabywczym, jak i produkcyjnym. Potwierdzają to liczne informacje w mediach dotyczące zamykanych przez organy ścigania nielegalnych linii produkcyjnych znanych marek kosmetyków, leków czy alkoholi.

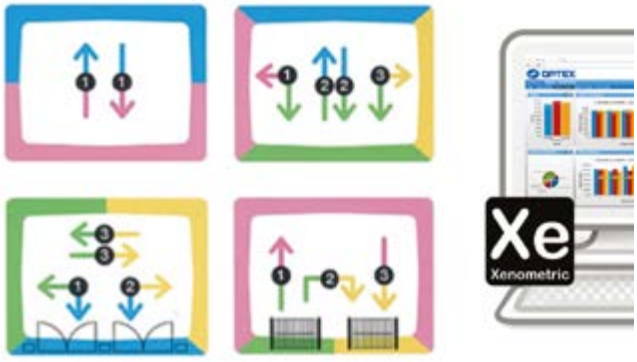
Niestety „podróbkowi przestępcy" zawsze będą krok przed security managerami, wymyślając coraz nowsze, najdziwniejsze i niewyobrażalne czasem sposoby na zarobienie pieniędzy. Ważna jest jednak konsekwencja – w walce z podrabianymi towarami liczą się działania prewencyjne oraz odpowiednio przygotowany i prowadzony program ochrony marki.


BIO

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

# Akribos: licznik przepływu osób z dedykowanym oprogramowaniem do analizy danych Xenometrix

**Model Akribos jest wewnętrzną kamerą 3D do liczenia przepływu osób. Główna funkcjonalność urządzenia wiąże się z możliwością śledzenia złożonego ruchu w czasie rzeczywistym (wejście/wyjście – w prawo/w lewo/na wprost).**




*Akribos określa przemieszczanie osoby w czterech kierunkach, a Xenometrix zapewnia przejrzystą i łatwą do interpretacji wizualizację danych*

Automatycznie przesyła dane przez TCP/IP w formacie XML lub TXT, wykazując dużą odporność na zakłócenia spowodowane cieniami czy zmianami oświetlenia.
Kamera umożliwia analizę przepływu osób. Może być wykorzystywana w takich miejscach, jak centra handlowe, sklepy wielkopowierzchniowe, obiekty użyteczności publicznej, centra konferencyjne i wystawowe oraz obiekty transportowe (dworce, lotniska itp.). Innym zastosowaniem jest monitorowanie liczby osób w budynku na potrzeby ewakuacji.
W ofercie firmy Xenometrix, będącego partnerem, pojawiło się oprogramowanie do analizy danych generowanych przez licznik przepływu osób OPTEX Akribos. Jest ono dostępne w wersji instalowanej na komputerze lokalnym lub w chmurze danych. Istnieje możliwość pobrania 30-dniowej wersji próbnej.

Więcej na: www.optex.com.pl

# DAHUA: *Omnia Panorama Videre*

**W systemach monitoringu miejskiego często spotykanym urządzeniem są kamery na głowicach obrotowych. Mogą dozorować rozległe obszary dzięki swobodzie określania kierunku obserwacji oraz stopnia powiększenia optycznego.** Pozwala to w pewnych warunkach zastąpić wiele kamer stacjonarnych. Ta właściwość głowic obrotowych jest jednocześnie ich wadą. Skupienie się na podglądzie wybranego miejsca oznacza utratę podglądu innych regionów.
Rozwiązaniem, które ma równocześnie zalety głowic obrotowych i urządzeń stacjonarnych, są kamery panoramiczne Dahua IPC-PFW8601-A180 pozwalające na obserwację sceny o szerokości 180°. Tak szeroki kadr jest możliwy dzięki zastosowaniu trzech przetworników obrazowych o rozdzielczości 2 Mpix, każdy wyposażony w oddzielną optykę. Algorytmy Dahua Technology odpowiedzialne za przetwarzanie sygnału tworzą z trzech składowych zespolony obraz panoramiczny 180° o sumarycznej rozdzielczości 6 Mpix. W rzeczywistych instalacjach pozwala to zastąpić kilka stacjonarnych punktów kamerowych. Wykorzystanie wysokoczułych przetworników Sony Starlight zapewnia wyjątkową jakość obrazu kolorowego w warunkach nocnych. Gdy oświetlenie staje się niewystarczające, kamera może przejść w tryb monochromatyczny po załączeniu wbudowanego promiennika podczerwieni. W przypadku scen o dużej dynamice jasności doskonale sprawdza się funkcja True WDR 120 dB. Obudowa kamery ma klasę


