CZASOPISMO RYNKU SECURITY

№ 02
2019 (14)
marzec /kwiecień

a&S POLSKA

Infrastruktura krytyczna

15 zł
(w tym 8% VAT)

ISSN 2451-5175

1. HIKVISION kamery dla SMB

odfiltrowujące fałszywe alarmy

HIKVISION

Technologia AcuSense Hikvision
oparta na Deep Learning

Rejestrator DVR AcuSense Turbo HD

INTELIGENTNY I DOKŁADNY, Z FUNKCJĄ DEEP LEARNING

AcuSense

Rejestrator DVR AcuSense Turbo HD

Technologia AcuSense, oparta na algorytmach deep learning, zapewnia większą dokładność analizy zawartości obrazu (VCA).

- Algorytm deep learning
- Architektura GPU
- Detekcja ludzi/pojazdów

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

@HikvisionPoland
www.hikvision.com/pl/

EDYTORIAL

Drodzy czytelnicy

Zmiana to proces, przez który przyszłość wchodzi w nasze życie. Zgodnie z maksymą amerykańskiego futurologa Alvina Tofflera, my także zmieniamy się, patrząc w przyszłość. Pierwszym elementem zmiany w naszej organizacji jest nowa, nowatorska i nowoczesna szata graficzna naszego czasopisma. Liczymy, że nowy styl przypadnie Państwu do gustu. Szykujemy kolejne zmiany, które ulepszą zarówno nasze dotychczasowe działania, jak i poszerzą ich zakres. Nie zwalniamy tempa...

Tematem tego wydania a&s Polska jest bezpieczeństwo infrastruktury krytycznej. W tym sektorze niezwykle istotna jest ochrona obwodowa (s. 16). Szacuje się, że do 2022 r. globalny rynek ochrony perymetrycznej wzrośnie ze 110 do ponad 196 mld USD. Ożywienie to wynika ze stale rosnących zagrożeń na całym świecie, a co za tym idzie z gotowości przeznaczania na to większych budżetów. Opisujemy także systemowe podejście do IK, prezentując je w czterech różnych, choć komplementarnych ujęciach: *safety, mission, business* i *security* (s. 22). Warto przy tym zwrócić uwagę na specyficzne problemy i wyzwania, z jakimi mierzą się osoby odpowiedzialne za bezpieczeństwo obiektów IK – jednymi z największych są uszkodzenie telekomunikacyjnej infrastruktury kablowej (s. 24) oraz konieczność zapewnienia operatorom obserwacji na duże odległości, co zapewnia technologia radarowa (s. 30). Podsumowaniem działu jest jak zwykle „Głos branży" prezentujący różne spojrzenia na temat.

Zmiany obserwujemy także na rynku kontroli dostępu. Od szerszego wykorzystania zamków bezprzewodowych po integrację uwierzytelniania i zarządzania dostępem – przedstawiciele branży kontroli dostępu komentują obecne trendy rynkowe (s. 42). W cyklu *Optyka dla każdego* opisujemy tym razem działanie ludzkiego oka oraz zjawisko dyfrakcji, co jest pomocne w zrozumieniu działania kamer dozorowych (s. 52). Obserwując intensywny rozwój w zakresie oprogramowania zarządzającego obrazem i integracji systemów, przybliżamy specyfikę, zasady działania i różnice między VMS i PSIM – prezentujemy obszerny materiał redakcyjny (s. 62) i przegląd dostępnych rozwiązań (s. 67).

Czy będziemy świadkami zmian w systemie bezpieczeństwa infrastruktury krytycznej kraju? Coraz bardziej widoczny jest trend tworzenia państwowych spółek ochrony, który może doprowadzić do dużych przetasowań na rynku ochrony fizycznej (s. 88). W dziale „Bezpieczeństwo biznesu" opisujemy nowe podejście do koncepcji bezpieczeństwa organizacji Security Concept (s. 92) oraz wstydliwy, choć niezwykle groźny dla biznesu problem kreta w firmie (96).

Gorąco zapraszamy na Warsaw Security Summit. Trzecia już edycja największej konferencji naszej branży odbędzie się 30 maja w Warszawie. Aktualna agenda, lista tematów i prelegentów oraz bezpłatna rejestracja są dostępne na: **www.WarsawSecuritySummit.eu**.
Zapraszamy! Do zobaczenia!

Marta Dynakowska
REDAKTOR NACZELNA

Jan T. Grusznic
Z-CA REDAKTORA NACZELNEGO

Mariusz Kucharski
DYREKTOR ZARZĄDZAJĄCY

a&S POLSKA

www.aspolska.pl

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

Dyrektor zarządzający
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

Z-ca redaktora naczelnego
Jan T. Grusznic

Stały felietonista
Andrzej Popielski

Dział marketingu i reklamy
Iwona Krawiec

Dział eventów i konferencji
Jolanta A. Kucharska
Aleksandra Czapska

Projekt graficzny i skład
Bogusław Kalwala

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

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

Korekta
Jolanta Kucharska

Prenumerata
www.aspolska.pl/prenumerata

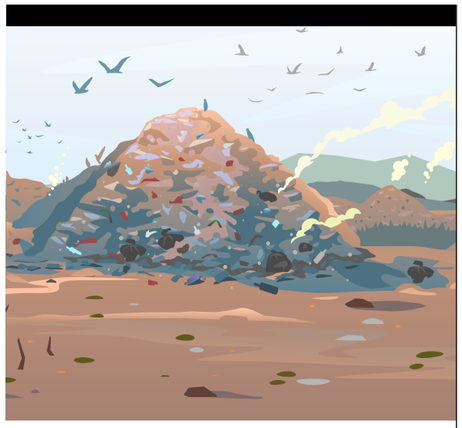
SPIS TREŚCI

№ 02

2019 (14)

marzec/kwiecień

a&S POLSKA



AXIS COMMUNICATIONS www.axis.com/pl

Obiektyw i-CS umożliwia zdalną regulację pola widzenia (ostrość ustawiana automatycznie)

F101-A XF P1367: odporna na wybuchy kamera sieciowa

Kamera sieciowa F101-A XF P1367 w obudowie przeciwwybuchowej wykrywa niepożądane osoby w strefach zagrożonych wybuchem i monitoruje bezpieczeństwo pracowników. Generuje doskonałej jakości szczegółowy obraz nawet przy słabym oświetleniu. Może też monitorować wydajność procesów produkcyjnych i wizualnie weryfikować dane przekazywane przez czujniki. Kamera jest lekka, można ją łatwo zamontować na wysokich wieżach czy budynkach. Ta przystępna cenowo profesjonalna kamera sieciowa w czerwonej aluminiowej obudowie ma certyfikaty: klasa I/II/III, Dział 1, Strefa 1 oraz ATEX i IECEx (IIB + H2, IIIC) potwierdzające możliwość jej stosowania w miejscach niebezpiecznych, zagrożonych wybuchem.

Kamera zapewnia obrazy zoptymalizowane pod kątem wykorzystania w postępowaniu wyjaśniającym. Ma dużą (światło)czułość, a dzięki technologii Lightfinder zapewnia wysokiej jakości kolorowe obrazy nawet podczas pracy w ciemności.

Funkcja WDR – *Forensic Capture* redukuje szumy i poprawia szczegółowość obrazów w scenach z kontrastowymi – jasnymi i ciemnymi obszarami, np. gdy jest skierowana na wejście lub w pobliżu okna.

Kamera dostarcza obraz w rozdzielczości **5 Mpix** przy przepływności **25/30 kl./s** i kodowaniu **H.264** oraz **MJPEG**. Dzięki funkcjom analizy **ACAP** poprawia bezpieczeństwo osób przebywających w strefach zagrożenia lub strefach o ograniczonym dostępie.

BCS www.bcscctv.pl

BCS-NVR3204-P-4K-AI

Dotychczas, chcąc skorzystać z funkcji zaawansowanej analizy obrazu w systemach IP, musieliśmy skupić uwagę na właściwym doborze kamer, aby dopasować je do potrzeb klienta. To kamery odpowiadały za to, z jakich funkcji będzie można skorzystać. W przypadku bardziej wymagających rozwiązań jedna kamera była odpowiedzialna za identyfikację tablic rejestracyjnych, inna za rozpoznawanie i porównywanie twarzy, kolejna za liczenie osób wchodzących do obiektu i wychodzących z niego, a jeszcze inne za ochronę obwodową.