szczelności IP67, klasę wandaloodporności IK10 i zakres temperatury pracy od -40°C do +60°C. Może pracować w trudnych warunkach środowiskowych, jest odporna na uszkodzenia mechaniczne.
Pracę kamery panoramicznej wspomaga wbudowana analityka wizyjna: detekcja twarzy, zliczanie osób, badanie stref aktywności (*Heat Map*), wykrywanie przekroczenia wirtualnej bariery oraz detekcje intruza, kradzieży czy pozostawienia przedmiotu oraz obiektu.
Kamery panoramiczne Dahua Technology są w stanie współdziałać z głowicami obrotowymi. Generowany kadr obrazu o szerokości 180° pozwala operatorom na podgląd pełnej sceny i selekcje jej fragmentów, na które następnie ogniskuje się kamera obrotowa (tzw. *Smart Tracking*). Ta funkcjonalność jest realizowana w trybach ręcznym ( przez osobę obsługującą) albo automatycznym (po wyzwoleniu detekcją ruchu lub zdarzeniem analityki wizyjnej).
Dzięki możliwościom kamera panoramiczna Dahua Technology oferuje znakomitą efektywność pracy i doskonałą skuteczność obserwacji, a zdolność monitorowania rozległych obszarów pozwala zredukować zarówno koszty instalacyjne, jak i sprzętowe.

# Małe zmiany, wielkie oszczędności. Zamki ABLOY LOW ENERGY

**Koszty utrzymania firmowego biura w dużej mierze zależą od bieżących rachunków za energię elektryczną. Jej zużycie rośnie wraz z rozwojem gospodarczym i poprawą standardów życia w firmach i gospodarstwach domowych.Jakie nowoczesne rozwiązania, poza najprostszymi sposobami oszczędzania energii, proponuje rynek?**

Zamki ABLOY LOW ENERGY LOCKS pozwalają zoptymalizować zużycie prądu podczas codziennych czynności. Zmiany można zauważyć już po krótkim okresie ich użytkowania. W porównaniu do standardowych zwór elektromagnetycznych zapewniają oszczędność na poziomie blisko 99% w rocznym bilansie zużycia prądu. Obliczenia wykonano na przykładzie biurowca z 1000 przejść KD i szacunkowej liczbie 100 dziennych otwarć trwających po 10 s. Przy tych założeniach tradycyjna zwora pobiera rocznie 52 kWh energii, natomiast LOW ENRGY LOCKS jedynie 0,018 kWh. Przyjmując cenę 0,17 euro/kWh, oznacza to oszczędność prawie 9000 euro rocznie przy jednoczesnym zachowaniu funkcjonalności konwencjonalnych rozwiązań.

Energooszczędne zamki ABLOY LOW ENERGY LOCKS są produktem nowatorskim w branży zabezpieczeń. Tradycyjne rozwiązania stale pobierają energię, nawet gdy są nieużywane. Zamki ABLOY zużywają ją jedynie w momencie zmiany statusu blokady. Nie wymagają integracji, są kompatybilne z innymi elementami systemu zabezpieczeń – nie ma konieczności wymiany całego systemu, jedynie pojedynczych zamków.

Urządzenia LOW ENERGY LOCKS doskonale sprawdzają się w drzwiach o dużym natężeniu ruchu oraz w miejscach newralgicznych, takich jak wyjścia ewakuacyjne czy drzwi ppoż. Mogą być stosowane w drzwiach zarówno drewnianych, jak i stalowych, a ich instalacja nie jest czasochłonna.

Gwarantują pełną wygodę obsługi, ponieważ mogą być sterowane elektrycznie w systemie kontroli dostępu oraz za pomocą klawiatury kodowej, przycisków lub timera.

# Konferencja Hanwha Techwin w Barcelonie


**W obecności ponad 200 delegatów na konferencji WiseNet w Barcelonie 14 marca poinformowano o wprowadzeniu lepszych warunków gwarancyjnych dla uczestników programu partnerskiego Hanwha Techwin – STEP.**
Partnerzy ze statusem Srebrnym, Złotym lub Platynowym otrzymują 5 lat gwarancji, obejmującej elementy urządzeń i bezpłatny serwis przy naprawie wszystkich kamer i rejestratorów sieciowych, wyłączając usterki obiektywów z regulacją zoomu i ostrości, silników pan/tilt i złącz obrotowych kamer PTZ oraz dysków twardych rejestratorów. Te elementy dalej będą objęte 3-letnią gwarancją.

**Nowe kamery serii WiseNet X**
WiseNet X to seria 26 nowych 2- i 5-Mpix kamer wykorzystujących kompresję H.265. Są wyposażone w procesor o największej mocy obliczeniowej, jaki kiedykolwiek zastosowano w linii kamer IP. Dzięki nowej architekturze opartej na jednym chipsecie kamery WiseNet X charakteryzują się doskonałą wydajnością przetwarzania obrazu oraz mnogością funkcji i funkcjonalności:
- WDR bez artefaktów wywołanych ruchem obiektów,
- doskonałe działanie w trudnych warunkach oświetleniowych,
- WiseStream II redukujący ilość wytwarzanych danych wideo nawet o 99%,
- dwa gniazda na karty pamięci pozwalające umieścić w kamerze nawet 512 GB pamięci do nagrań,
- stabilizacja obrazu oparta na czujniku przyspieszenia,
- analityka audio rozpoznająca takie dźwięki, jak strzały z pistoletu, eksplozje, krzyki, tłuczone szkło.


**Nowa kamera serii WiseNet P**
Seria kamer WiseNet P powiększyła się o model szybkoobrotowy 4K PTZ z wbudowanym oświetlaczem IR. PNP-9200RH wyróżnia się 20x zoomem optycznym i kompresją H.265. Ma wbudowany oświetlacz IR o zasięgu 200 m.
Funkcjonalność kamery podnosi pełen zakres obrotu w poziomie n x 360°, ruch w płaszczyźnie pionowej 190° oraz ulepszona funkcja automatycznego śledzenia obiektów.
Kamera PNP-9200RH może być stosowana w dowolnych warunkach środowiskowych na zewnątrz pomieszczeń (IP66, IK10). Dzięki zastosowaniu przetwornika ze skanowaniem progresywnym dostarcza wyraźne i ostre obrazy poruszających się obiektów i pojazdów.
W kamerze zaimplementowano funkcje dostępne w innych modelach serii P: dwukierunkowy tor audio, maski prywatności, funkcję *Defog* oraz gniazdo na kartę pamięci SD.
Funkcje analizy obrazu (wykrywanie pojawiania się i znikania przedmiotu, detekcja poziomu sygnału audio wraz z przesyłaniem metadanych) są fabrycznie zaimplementowane w kamerze. Moc obliczeniowa procesora DSP kamery pozwala użytkownikom na wybór innych aplikacji do analityki obrazu wideo spełniających ich indywidualne potrzeby.

# Piąta edycja WiseNet Star 2017

**Polski zespół Hanwha Techwin Europe (dawniej Samsung) zorganizował piątą już, jubileuszową edycję Samsung STAR, tym razem pod nową nazwą i marką. W konferencji 29 marca w Centrum Olimpijskim w Warszawie uczestniczyło 220 osób.**
Nowe kamery 4K serii P, premiera serii X z procesorem WiseNet 5, najnowsza panoramiczna kamera wieloobiektywowa, rodzina nowych rejestratorów sieciowych serii P, innowacyjne technologie w nowej wersji oprogramowania SSM 1.6 czy nowy system rozpoznawania tablic rejestracyjnych z identyfikacją kraju i kontrolą dostępu – to tylko niektóre z poruszonych na konferencji tematów.
Gośćmi tegorocznej edycji WiseNet była brytyjska firma Veracity, której rewolucyjny system rejestracji sekwencyjnej, zintegrowany z programowaniem Hanwha SSM, zyskał uznanie ekspertów międzynarodowych.