Aby uniknąć takich sytuacji, z pomocą przychodzi nowy rejestrator **BCS-NVR3204-4K-P-AI serii Line**. Ma on zaimplementowaną w oprogramowaniu systemowym obsługę funkcji zaawansowanej analizy obrazu. Na 16 kanałach obsługuje funkcje związane z ochroną obwodową (przekroczenie linii czy wtargnięcie w strefę). Na 4 kanałach ujawnia wszystkie swoje możliwości, oferując dostęp do takich funkcji, jak rozpoznawanie i identyfikacja twarzy, rozpoznawanie tablic rejestracyjnych czy rozpoznawanie i identyfikacja obiektów.

Rejestrator na podstawie otrzymanego obrazu zbiera metadane, dzięki którym wyszukiwanie interesujących zdarzeń staje się wyjątkowo proste i skuteczne, bez potrzeby przeglądania wielu godzin nagrań. Wystarczy określić dodatkowe parametry nagrania, które potrzebujemy wyszukać – m.in. przedział wiekowy, płeć, kolor i typ ubrania w przypadku ludzi czy numer tablicy rejestracyjnej, kolor i markę dla samochodów – by po chwili mieć do niego dostęp.

COMMAX www.commax.pl

Nowa jakość systemów wideodomofonowych

Na rynku wideodomofonowym pojawił się produkt o niespotykanej dotychczas jakości i funkcjonalności. Monitor COMMAX CDV-704MA z panoramicznym 7" ekranem wyświetla obraz z paneli wejściowych wyposażonych w optykę **HD 960p (1,3 Mpix),** co przekłada się na 3-, a nawet 4-krotnie większą szczegółowość obrazu w porównaniu do standardowych kamer analogowych.

Zwiększenie jakości toru wideo nie wymaga dodatkowych zabiegów instalacyjnych – system pracuje poprawnie na standardowym okablowaniu. Na monitorze można również wyświetlać obrazy z dodatkowych kamer obserwacyjnych pracujących również w rozdzielczości **AHD 1,3 Mpix**.

System przeznaczony do zabudowy jednorodzinnej można rozbudować do 4 monitorów, zapewniając selektywną łączność interkomową między nimi. Na wbudowany moduł pamięci

(możliwość rozbudowy o karty **microSD**) zostają zapisane zdjęcia lub filmy podczas wywołania monitora oraz w przypadku wykrycia ruchu na obrazie z wybranej kamery. Obsługę ułatwia ekran dotykowy. Monitor jest dostępny w dwóch wersjach kolorystycznych: klasycznej biało-perłowej oraz designerskiej ciemnoszarej z granatowym akcentem wokół ekranu.

Monitor obsługuje panele wejściowe **COMMAX** – analogowe oraz z optyką **HD 1,3 Mpix.** Użytkownik może wybrać modele do montażu na wąskich słupkach **(np. DRC-4CPHD) lub klasyczne (np. DRC-41UNHD)**, wyposażone w czytnik kart/breloków i/lub klawiaturę kodową, umożliwiające otwarcie furtki i bramy za pomocą kodu i/lub transpondera zbliżeniowego **(np. DRC-40DKHD).**

DAHUA TECHNOLOGY POLAND
www.dahuasecurity.com/pl

ITC215-PW4I-IRLZF27135 – zaawansowana kamera szlabanowa

Systemy parkingowe to coraz częściej spotykana grupa rozwiązań z pogranicza aplikacji związanych z bezpieczeństwem obiektów, a także zapewniających im dodatkowe wartości użytkowe. Zautomatyzowany wjazd na parking podziemny czy do bazy przeładunkowej to typowe przykłady zastosowań kamer odczytujących tablice rejestracyjne pojazdów.
Dotychczas podstawową funkcją tego typu urządzeń było odczytanie numerów tablicy i zakwalifikowanie pojazdów do listy uprzywilejowanych bądź nie. Nawet tak podstawowe działanie znacząco usprawniało przepływ pojazdów i odciążało/redukowało osoby z obsługi. Technologia nie stoi w miejscu, a postęp nie omija również kamer **ANPR**, które – zgodnie z trendami – zostały wzbogacone o coraz popularniejsze algorytmy głębokiego uczenia.
Przykładem jest **ITC215-PW4I-IRLZF27135** firmy Dahua Technology. Kamera ta – oprócz standardowych informacji o numerze rejestracyjnym – wzbogaciła się o możliwość klasyfikacji obiektów pod kątem różnych cech. Rozpoznaje również typ pojazdu (**sedan, bus, SUV, ciężarówka itp.)** oraz jego kolor. Można także uzyskać informację o kierunku ruchu oraz – dzięki obecności wejść alarmowych – podłączyć do kamery pętlę indukcyjną.
Z kolei obecność wyjść alarmowych pozwala na montaż kamery w bezpośrednim sąsiedztwie szlabanu i wykorzystanie jej jako modułu wykonawczego. Możliwość użycia „białej listy" (**do 10 000 rekordów)** dodatkowo rozszerza ten wariant. Pełna specyfikacja pokazuje, że jest to urządzenie wszechstronne.

EBS
www.ebssmart.com

System CALLISTO 32

Nowa odsłona znanego już dobrze systemu alarmowego Callisto 32 firmy EBS jest rozwiązaniem hybrydowym, które można dopasować do niemal każdego typu obiektu. 32 wejścia bezprzewodowe, 7 przewodowych (dla konfiguracji TOEL nawet 14), czujki (ruchu, zalania, dymu, gazu, przesunięcia i zbicia szyby), przyjazne aplikacje mobilne dla użytkownika i instalatora to tylko podstawowe zalety tego systemu.

Programowanie centrali i dodawanie czujek online za pomocą kodów QR skraca czas instalacji systemu do 7 minut. Instalator może też skorzystać z gotowych szablonów konfiguracyjnych. Dzięki tym zaletom Callisto 32 znalazło się w światowej czołówce najłatwiej i najszybciej instalowanych systemów na świecie!
Użytkownik dzięki swojej aplikacji steruje systemem z dowolnego miejsca na świecie. Z jednego konta aplikacji może monitorować kilka obiektów (dom, biuro, działkę, magazyn itp.). Liczba użytkowników aplikacji jest nieograniczona!
Agencja ochrony, proponując swoim klientom system Callisto 32 marki EBS, ma zapewnione:
- konkurencyjną ofertę wyróżniającą ją na lokalnym rynku,
- dodatkowe dochody dzięki zdalnemu serwisowi,
- dogodne warunki zakupu (sprzedaż subsydiowana, kontrakty 2- i 3-letnie),
- profesjonalne narzędzia do zarządzania praktycznie nieograniczoną liczbą systemów alarmowych podłączonych do centrum monitorowania alarmów,
- gotowe narzędzia i praktyki sprzedażowe,
- wsparcie techniczne i marketingowe,
- zadowolenie klienta (sprzęt najwyższej jakości, intuicyjny w obsłudze, łatwy w rozbudowie i modyfikacji, spełniający wymagania normy PN-EN 50131 Grade 2.

Więcej szczegółów na www.ebssmart.com.

HIKVISION POLAND
www.hikvision.com/pl/

Centrala AXHub DS-PWA32-N

Firma Hikvision poszerza ofertę o nowatorską centralę alarmową do małych i średnich obiektów, głównie mieszkalnych i biurowych. Centrala AXHub łączy w niedużym urządzeniu system alarmowy obsługujący do **32 czujek** bezprzewodowych oraz system wideoweryfikacji zdarzeń na podstawie podglądu z kamer IP Hikvision. System oparto na uznanym dwukierunkowym systemie bezprzewodowym Enforcer firmy Pyronix pracującym na częstotliwości 868 MHz i doświadczeniu Hikvision jako producenta systemów dozoru wizyjnego.
Ważnym atutem **AXHub** jest dostępność interfejsów komunikacyjnych, umożliwiających rejestrację w chmurze **Hik-Connect.** Już podstawowa wersja urządzenia jest wyposażona w łączność **Ethernet i Wi-Fi**, są też wersje z dodatkowym modemem **GPRS lub 3G/4G**. Wybranym kanałem komunikacji można przekazywać komunikaty **Contact ID** do stacji monitoringu.
Centralę można obsługiwać za pomocą aplikacji **Hik-Connect,** która pozwala na sterowanie systemem, odbiór powiadomień o zdarzeniach, a także podgląd zdarzeń (wideoweryfikację). W przypadku wystąpienia zdarzenia powiązanego z kamerą użytkownik może obejrzeć 7-sekundowe nagranie (**5 s pre-alarmu oraz 2 s po wystąpieniu zdarzenia**).
Systemem można sterować również za pomocą jednego z 8 pilotów sterujących Pyronix lub breloków zbliżeniowych Mifare. Powiadamianie o zdarzeniach w systemie może odbywać się także w klasyczny sposób poprzez jeden z 2 bezprzewodowych sygnalizatorów **Pyronix** oraz komunikaty głosowe emitowane z urządzenia.
Centralę konfiguruje się poprzez interfejs dostępny przez przeglądarkę www.

LINC POLSKA
www.linc.pl

MAGOS Systems: RADAR w branży zabezpieczeń?

Pierwsze skojarzenie ze słowem radar to lotnisko, statek czy rozwiązania typowo wojskowe. Ale ta technologia jest już także skutecznie stosowana w branży ochrony do nadzorowania dużych otwartych terenów. MAGOS Systems jest producentem radarów kierunkowych o zasięgu nawet 1 km, przy rozdzielczości poniżej 1 m. Pojedynczy radar umożliwia pokrycie terenu nawet w zakresie **120° w poziomie i 30° w pionie.** Dzięki temu strefa martwa praktycznie nie występuje, a możliwość połączenia 3 radarów w jeden system zapewnia pełną ochronę **360°**.
Pojedynczy radar może nadzorować teren o powierzchni nawet 500 tys. m², z możliwością wykluczenia dowolnych stref, w których ruch dopuszczono. Ważnym elementem systemu jest możliwość bezpośredniego połączenia z kamerą obrotową poprzez Onvif oraz natychmiastowej obserwacji i śledzenia wykrytego intruza. Dzięki zastosowaniu radarów można znacznie zredukować liczbę kamer, czujników i okablowania, niezbędnych do zabezpieczenia rozległych terenów.
Radar jest pyło- i wodoszczelny, komunikuje się po sieci LAN i pobiera zaledwie **3-5 W** bezpośrednio z zasilania PoE. Dostępne modele o zasięgu **250, 500 i 1000 m** pozwalają dopasować konfigurację do różnych potrzeb. System nie wymaga dodatkowych homologacji czy zezwoleń, wykorzystuje nielicencjonowane pasma cywilne, dlatego można go stosować w krajach UE.
System radarowy **MAGOS** integruje się z platformami **VMS (FLIR Latitude, Milestone, Genetec, Avigilon, EXACQ** i wieloma innymi).

SCHRACK SECONET POLSKA
www.schrack-seconet.pl

APS®-APROSYS: dźwiękowy system ostrzegawczy

Dźwiękowy system ostrzegawczy APS®--APROSYS (produkcji g+m elektronik AG) to przewodowy, modułowy system służący przede wszystkim do powiadamiania osób znajdujących się w zagrożonych obszarach o ewakuacji lub zmobilizowania ich do innego działania. Dzięki wykorzystaniu technologii warstw i priorytetów może też służyć jako system rozgłaszania komercyjnego (PA – *public address*), system zegarowy czy system dystrybuujący tło muzyczne w obiekcie (**BGM – *background music***) w tym samym czasie.
Rozwiązaniem wyróżniającym system **APS®--APROSYS** jest m.in. możliwość optymalizacji instalacji **DSO** dzięki zastosowaniu elastycznego rozdziału mocy wzmacniaczy.
Zaawansowane kontrolery linii głośnikowych **APS-178.1-XX-EV** z wbudowanymi selektorami stref pozwalają na pełne wykorzystanie zakresów mocy oferowanych przez dobrane wzmacniacze. Gdy w obiekcie występuje wiele stref nagłośnienia małej lub średniej mocy obsługiwanych przez jedną lub kilka par linii głośnikowych, można tu zastosować tylko jedną końcówkę wzmacniacza! Ponadto każda pożądana funkcja fakultatywna systemu to zaledwie jedna lub dwie karty systemowe dołożone do ramy montażowej **MC-03 systemu**.
Projektując system z użyciem kontrolerów linii z selektorami stref można znacznie zredukować liczbę wzmacniaczy, a co za tym idzie wymaganą pojemność akumulatorów zasilania rezerwowego, okablowanie systemowe, rozmiar i liczbę szaf, bez zbędnego przewymiarowania systemu.

TP-LINK
www.tp-link.com.pl

TL-SL1218MP: wydajny przełącznik do zastosowań CCTV

Przełącznik TL-SL1218MP został zaprojektowany z myślą o systemach monitoringu wizyjnego IP. Dzięki przełącznikowi **PoE** instalacja systemu jest łatwiejsza, bardziej bezpieczna i mniej kosztowna. Tryb Extend powiększa zasięg transmisji PoE nawet do 250 metrów, dzięki czemu urządzenie doskonale sprawdzi się w instalacjach, gdzie kamery IP są rozmieszczone na dużym obszarze.
TL-SL1218MP działa w standardzie 802.3af/at (**PoE+**). Łączna moc urządzeń zasilanych przez 16-portowy przełącznik może wynosić **192 W**, przy czym każdy port PoE dostarcza do **30 W mocy**.

NAJWAŻNIEJSZE CECHY I FUNKCJE

- 16 portów RJ45 PoE+ 10/100 Mb/s,
- 2-gigabitowe porty RJ45,
- 2-gigabitowe gniazda combo SFP,
- do 250 m zasięgu transmisji danych i zasilania w trybie Extend, stworzony z myślą o systemach dozorujących,
- tryb priorytetowania dla portów 1–8,
- wysoki budżet mocy PoE: do 30 W na każdy port PoE, 192 W łącznej mocy zasilanych urządzeń,
- łatwość obsługi, brak konieczności przeprowadzania konfiguracji czy instalacji.

Wysoki budżet PoE sprawia, że urządzenie idealnie sprawdzi się w małych i średnich firmowych systemach dozoru wizyjnego.

Śniadanie ekspertów

transport i logistyka

Ciekawą dyskusję o bezpieczeństwie prowadzili uczestnicy kolejnego śniadania ekspertów a&s Polska. Przedstawiciele sektora transportu i logistyki mieli okazję już po raz trzeci porozmawiać z ekspertami branży bezpieczeństwa o najbardziej palących problemach.

Jan T. Grusznic

a&s Polska

→ ***Zabezpieczenie całego procesu logistycznego to nie lada wyzwanie.*** *Spotkanie uświadomiło uczestnikom, z jakimi problemami zderzają się firmy transportowe i w jaki, często nietypowy sposób, radzą sobie z nimi. Podane przykłady pokazały również, że istnieje potrzeba ujęcia systemów zabezpieczeń całościowo, na poziomach integracji systemów i operacyjnym. W ten sposób zapewniony zostanie lepszy efekt wykorzystania dostarczanych narzędzi, jakimi są elektroniczne systemy zabezpieczeń.*

Bogumił Szymanek

Axis Communications

→ ***Bardzo dobra i merytoryczna dyskusja, która po raz kolejny pokazała, jak ważne jest zrozumienie potrzeb klienta.*** *Sektor transportu i logistyki napotyka problemy z zakresu bezpieczeństwa, które nie zawsze są oczywiste. Wiedza przekazywana przez osoby znające branżę „od podszewki" jest bezcenna dla producentów. Kluczowe jest spojrzenie na zagadnienie z wielu perspektyw, gdyż dynamika zmian sprawia, że wciąż będą pojawiały się nowe wyzwania. Dlatego w Axis bazujemy na otwartej współpracy i myśleniu długoterminowym.*

Tomasz Siwicki

GEFCO Polska

→ ***Na spotkaniu była bardzo widoczna dysproporcja między tym, co oferują dostawcy, a tym, czego potrzebują np. operatorzy logistyczni.*** *Jest potrzeba pogłębionych wypowiedzi osób odpowiedzialnych za bezpieczeństwo, które mogłyby pomóc sprostać potrzebom branży logistycznej.*