# Z „Pierścieniem Patrioty” w tle

**Noworoczne spotkanie Krajowego Stowarzyszenia Ochrony Informacji Niejawnych (KSOIN) oraz Stowarzyszenia Wspierania Bezpieczeństwa Narodowego połączyło obchody Dnia Ochrony Informacji Niejawnych.**

W pewnym sensie bohaterem spotkania był „Pierścień Patrioty”. To srebrny sygnet z napisem odnoszącym się do miłości ojczyzny: *Amor Patriae Nostra*. Oba stowarzyszenia honorują nim zasłużonych dla ojczyzny. Jeden znajduje się już w zbiorach sztuki na Jasnej Górze, kolejny na tegorocznej aukcji dla Wielkiej Orkiestry Świątecznej Pomocy został wylicytowany za blisko 10 tys. zł.

„Pierścień Patrioty” wręczono m.in. senator Annie Marii Anders, sekretarz stanu w KPRM i pełnomocnik premiera ds. dialogu międzynarodowego oraz przewodniczącej Rady Ochrony Pamięci Walk i Męczeństwa. Sygnet otrzymał także Janusz Onyszkiewicz – polityk, matematyk, himalaista, dwukrotny szef MON. Uhonorowano prof. Leszka Żukowskiego, powstańca warszawskiego, prezesa Światowego Związku Żołnierzy AK, oraz Włodzimierza Sokołowskiego, byłego oficera polskiego wywiadu, dziś popularnego autora wysokonakładowych książek o tematyce szpiegowskiej, które pisze pod pseudonimem Vicent V. Severski.

Na spotkaniu nie zabrakło treści merytorycznych. Były to w kolejności wystąpień: „Kształtowanie się ochrony informacji niejawnych w latach 1999–2016” (Tomasz Borkowski) i „Ochrona Danych Osobowych wczoraj, dziś i jutro” (Andrzej Lewiński). O zagrożeniach terrorystycznych mówił ciekawie Dariusz Deptała.

Noworoczne spotkanie członków i sympatyków stowarzyszeń odbywa się tradycyjnie na terenie Warszawskiego Przedsiębiorstwa Geodezyjnego, właściciela jedynego w Polsce Muzeum Geodezji. Oba są zlokalizowane w historycznej stołecznej kamienicy u zbiegu placu Trzech Krzyży oraz Nowego Światu i Książęcej.

*Tekst i foto: Andrzej Popielski*

# Różne typy obiektów i sposoby ich zabezpieczenia – konferencja EBS

**Firma EBS od 7 lat organizuje coroczne spotkania branżowe. Początkowo tylko dla największych klientów, obecnie odbiorcą treści są wszystkie agencje ochrony powiązane z siecią dystrybucji EBS lub zainteresowane poruszaną tematyką.**

Konferencja zgromadziła w tym roku prawie 200 osób z 78 firm. Ta edycja była wyjątkowa – agenda obejmowała nie tylko najważniejsze obecnie problemy i zagadnienia rynku ochrony, ale również wskazywała rozwiązania i kierunki rozwoju.

Wysoki poziom merytoryczny tegoroczne spotkanie zawdzięcza niebanalnemu gronu ekspertów (m.in. z Auchan Polska, McDonald's, Raiffeisen, Pekao SA) oraz bogatej ofercie produktowej partnerów: firmy Orange, Hikvision, Protect oraz DMSI.

Firma EBS, pomysłodawca i organizator wydarzenia, postawiła sobie za cel kreowanie i wywieranie pozytywnego wpływu na rynek security w Polsce. Szersze portfolio produktów powstaje w efekcie dialogu z uczestnikami i partnerami, co przekłada się na lepszą jakość usług i poszerzenie wiedzy będącej kluczem do sukcesu, zwłaszcza że branża stoi na progu zmian prawnych i technologicznych.

Niektóre wystąpienia prelegentów wzbudziły wiele gorących emocji, co może przyczynić się do szybszego otwarcia się na zmiany zachodzące na rynku ochrony.

Patronem konferencji byli m.in. stowarzyszenie Polski Związek Pracodawców Ochrona, firma SASMA oraz redakcja „a&s Polska".