Andrzej Żochowski

TNT Express Polska

→ ***Było to kolejne spotkanie ekspertów ds. bezpieczeństwa z różnych obszarów, którzy mieli możliwość podyskutowania o najbardziej dotkliwych zagrożeniach i incydentach dla bezpieczeństwa biznesu.*** *Tego typu wymiana poglądów pozwala na określenie trendów w zagrożeniach, które przekładają się na sprawność funkcjonowania organizacji i zachodzących procesów biznesowych. Z drugiej zaś strony w spotkaniu udział wzięli dostawcy rozwiązań technicznych, którzy podnoszą poziom bezpieczeństwa i pozwalają zabezpieczyć istotne procesy. Dlatego też dyskusja dotycząca zagrożeń i trendów pozwala w mojej ocenie na lepsze zrozumienie potrzeb rynku przez dostawców i obustronną wymianę doświadczeń.*

Anna Twardowska

Nedap Security Management

→ ***Spotkanie było doskonałą okazją do poznania potrzeb rynku logistycznego i transportowego.*** *Bardzo interesująca była dyskusja dotycząca potrzeb zwiększenia zabezpieczeń przed cyberatakami. Ubiegły rok przyniósł wielu firmom w Polsce dużo wyzwań w tym zakresie. Uważam, że takie spotkania są ważne, ponieważ każda okazja do wymiany doświadczeń i wysłuchania klientów pomaga producentom lepiej dostosowywać swoje rozwiązania do oczekiwań rynku.*

Łukasz Michałowski

NSS

→ ***Uważam, że takie spotkania są ważne i potrzebne dla całej branży.*** *Spotykają się tutaj zarówno dostawcy systemów zabezpieczeń, jak i klienci końcowi. Dzięki wymianie doświadczeń i spostrzeżeń możemy lepiej dopasować naszą ofertę do aktualnych zagrożeń i problemów w logistyce i transporcie.*

Bezpieczne obiekty IK dzięki zaawansowanej ochronie obwodowej

WZROST ZAGROŻENIA TERRORYZMEM POWODUJE, ŻE RYNEK OCHRONY OBWODOWEJ (PERYMETRYCZNEJ) ROZWIJA SIĘ W SZYBSZYM TEMPIE. NOWE TECHNOLOGIE OFERUJĄ OPERATOROM SECURITY CORAZ SKUTECZNIEJSZĄ DETEKCJĘ.

TEKST
Eifeh Strom
a&s International

Na początku były ogrodzenia instalowane wokół zewnętrznych granic terenu – od tego czasu ochrona obwodowa przeszła długą drogę. Ożywienie rynku wynika przede wszystkim ze wzrostu liczby ataków terrorystycznych na całym świecie. Postęp technologiczny w zakresie dozoru wizyjnego również wpływa na popyt na systemy i usługi ochrony obwodowej, podobnie jak zwiększone wykorzystanie Internetu Rzeczy (IoT) oraz rozwiązań inteligentnych (*smart*).

Według raportu Markets and Markets rynek ochrony perymetrycznej osiągnie w 2022 r. wartość 196,6 mld USD (wobec 110,6 mld USD w 2017 r.). Sprzedaż w latach 2017–2022 ma co roku rosnąć średnio o 12,2 proc.

SYSTEMY PLUG-AND-PLAY ZWIĘKSZAJĄ DOSTĘPNOŚĆ OCHRONY OBWODOWEJ

Cena i skomplikowana instalacja to najczęstsze przeszkody w wykorzystaniu nowych technologii. Sytuację ratują rozwiązania plug-and-play, dzięki którym więcej inwestorów wdraża systemy ochrony obwodowej.

Przechodzenie z systemów, które są niestandardowe, drogie, skomplikowane w instalacji i kosztowne w utrzymaniu, do rozwiązań ekonomicznych typu plug-and-play, niewymagające specjalistycznej wiedzy, certyfikacji i szkoleń, a przy tym łatwe w utrzymaniu, to jeden z najważniejszych trendów na globalnym rynku ochrony obwodowej. Przykładowo jeszcze pięć lat temu właściciel magazynu samoobsługowego lub hurtowni, doświadczający ciągłych napadów (z przecinaniem ogrodzenia itp.), nie dysponował środkami mogącymi temu skutecznie zapobiegać. Mógł próbować wykorzystać bariery podczerwieni, ale generowały one fałszywe alarmy powodowane trudnymi warunkami atmosferycznymi, działaniem zwierząt i roślinnością. Mógł też starać się rozwiązać problem przy użyciu kamer, ale one zwykle pokazywały człowieka w bluzie z kapturem, który poruszał się skradzionym pojazdem. Ewentualnie użyć taniej analityki, która wysyłałaby fałszywe alarmy w czasie deszczu.

Obecnie, dzięki np. prostym alarmowym zestawom kabli sensorycznych, operatorzy ochrony, którzy wcześniej nie dysponowali odpowiednim budżetem albo brakowało im kompetencji, teraz mają dostęp do skutecznych rozwiązań. Takie zestawy instaluje się na ogrodzeniu i podłącza do istniejącego systemu alarmowego. Nawet integrator, który w swoim zawodowym życiu nigdy nie wdrażał ochrony obwodowej, może teraz łatwo kupić system i zainstalować go, nie martwiąc się o swoje umiejętności w dostarczeniu dobrze działającego systemu.

Według raportu Markets and Markets Ameryka Północna ma największy udział w światowej sprzedaży detektorów ochrony obwodowej. Za wzrost na tym rynku odpowiadają przede wszystkim takie czynniki, jak większa aktywność terrorystów, nielegalna imigracja oraz przestępstwa kryminalne – przestępczość, rosnąca liczba kradzieży i aktów wandalizmu w sektorach komercyjnych i przemysłowych, przy jednocześnie trudniejszym dostępie do policji, która zmusza firmy, by same zapewniały sobie ochronę. Najszybciej rosnącym regionem jest jednak APAC (region Azji i Pacyfiku). Wynika to z ożywienia gospodarczego w obszarze infrastruktury (lotniska, koleje i autostrady) oraz silnego rozwoju usług finansowych i bankowych, jakie zachodzą na tym rynku. Zdaniem analityków z Markets and Markets będzie się to przekładać na duży wzrost na regionalnym rynku ochrony obwodowej.

Branże mają większe oczekiwania

Jak twierdzą analitycy z Memoori, rosnąca liczba zagrożeń sprawiła, że ochrona perymetryczna odgrywa coraz ważniejszą rolę w zabezpieczaniu infrastruktury krytycznej. Dotyczy to np. dostawców mediów użytkowych, usług transportowych, administracji publicznej czy służb mundurowych. Ataki mogą powodować poważne zakłócenia w funkcjonowaniu tego rodzaju infrastruktury i prowadzić do ogromnych strat w całej gospodarce. Firmy specjalizujące się w ochronie obwodowej odnotowują stały wzrost sprzedaży, wynikający z rosnącego zaangażowania organizacji w zapewnienie bezpieczeństwa infrastruktury krytycznej i gotowości przeznaczania na to większych budżetów. Dostawcy mediów użytkowych (wody, ciepła, prądu) znajdują się pod presją oczekiwań, by dostęp do tych usług był ciągły, a obiekty były chronione przed aktami wandalizmu i atakami bojówkarzy oraz terrorystów. Wzrost zapotrzebowania wynika też z ostrzejszych regulacji rządowych.
Dużym odbiorcą systemów ochrony obwodowej jest od dawna również sektor naftowo-gazowy ze względu na różne zagrożenia, na jakie jest narażony. Wiele krajów, nawet Kanada uważana za państwo o niskim poziom zagrożenia, zainwestowało duże kwoty w zabezpieczenie infrastruktury naziemnej, głównie z powodu zwiększonej świadomości jej krytycznego znaczenia.
W sektorze komercyjnym rosnący popyt na ochronę perymetryczną jest stymulowany przez rozwój technologiczny,

Wzrost sprzedaży na rynku ochrony obwodowej wynika z rosnącego zaangażowania przedsiębiorstw w poprawę bezpieczeństwa i gotowość przeznaczania na to większych budżetów.

WYKORZYSTANIE ANALIZY WIZJI I TERMOWIZJI WZMACNIA OCHRONĘ OBWODOWĄ

Na całym świecie dochodzi do coraz częstszych naruszeń ochrony obwodowej. Gdy mowa o zbudowaniu kompleksowego systemu zabezpieczeń, w monitorowaniu potencjalnych intruzów kluczową rolę mogą odgrywać kamery wyposażone w termowizję oraz wbudowane funkcje analizy obrazu.

W raporcie Markets and Markets szybszy postęp technologiczny w obszarze dozoru wizyjnego został uznany za jeden z najważniejszych czynników zwiększających popyt na systemy i usługi ochrony obwodowej. Intruzi jednak od dawna wykorzystują słabości technologiczne tradycyjnych kamer dozorowych, m.in. martwe strefy i błędy wynikające z obsługi człowieka.
Aby ograniczyć te problemy, producenci obierają dwie drogi. Po pierwsze, słabości związane z obsługą człowieka skutecznie eliminuje analiza zawartości wizji (VCA), automatycznie uruchamiająca alarmy po wykryciu intruzów. Po drugie, niedoskonałości kamer działających w świetle widzialnym można przezwyciężyć przy użyciu kamer termowizyjnych. Te urządzenia w ostatnich latach stały się bardziej wydajne i tańsze.
Aby postęp był zauważalny, analityka VCA oraz kamery termowizyjne powinny współpracować ze sobą. Bez obrazu przechwytywanego z kamery termowizyjnej pracującej w ekstremalnych warunkach (deszcz, dym i odblaski światła) nawet najpotężniejsze algorytmy VCA nie mają szansy wykrycia intruzów, którzy wykorzystują np. martwe strefy kamer dozorowych. I na odwrót – bez pomocy VCA efekt kamer termowizyjnych zostanie zredukowany do obrazu na kolejnym ekranie, który szybko przestanie być obserwowany. Trudno będzie też wyeliminować ludzkie błędy. Tylko połączenie analityki i termowizji zapewnia skuteczną ochronę przed intruzami.
W rezultacie producenci, np. Bosch, opracowują kamery termowizyjne z wbudowaną inteligentną analizą wizji (np. DINION IP thermal 8000). Ułatwiają one operatorom tworzenie ochrony obwodowej, dostarczając dane najlepiej obrazujące sytuację. I chociaż kamery termowizyjne nie zastępują kamer tradycyjnych, to pracując w tandemie, zapewnią operatorom maksymalną świadomość sytuacyjną i wczesne wykrycie intruzów.
Dzięki współpracy kamer termowizyjnych z zaimplementowaną analityką VCA z systemami ochrony obwodowej operatorzy mają szansę nigdy nie przeoczyć potencjalnego zagrożenia, szybko uzyskując właściwe dane – bez względu na to, jak niekorzystne panują warunki.

który sprawia, że rozwiązania stają się bardziej przystępne cenowo i lepiej dostosowane do potrzeb mniejszych instalacji. Firmy zaczynają również akceptować ochronę obwodową jako niezbędny system alarmowy zabezpieczający ich firmę. Poszukują rozwiązań, które będzie można łatwo zamontować na istniejącym ogrodzeniu.
W czasach, gdy coraz więcej osób i firm korzysta z usług opartych na chmurze, także centra danych przyczyniają się do wzrostu liczby wdrożeń ochrony obwodowej. Coraz częściej są one bowiem celem napastników.

Trendy technologiczne

Rozwój rynku ma napędzać integracja systemów i wykorzystanie nowych, zaawansowanych technologii. Analitycy z Memoori wskazują zwłaszcza na postęp, jaki dokonuje się w detektorach, technologiach bezprzewodowych i radarach. Podkreślają też rolę integracji systemów ochrony obwodowej z systemami dozoru wizyjnego czy kontroli dostępu z oświetleniem zewnętrznym. Wprowadzenie analityki VCA i oprogramowania opartego na technologii *deep learning* także ma duży wpływ na rynek systemów alarmowych antywłamaniowych i ochrony obwodowej.
Stały rozwój VCA w połączeniu z taniejącymi kamerami o wyższej wydajności zwiększa efektywność wykorzystania tego rozwiązania w ochronie perymetrycznej. Integracja tych systemów z inteligentnym oświetleniem wpływa na obniżenie całkowitego kosztu posiadania, przy jednoczesnym zwiększeniu skuteczności odstraszania, detekcji i oceny. Integracja systemów, mająca na celu tworzenie kompleksowych rozwiązań bezpieczeństwa, jest kluczowym trendem na rynku ochrony obwodowej.
Duży wpływ na skuteczność ochrony perymetrycznej ma technologia wizualizacji strefy detekcji, zapewniana przez kamery VSS z algorytmami rozpoznawania obiektów, takich jak ludzie, samochody i zwierzęta. Jednak wydajność i niezawodność wykrywania nie spełnia oczekiwań branży ze względu na problemy, takie jak brak alarmu czy duża liczba fałszywych alarmów powodowanych przez światło, deszcz, owady itp. Zaleca się stosowanie sprawdzonych technologii, takich jak skanery laserowe, światłowodowe kable sensoryczne, bariery i czujki podczerwieni czy mikrofalowe.
Na znaczeniu wciąż zyskują technologie światłowodowe, w instalacjach zarówno montowanych na ogrodzeniach,

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

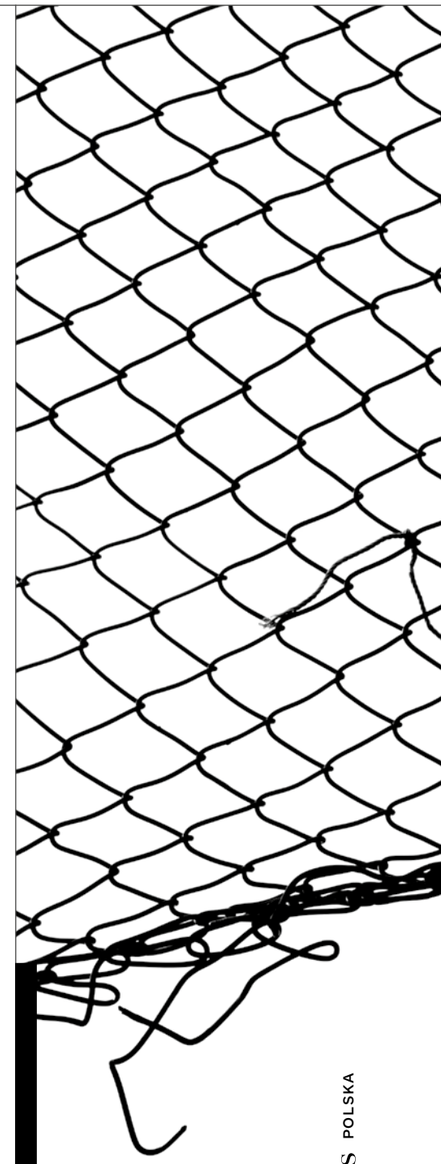
jak i zakopywanych. Kluczem do ich popularności jest całkowita odporność na wyładowania i zakłócenia elektromagnetyczne. Są one również bezpieczne w strefach zagrożonych wybuchem gazu.

Najczęściej wybierane sensory

Do wzrostu sprzedaży rozwiązań ochrony obwodowej przyczynia się także postęp w technologii czujników. Już teraz sensory – począwszy od przeznaczonych do montażu na ogrodzeniu, aż po czujniki drgań i termiczne – są jednymi z najpopularniejszych produktów na tym rynku. Postęp technologiczny dotyczy bardziej zaawansowanych algorytmów oprogramowania, które zmniejszają liczbę fałszywych alarmów oraz zwiększają dokładność lokalizacji. Dzięki tym ulepszeniom sensory montowane obecnie na ogrodzeniu są postrzegane jako bardziej wartościowa opcja. Integracja czujników ogrodzeniowych z innymi systemami, np. z inteligentnym oświetleniem, również wprowadza nowe funkcje i zastosowania. Przykładowo inteligentne oświetlenie może zareagować na włamanie, zmieniając intensywność światła lub tworząc efekt stroboskopowy w zagrożonej strefie, co działa odstraszająco na intruza, dając jednocześnie ocenę sytuacji.
Na popularności zyskują także montowane na ogrodzeniu mikrofalowe kable sensoryczne wykrywające wibracje oraz czujki sejsmiczne montowane pod ziemią. Oferowane w formie zestawów mogą być podłączane do standardowego systemu alarmowego lub dozoru wizyjnego. W ostatnich latach uznanie zyskują również sensory termowizyjne, czujniki radarowe i skanery laserowe oraz detektory wizyjne (np. z zastosowaniem algorytmów VCA). Dostarczają one nie tylko informacji wyzwalających alarmy, ale także danych o rozmiarze, kierunku czy prędkości poruszania się, zwiększających – wraz z systemami zarządzania dozorem wizyjnym – funkcjonalność ochrony.