# Dni Otwartej Platformy Milestone Polska

**Na spotkaniu z cyklu Dni Otwartej Platformy Milestone w Polsce, które odbyło się 29 marca w Warszawie, firma Milestone Systems wraz z partnerami technologicznymi (2N, Aten, Ela-compil, Hertasecurity, Hikvision, IPS, NEC, Nedap, Optex, Qnap, Raytec, Vivotek , WD) zademonstrowała najnowsze rozwiązania zintegrowanych systemów zabezpieczeń.**

Spotkanie było doskonałą okazją do stworzenia sieci znajomych i nowych kontaktów biznesowych. Można było dowiedzieć się, jak wykorzystać rozwiązania branżowe zintegrowane z urządzeniami firm partnerskich z ekosystemu Milestone. Przedstawiono technologię ukazującą możliwości integracji oprogramowania XProtect® z rozwiązaniami partnerów. Zaprezentowano harmonogram produktów oraz aktualizację na temat kampanii na rzecz sprzedaży.

**Anders Johansson, Director Eastern/Central Europe, Milestone Systems**

# Autoryzowani Partnerzy Schrack Seconet w Polsce

**Schrack Seconet Polska organizuje coroczne spotkania partnerów biznesowych reprezentujących firmę na terenie kraju. Tegoroczna edycja odbyła się 9–10 marca. Wzięli w niej udział przedstawiciele szczebla zarządzającego z kilkudziesięciu firm z całego kraju ściśle współpracujących z producentem.**

Spotkania Autoryzowanych Partnerów Schrack Seconet Polska mają długoletnią tradycję. W tegorocznym wzięło udział kilkudziesięciu przedstawicieli firm partnerskich. Prezentacje dotyczyły m.in. wyników sprzedaży, zrealizowanych najciekawszych obiektów referencyjnych, analizy rynku oraz nowości produktowych.
**Tytuł Partnera Roku przyznano firmie RS-System z Michałowic za najlepszy wynik w sprzedaży systemów sygnalizacji pożarowej Schrack Seconet oraz wysoką jakość usług.**
Pod koniec ub.r. lista firm partnerskich Schrack Seconet w Polsce została zmodyfikowana. Nadal podstawowym statusem pozostał Autoryzowany Partner. Firmy wyróżniające się w tym gronie, spełniające najbardziej restrykcyjne warunki autoryzacji, tworzą dziś grupę Autoryzowanych Partnerów Wiodących. Statusy autoryzacji są przyznawane na dwa lata, dlatego rok 2016 zakończono weryfikacją wszystkich firm z grona Partnerów, a także aktualizacją uprawnień dla inżynierów w nich zatrudnionych. Kilka przedsiębiorstw – dzięki wysokiej jakości współpracy, bardzo dobrej kondycji finansowej, pozytywnym wynikom regularnych audytów producenta, wysoce wykwalifikowanej kadrze specjalistów, bogatej liście referencyjnej wspólnie zrealizowanych obiektów – zmieniło swój dotychczasowy status na wyższy.
Do Autoryzowanych Partnerów Wiodących (APW) dołączyły cztery firmy, a grono to liczy obecnie 18 firm.
Do Autoryzowanych Partnerów Schrack Seconet w Polsce w 2017 r. dołączyło pięć firm posiadających dotychczas status Partnera Handlowego. Z kolei kilku przedsiębiorstwom z grona Autoryzowanych Partnerów w latach 2015–2016 nie udało się utrzymać statusu i kontynuują współpracę z producentem na zasadach Partnera Handlowego.
Obecnie lista Autoryzowanych Partnerów Schrack Seconet obejmuje 33 firm z całego kraju, łącznie cała grupa (z APW) liczy 51 przedsiębiorstw.
Szczegóły dot. nowej polityki sprzedaży oraz uprawnień każdej z trzech grup partnerów Schrack Seconet w Polsce na: www.schrack-seconet.pl.

Ostatnie miesiące ub.r. w firmie Schrack Seconet Polska były również bardzo intensywnym okresem szkoleniowym. W związku z weryfikacją listy firm partnerskich ważność straciły uprawnienia dla inżynierów zatrudnionych w tych przedsiębiorstwach. W listopadzie, grudniu i styczniu zostało przeszkolonych ponad 400 inżynierów, którzy podczas szkoleń aktualizacyjnych mieli okazję zapoznać się z najnowszymi funkcjami systemowymi i programowymi rozwiązań Schrack Seconet.