Odstraszyć intruza

Tak długo, jak terroryzm pozostanie poważnym zagrożeniem, światowy rynek ochrony obwodowej będzie odnotowywał wyraźny wzrost. Pozytywne jest to, że technologie są coraz doskonalsze i inteligentniejsze, a przy tym coraz bardziej przystępne cenowo. W rezultacie stają się dostępne dla większej liczby inwestorów z różnych branż. □



Infrastruktura (nie?)krytyczna

INFRASTRUKTURA KRYTYCZNA TO POJĘCIE DOŚĆ POWSZECHNE. NALEŻĄ DO NIEJ 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.

TEKST
Jacek Grzechowiak

Kwestie te reguluje to ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Przepisy prawa w tym zakresie wskazują kierunek wynikający z potrzeby uregulowania tej tematyki na poziomie państwowym. Infrastruktura krytyczna jest definiowana w różny sposób w różnych krajach, niemniej jest związana z krytycznym wpływem na społeczeństwo i ekonomię państwa. W gospodarkach rozwiniętych są nią nie tylko systemy i obiekty, ale także zasoby wirtualne. Takie podejścia jest też bliższe biznesowi, którego zasoby nie muszą mieć waloru materialnego, ważne, by miały krytyczne znaczenie przede wszystkim dla ciągłości biznesu. W przedsiębiorstwach infrastruktura krytyczna jest postrzegana jako ta część zasobów, której uszkodzenie lub zniszczenie może doprowadzić do kryzysu organizacji. Z reguły wyróżnia się jej zasadnicze komponenty *Safety – Mission – Business – Security.* Ponieważ poruszamy się w obszarze security, a jednocześnie security jest procesem wspierającym zasadniczą działalność przedsiębiorstwa, ograniczę się do tego aspektu.
Truizmem jest twierdzenie, iż wszystkie obszary działalności security mają wpływ na biznes i infrastrukturę krytyczną. Spójrzmy więc na przykładowe możliwości wpływu ochrony (security) na infrastrukturę krytyczną, widzianą przez pryzmat poszczególnych jej komponentów.

SAFETY

Zespół pracowników ochrony jest rozlokowany w całym obiekcie, ma więc możliwość obserwowania zjawisk, które mogą mieć wpływ na bezpieczeństwo operacji. W zakładach produkcyjnych obecnie to właściwie standard. Pracownicy ochrony ujawniają dużą część zjawisk mogących spowodować incydent w bezpieczeństwie. Przykładowo wyciekający olej silnikowy, zeskakiwanie z naczepy (bez użycia drabinki) czy jazda z niezabezpieczonym lub niewłaściwie zabezpieczonym ładunkiem są dziś ujawniane właśnie przez pracowników ochrony i dzięki nim nie dochodzi do wypadków przy pracy. Innym obszarem jest bezpieczeństwo w wymiarze przeciwpożarowym i (lub) przeciwwybuchowym. W zakładach przemysłowych może przebywać dzisiaj wiele osób z zewnątrz, np. pracownicy agencji pracy tymczasowej czy podwykonawcy. Wiedza tych osób oraz ich podejście do kwestii bezpieczeństwa ppoż. i przeciwwybuchowego są różne. Wynika to z kilku powodów. Pierwszym jest słaba znajomość obiektu, w którym wykonują pracę, nie mogą więc mieć wystarczającej wiedzy o newralgicznym charakterze miejsc, w których przebywają. Nie zawsze widać np. infrastrukturę gazową czy hydrauliczną, podatną na zagrożenia pożarowe w stopniu ponadprzeciętnym. Każdy wie, że palenie jest zabronione, ale życie pokazuje, że mimo takich – wydawałoby się oczywistych – wymogów nie wszyscy stosują się do tego zakazu, nie bacząc, że stoją np. przy żółtej rurze gazowej. Rola ochrony jest ważna, a właściwe postawienie zadań pracownikom ochrony przynosi dobre efekty. Pracownicy ochrony są lepiej przygotowani do obcowania z uzbrojeniem i tam, gdzie ryzyko pojawienia się niewybuchów jest ponadprzeciętne, to właśnie oni bardzo często ujawniają przedmioty niebezpieczne.
Duża rotacja personelu, niska świadomość bądź nieidentyfikowanie się pracowników tymczasowych z zakładem, w którym wykonują swoje obowiązki, potęgują ryzyko zagrożeń.

W identyfikowaniu IK kluczowe znaczenie ma cecha zasobu, jaką jest krytyczny wpływ na ciągłość działania firmy

MISSION

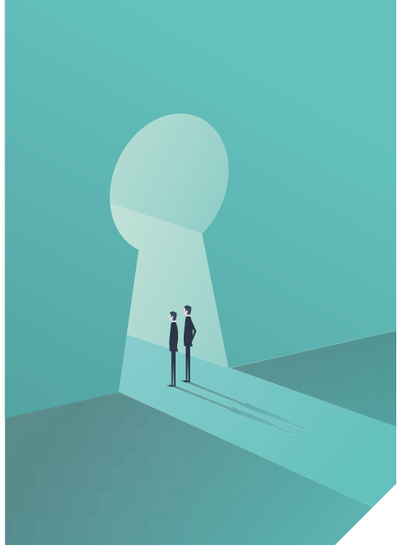
Systemy z tej grupy koncentrują się na zapewnieniu ciągłości i ukończenia określonego procesu. Procesy natomiast są determinowane charakterem organizacji, a ich podatność na zakłócenia jest wielowymiarowa. I tutaj ochrona ma także swoją rolę do odegrania. Jedną z częstszych przyczyn nieukończenia procesu jest brak, uszkodzenie lub zniszczenie zasobu krytycznego. Zasób nawet niewielkiej wartości materialnej może z czasem nabrać znaczenia krytycznego. Typowym przykładem zasobu krytycznego mogą być kule używane w młynach przemysłowych do mielenia kamienia, które się zużywają. Takich przykładów jest wiele w każdej branży. Z mojego ponad 20-letniego doświadczenia w branży ochrony wiem, że wszystkie mają co najmniej jeden zasób wspólny. Są nim klucze. Klucze, które giną, są kradzione albo wręcz przeciwnie są w nadmiarze i nikt ich nie kontroluje. W efekcie nie można np. otworzyć na czas pomieszczenia lub obiektu i mamy problem. Wyobraźmy sobie duży sklep otwierany z opóźnieniem – straty łatwo obliczyć. Jeśli jednak będzie częściej otwierany z opóźnieniem, straty będą dotyczyły nie tylko jednego dnia, a klienci odejdą do konkurencji. Nadmiar kluczy, zwłaszcza niekontrolowany, także może prowadzić do problemu. Przytoczę historię sprzed wielu lat, która wydarzyła się w jednym z wielkopolskich przedsiębiorstw. Istotne, ale drogie urządzenie parametryzujące kilka obrabiarek znajdowało się w pomieszczeniu zamykanym na klucz. Ponieważ sprzęt musiał być dostępny dla kilku osób na każdej zmianie, było więc ponad 30 kluczy. Zdarzyło się, że gdy był potrzebny, żadnego nie było na miejscu. Banalne? Niekoniecznie – postój trwał 4 godziny, trzeba było skontaktować się z wieloma osobami, ponieważ ktoś (nie wiedziano kto) zmienił zamek.
Innym przykładem, z którego „krytycznym znaczeniem" wielu z nas miało do czynienia, jest system obsługi bagażu na lotnisku. Uszkodzenie systemu powoduje, że pasażerowie, którzy wylądowali, nie mogą odebrać swoich walizek, a bagaż tranzytowy nie może zostać skierowany we właściwe miejsce. Również w przypadku takich systemów ochrona ma swoją rolę do odegrania, przede wszystkim w zakresie zabezpieczenia przed nieuprawnionym dostępem do elementów systemu. Lotniska z zasady są dobrze zabezpieczone, ale podobnie funkcjonują linie kompletacji zamówień w centrach logistycznych, a one bardzo rzadko są traktowane jako infrastruktura krytyczna.

W identyfikowaniu infrastruktury krytycznej kluczowe znaczenie ma cecha zasobu, jaką jest krytyczny wpływ na ciągłość działania firmy. Nie jej wartość czy innowacyjność, ale właśnie ta cecha, to ona bowiem może spowodować przestoje. A skoro tak, to identyfikując zasoby krytyczne, powinniśmy przede wszystkim patrzeć na ich wpływ na ciągłość biznesu. Bywając w różnych miejscach, dość często spotykam mienie, które ze względu na wiek jest już niewiele warte, księgowo ma wartość zerową, a mimo to, patrząc przez pryzmat ciągłości biznesu, ma ono wartość wyjątkową. Kilka miesięcy temu miałem okazję zobaczyć urządzenie iPAQ, którego nie widziałem już chyba dziesięć lat. Jego dzisiejsza wartość jest zerowa, jednak steruje ono istotnym procesem produkcyjnym i gdyby zginęło, pojawiłby się poważy problem – miejsce, w którym się znajduje, to dzisiaj zasób krytyczny. Firma na szczęście jest tego świadoma i ma zarówno plan zarządzania kryzysowego, jak i plan modernizacji. Wkrótce ten element procesu nie będzie już infrastrukturą krytyczną. Przykład ten skłania mnie do ciągłego szukania „bezcennego mienia bez wartości".

BUSINESS

Systemy biznesowe są skierowane na uniknięcie nadmiernych wydatków lub strat. Obecnie są to przede wszystkim systemy IT. Serwerownie główne i zapasowe, powszechnie traktowane jako zasoby krytyczne, z reguły są chronione zarówno fizycznie, technicznie, jak i proceduralnie. Jednak łańcuch jest tylko tak mocny, jak jego najsłabsze ogniwo. I tu pojawia się sporo takich potencjalnie słabych ogniw, poczynając od haseł przyklejonych do monitora, a kończąc na wydrukach zostawianych w drukarkach po zakończeniu pracy. Mimo powszechnej informatyzacji papier jest ciągle obecny w życiu biznesowym. Wiele firm nadal przyjmuje zamówienia faksem, ponieważ klienci takie urządzenia wciąż użytkują. Infrastruktura krytyczna może się wówczas sprowadzać do kilku kartek, o ile (1) zawierają odpowiednie informacje, a (2) w ich sąsiedztwie jest osoba, która takie zamówienia po prostu wrzuci do kosza. W efekcie takie informacje, jak cena i rabat (1) mogą się znaleźć w posiadaniu konkurencji, a zamówienia złożone po zakończeniu pracy (2) mogą zniknąć, stwarzając poważy problem biznesowy.
W tym kontekście właściwe zdefiniowanie i ochrona infrastruktury krytycznej łączy się z przeciwdziałaniem szpiegostwu. To zagrożenie jest wciąż aktualne. Jako przykład może posłużyć ujawniona w lutym 2014 r. kradzież informacji poufnych z jednego ze znanych zakładów przetwórstwa mięsnego w województwie wielkopolskim. W wyniku przeprowadzonego postępowania wyjaśniającego stwierdzono, iż osoba pracująca w tej firmie przekazywała konkurencyjnemu przedsiębiorstwu informacje dotyczące produkcji, sprzedaży i kontrahentów. Szczególnego znaczenia nabiera w tym aspekcie ochrona wszelkich miejsc dostępu do systemów controllingu finansowego i ERP (*Enterprise Resource Planning* – planowanie zasobów przedsiębiorstwa), gromadzących informacje, które należy zakwalifikować jako zasób krytyczny.
Systemy biznesowe o znaczeniu krytycznym to także takie, które mają wpływ na zarządzanie własnością intelektualną i reputację firmy. W pierwszym przypadku mamy szerokie spektrum, poczynając od miejsc prowadzenia spotkań biznesowych, które coraz częściej są traktowane jako infrastruktura krytyczna właśnie z powodu „niekontrolowanego ulotu informacji". Ich ochrona najczęściej sprowadza się do okresowego sprawdzania pomieszczeń pod kątem ewentualnych podsłuchów. W tym przypadku zasobem krytycznym jest jednak przede wszystkim człowiek, którego należy odpowiednio wyedukować, a także archiwa (informatyczne i tradycyjne).

Z perspektywy wizerunku firmy spektrum zasobów krytycznych jest równie szerokie, ponownie poczynając od miejsc dyskutowania newralgicznych projektów. Impreza integracyjna jednej z dużych firm wywołała przed laty szeroką dyskusję na temat zachowań zarządu i zmusiła PR oraz sam zarząd do zajmowania się tematem wizerunku przez wiele miesięcy. Można polemizować, czy miejsce organizacji imprezy integracyjnej należy traktować jako infrastrukturę krytyczną, czy też nie. Jedno jest pewne – jeśli z tego miejsca mogą wydostać się informacje, które zmuszą firmę do poniesienia dużych nakładów na poprawę wizerunku, a jednocześnie podważą zaufanie kontrahentów, to szef bezpieczeństwa ma tu dużo do zrobienia.



SECURITY

W systemach zabezpieczeń zawsze są przetwarzane dane wrażliwe. Z tego powodu dostęp do urządzeń powinien być szczególnie ograniczany, a bezpieczeństwo transmisji sygnału, jego rejestracji oraz zasilanie zasadnicze i awaryjne odgrywają kluczową rolę. Traktowanie ich jako infrastruktury krytycznej jest oczywiste. To samo dotyczy dostępu do materiału zarejestrowanego. Powinien być kontrolowany i limitowany, a uprawienia do kopiowania nadawane rozważnie. Oczywiście nie zabezpieczy to nas np. przed skopiowaniem za pomocą telefonu komórkowego, ale jeśli dobór personelu będzie właściwy, ryzyko takich incydentów znacznie spadnie.
Bardzo ważną sprawą w systemach zabezpieczeń jest pozostawianie w nich kodów fabrycznych. Ciekawym przykładem jest tu portal niebezpiecznik.pl, który co prawda pokazuje sejf hotelowy, ale co do zasady problem dotyczy wszystkich systemów.
Ostatnią sprawą jest traktowanie wiedzy pracowników ochrony jako zasób krytyczny. Wiedzy nie tylko na temat regulacji prawnych, ale także – a może przede wszystkim – umiejętności posługiwania się systemami zabezpieczeń i znajomości taktyki ochrony. W tym upatruję największych wyzwań. Ponownie posłużę się metaforą o najsłabszym ogniwie łańcucha – dobrze wykonana praca w zakresie identyfikacji zasobów krytycznych, połączona z dobrym ich zabezpieczeniem może zostać zniweczona niskim poziomem wiedzy zespołu ochrony.

BIO

Jacek Grzechowiak

Menedżer ryzyka i bezpieczeństwa. Przez kilkanaście lat związany z grupą Securitas, obecnie w grupie Celsa. Absolwent WAT, studiów podyplomowych w SGH i Akademii L. Koźmińskiego. Gościnnie wykłada na uczelniach wyższych.

Uszkodzenia infrastruktury kablowej

zagrożeniem dla bezpieczeństwa obiektów IK

TEKST
mgr inż. Stanisław Dziubak
Instytut Łączności, Państwowy Instytut Badawczy

TEKST
dr inż. Andrzej Sobolewski
Polska Agencja Przemysłowo-Obronna

Zagrożenia dla infrastruktury telekomunikacyjnej kablowej stanowi jedno z największych wyzwań dotyczących zapewnienia bezpieczeństwa obiektom infrastruktury krytycznej.

Najczęściej przyczynami uszkodzeń infrastruktury kablowej są zdarzenia losowe i starzeniowe oraz działania celowe.
Uszkodzenia losowe i starzeniowe to przede wszystkim:

- → roboty budowlane i drogowe, których skutkiem są przecięcia lub zgniecenia kabli oraz uszkodzenia kanalizacji i studni kablowych,
- → wypadki komunikacyjne powodujące uszkodzenia podpór linii napowietrznych i szaf ulicznych, uszkodzenia studni kablowych przez pojazdy,
- → warunki zewnętrzne: wichury, szkody górnicze, osuwiska gruntu, oblodzenie, uszkodzenia linii napowietrznych przez złamane drzewa,
- → błędy w trakcie prac przy utrzymaniu i eksploatacji sieci: przecięcia kabli, zwarcia przewodów, błędne przełączenia, nadmierne zginanie światłowodów,
- → starzenie kabli i osprzętu pod wpływem zmian temperatury, wilgoci i wibracji,
- → przegryzanie kabli przez szczury i inne zwierzęta.

Elementy sieci napowietrznych i szafy uliczne muszą sporadycznie wytrzymać temperaturę od -40°C zimą do 70°C latem, uwzględniając ich nagrzewanie wskutek nasłonecznienia. W tym ostatnim przypadku temperatura wewnątrz szafy z urządzeniami aktywnymi może przekroczyć nawet 80°C, co prowadzi do niestabilności parametrów, szybkiego starzenia i awarii urządzeń. Z kolei w temperaturze poniżej -25°C dochodzi do trwałego uszkodzenia i utraty pojemności hermetycznych akumulatorów ołowiowo-kwasowych używanych w systemach zasilania rezerwowego.