Obecnie cykl szkoleń projektowych jest kontynuowany w całej Polsce. Nowością jest wprowadzenie zagadnień z tematyki systemów DSO, które od ubiegłego roku uzupełniły ofertę Schrack Seconet. Plan szkoleń i formularz rejestracji online na: www.schrack-seconet.pl

# Cykliczne Spotkania Projektantów Alpol

**Katowickie spotkanie 3 marca br. zainaugurowało Cykliczne Spotkania Projektantów organizowane przez firmę Alpol.**
Spotkanie poświęcone merytorycznym aspektom nowoczesnego projektowania instalacji systemów zabezpieczeń ppoż. cieszyło się dużym zainteresowaniem – w CSP uczestniczyło prawie 100 osób. Swoje prezentacje przedstawili Alpol (organizator) oraz partnerzy:
**Detectomat**: innowacyjny system sygnalizacji pożarowej – centrala SSP InteliDetect DC3500 oraz AMFE, autonomiczny system gaszenia,
**AFG**: systemy oddymiania oraz systemy odcięć ogniowych,
**Q07**: zasysająca detekcja dymu w serwerowniach, komorach trafo i szybach windowych,
**Kabe**: KBZB-38 – zasilacz do systemów SSP, kontroli rozprzestrzeniania dymu i ciepła oraz urządzeń ppoż. i automatyki pożarowej,
**Cerbex**: nowoczesne rozwiązania w zakresie sterowania i kontroli urządzeń ppoż., centrala CX-1201, wymagania,
**Ifter**: nowa jakość w integracji i wizualizacji systemów bezpieczeństwa i automatyki budynkowej.
Kolejne CSP odbędą się:
• w Poznaniu – 19.05.2017,
• w Warszawie – 22.09.2017,
• we Wrocławiu – 20.10.2017.
Więcej na **www.csp-alpol.pl**

# Jak guma

**Słowo terroryzm jest boleśnie modne.** Niedawno Bill Gates na konferencjach w Davos i Monachium mówił o bioterroryzmie. Nie jesteśmy na niego przygotowani, a jest groźniejszy niż tysiąc samobójców.

Epidemie bywały straszniejsze niż uśmiercające możliwości broni atomowej (poza totalną zagładą). Grypa, tzw. hiszpanka, po I wojnie światowej zabiła 50– 100 mln ludzi; więcej niż ta wojna. Gates uważa, że prawdopodobieństwo wybuchu nowej pandemii jest duże. Może być tworzona w komputerach terrorystów produkujących np. syntetyczną odmianę wirusa ospy lub śmiertelnego szczepu grypy. Lekceważący związek pomiędzy bezpieczeństwem zdrowotnym a międzynarodowym nie zauważają faktu, że epidemia granicami państw się nie przejmuje.

Bezpieczeństwo – jak dowcipnie określił je pewien właściciel firmy security – ma cechę wspólną z gumą od majtek: dużą rozciągliwość. Pojęcie można rozciągnąć chyba na większość dziedzin życia. Wymieńmy bezpieczeństwo państwa, publiczne, militarne, przemysłowe, finansowe, informacji, telekomunikacji i świata cyfrowego, infrastruktury krytycznej, energetyczne, transportowe, zdrowotne, osobiste, mienia itd. Im bardziej zawężimy filtry szczegółowości, tym więcej specjalności wypłynie na wierzch.

W felietonach w „a&s Polska" będę je zauważać. Lekko i powierzchownie, bo taka jest uroda gatunku. Czasem, bo świat jest kolorowy, będą to jednostkowe ciekawostki. Ale i takie sprawy, które zagrażają dużym grupom, a nawet ludzkości. Może padnie do niej pytanie: Dlaczego jest tak głupia? Zamierzam dostrzegać także rozwiązania oraz wynalazki techniczne sprzyjające poprawie bezpieczeństwa.

Do tej pory słyszałem tylko o Amerykanach wjeżdżających pod pociąg albo do rzeki, bo tak im pokazywał drogę GPS; ale oni nie są wyjątkowi. Również inne techniczne wytwory mają wpływ na bezpieczeństwo. Psychiczną siłę oddziaływania kamer telewizji pokazało zabójstwo przyrodniego brata dyktatora Korei Płn. być może będące nową i tanią metodą zabójstwa na zlecenie. Prawdziwy przebieg wydarzeń MOŻE wyjaśni śledztwo. Ale możliwe że *modus operandi* było takie: sprawca wytypował na lotnisku dwie przypadkowe kobiety i za „parę groszy" skusił do udziału w rozrywkowym programie typu ukryta kamera (o ile nie były to agentki reżimu z odpowiednią legendą). Miały w tej zabawie posmarować olejkiem dziecięcym twarz przechodnia. Kosmetyk był paskudniejszą mutacją morderczego sarinu, gazu bojowego o działaniu paraliżująco-drgawkowym.

W TVN24 obejrzałem felietonik filmowy o 300-kamerowym monitoringu wizyjnym w brukselskiej dzielnicy Molenbeek, nazywanej wylęgarnią dżihadystów. Pokazano kilka jego możliwości, dla fachowców zwyczajnych, np. detekcji po kolorach ubrań i samochodów. Daną osobę można obserwować właściwie od jej wyjścia z domu. A to już jest ważna informacja, być może świadcząca o pokryciu obrazem tej newralgicznej dzielnicy, stolicy Belgii i europejskiej dyplomacji.

Komisja Europejska powiadomiła, że europejski system nawigacji satelitarnej zaczął oferować pierwsze usługi. Galileo jest konkurentem amerykańskiego GPS i rosyjskiego GLONASS, chiński Beidou działa na razie tylko w Azji. Galileo ma osiemnaście satelitów, docelowo będzie trzydzieści, w tym sześć rezerwowych. Jego zegary systemowe mają opóźnienie jednej sekundy na kilka milionów lat. Jest dokładny – w wersji powszechnie dostępnej chodzi o lokalizacyjną precyzję jednego metra (z odległości ponad 23 tys. km, bo na tej wysokości na trzech orbitach krążą jego satelity), a w wersji komercyjnej – centymetra! Jego silny sygnał będzie odbierany w budynkach i tunelach. Poprawi też skuteczność akcji ratunkowych w wysokich górach, w których sygnał GPS często zanika. Ma świadczyć bezpłatne usługi wspierające działania pomocowe, poprawić synchronizację czasową, nawigację i podnieść jakość bezpiecznych usług na rzecz podmiotów sektora publicznego.

7 lutego był Dniem Bezpiecznego Internetu. Kolejny temat rzeka. To ocena minimalisty. Internauci tylko w Google zadają 40 tys. pytań na sekundę. Z sieci korzysta ok. 3 mld ludzi, a ilość informacji jest niesamowita. Raz wstawiona, nie ginie i może być przetwarzana wielokrotnie w różnych miejscach. Zespół prof. Janusza Hołysta z Politechniki Warszawskiej prowadzi ciekawe badania nt. rozprzestrzeniania się informacji i znajdowania tej pierwszej, źródłowej. Niech sieć ich nie zaplącze – to tak w stylu z „Gwiezdnych wojen".

BIO

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

organizator:

a&S POLSKA

PIERWSZA MIĘDZYNARODOWA
KONFERENCJA BRANŻY SECURITY W POLSCE

# Warsaw Security Summit

**prestiżowe wydarzenie branżowe**
**prelekcje ekspertów z Polski i zagranicy**
**ciekawe bloki tematyczne i panele dyskusyjne**

- światowe trendy na rynku security
- innowacje w zabezpieczeniach
- przyszłość branży
- ranking największych firm security w Polsce

**9.06.2017 r.**
**Warszawa**
**Hotel Westin 5★**

**www.WarsawSecuritySummit.eu**

**WSTĘP BEZPŁATNY**
REJESTRACJA ONLINE

partnerzy:

AXIS COMMUNICATIONS · alhua TECHNOLOGY · Hanwha Techwin · HIKVISION · orange

# Zobacz każdy szczegół
## w jego naturalnej postaci

Panoramiczny obraz 180° bez zniekształceń









### Cechy kamery

- **Jedna** obudowa - **trzy** przetworniki - **jeden** adres IP
- Jednolity obraz wysokiej jakości bez podziału sceny
- Panoramiczny obraz 180° bez zniekształceń
- Łatwa instalacja
- Wysoki stopień ochrony - IP67, IK 10

H.265 | 180° Panoramic | TRACKING Smart Tracking | Starlight | WDR | IP67 | Vandal-proof

CE FC ISO 9001:2000

www.dahuasecurity.com/pl


**Dahua Technology Poland Sp. z o.o.**

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