Uszkodzenia celowe są np. powodowane:

- → wandalizmem, dywersją i sabotażem. Przecięcie światłowodów w kilku punktach w celu zablokowania mechanizmów protekcji w sieci szkieletowej lub metropolitalnej to tani sposób na sparaliżowanie sieci obsługującej miasto, bank czy przedsiębiorstwo bez używania broni palnej, materiałów wybuchowych. Danych o lokalizacji i funkcji kabli mogą dostarczyć byli pracownicy firm telekomunikacyjnych, użytkujących sieć itp.

W kraju notowano m.in. przypadki przecinania kabli w celu popsucia reputacji konkurującego operatora lub konkurencyjnej firmy, by przejąć klientów, oraz w wyniku sporów o opłaty za przejście przez nieruchomości lub wynajem kanalizacji kablowej;

- → kradzieżą kabli miedzianych w celu ich sprzedaży na złom, często połączoną z uszkodzeniami studni kablowych oraz przecinaniem rur kanalizacji i kabli światłowodowych. Zdarzają się też przypadki nielegalnego korzystania z kanalizacji kablowej – układanie kabli przez obce firmy bez zgody właściciela i opłat; możliwe jest uszkodzenie już istniejącej infrastruktury;
- → instalowaniem odgałęzień do przechwytywania danych, także ze światłowodów.

W tym ostatnim przypadku instalacja odgałęzienia przez rozcięcie włókna światłowodowego i wstawienie pasywnego sprzęgacza odprowadzającego 1–20% sygnału powoduje w przesyle sygnału krótkotrwałą przerwę, a następnie trwały wzrost jego tłumienności, zwykle o 0,5–1,5 dB, stanowiący sumę strat sprzęgacza i dwóch złączy spawanych.
Odgałęzienie umożliwia też zagłuszanie lub wprowadzanie fałszywych danych. Wspólny port sprzęgacza znajduje się wtedy od strony odbiornika atakowanego łącza. Przerwa włókna podczas montażu odgałęzienia trwa od 2 do 4 minut. To może uniemożliwić wykrycie tego zdarzenia.
Bezpieczeństwo obiektom infrastruktury telekomunikacyjnej może zapewnić monitoring infrastruktury sieciowej. □

Integracja systemów

sposobem na zabezpieczenie infrastruktury krytycznej

TEKST
Tomasz Białek
inżynier ds. zintegrowanych systemów bezpieczeństwa

Infrastruktura krytyczna odgrywa niezwykle istotną rolę w prawidłowym funkcjonowaniu państwa i niezakłóconym życiu jego obywateli. Jej ochrona jest jednym z kluczowych priorytetów. Jak jest to ważne, potwierdza Ustawa o zarządzaniu kryzysowym z 26 kwietnia 2007 r. (Dz.U. 2007 nr 89 poz. 590).

Zgodnie z ustawą infrastruktura krytyczna to systemy oraz wchodzące w ich skład powiązane ze sobą obiekty funkcjonalnie, 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.

INFRASTRUKTURA KRYTYCZNA OBEJMUJE SYSTEMY:

a) zaopatrzenia w energię, surowce energetyczne i paliwa,
b) łączności,
c) sieci teleinformatycznych,
d) finansowe,
e) zaopatrzenia w żywność,
f) zaopatrzenia w wodę,
g) ochrony zdrowia,
h) transportowe,
i) ratownicze,
j) zapewniające ciągłość działania administracji publicznej,
k) produkcji, składowania, przechowywania oraz stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Nieprawidłowe działanie któregokolwiek z powyższych elementów niesie zagrożenie dla przedsiębiorców, instytucji, organów administracji publicznej, miast, powiatów, województw czy nawet całego kraju.
Jak stanowi wspomniana ustawa, przez ochronę infrastruktury krytycznej należy rozumieć wszelkie działania zmierzające do zapewnienia jej funkcjonalności, ciągłości działania i integralności w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom, ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury w przypadku awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.
Aby uchronić się przed zagrożeniami spowodowanymi przez klęski żywiołowe czy celowe działanie człowieka (np. sabotaż, terroryzm), infrastrukturę należy zabezpieczyć za pomocą elektronicznych systemów zabezpieczeń.

Najlepszą ochroną infrastruktury krytycznej jest dedykowana do tego typu zadań inteligentna platforma monitoringu wizyjnego Arkiv. Jest ona w pełni zintegrowana z systemem zarządzania bezpieczeństwem ProtegeGX. Zarówno Arkiv, jak i ProtegeGX są oparte na serwerach posiadających zaawansowane mechanizmy zabezpieczające ich bezawaryjne działanie. Są to m.in. nadmiarowy zasilacz i karta sieciowa. Z kolei cenne dane można zabezpieczyć za pomocą macierzy dyskowej RAID. System operacyjny serwerów może pracować, bazując na osobnej macierzy lustrzanej. Jeżeli zabezpieczany obiekt jest szczególnie ważny lub wrażliwy, zaleca się korzystanie z funkcji nadmiarowego serwera (*server failover*).

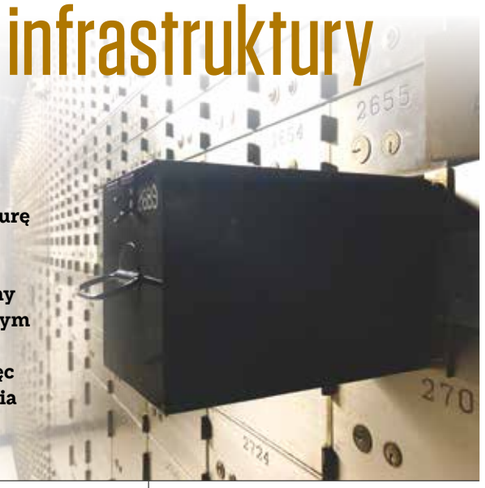
Aby system działał najefektywniej, należy dążyć do maksymalnej automatyzacji. Właśnie z tego względu serwery CCTV mają wbudowane zaawansowane funkcje analityki wideo, które potrafią automatycznie wykryć ogień bądź dym na obrazie z którejkolwiek z kamer znajdujących się w systemie. Potrafią również rozpoznać twarz poszukiwanej osoby, tablice rejestracyjne pojazdów, wykryć obiekty przecinające wcześniej zdefiniowane wirtualne linie lub monitorować obecność w zdefiniowanych strefach zagrożeń i wiele innych. Operator systemu zostaje zaalarmowany o tych zdarzeniach. Arkiv, dzięki zapisowi metadanych razem z materiałem wideo, jest w stanie w ułamku sekundy wyszukać zdarzenia również w nagraniach.

Podczas sytuacji kryzysowej tradycyjny sposób przeglądania danych jest niedopuszczalny. „Ślęczenie" przed monitorem i przeglądanie dostępnego materiału w poszukiwaniu interesującego nas zdarzenia może trwać niemal w nieskończoność i niebezpiecznie opóźniać podjęcie stosownych działań zaradczych. W systemie Arkiv wskazujemy jedynie wytyczne do wyszukiwania, a wyniki otrzymujemy natychmiast w formie miniatur. Możemy np. zaznaczyć strefę w kadrze, po czym wyszukać trzy osoby znajdujące się w tej strefie w tym samym czasie. Innym przykładem może być wyszukiwanie samochodów w określonym kolorze. Nikogo nie trzeba chyba przekonywać, że w sytuacji zagrożenia najważniejszy jest czas. Im szybciej operator zidentyfikuje zdarzenie, tym szybciej zainterweniują odpowiednie służby w celu zminimalizowania lub zapobieżenia jego skutkom.
Platforma monitoringu wizyjnego Arkiv jest kompatybilna z większością kamer IP dostępnych na rynku, a jako jeden z nielicznych systemów ma możliwość przejęcia strumieni wideo z rejestratorów zarówno IP, jak i analogowych. Powyższe cechy pozwalają zastosować Arkiv w istniejących już systemach, które nie mają tak zaawansowanych funkcjonalności.

Doskonałym uzupełnieniem funkcjonalności platformy Arkiv jest ProtegeGX – system łączący cechy systemu antywłamaniowego, kontroli dostępu, systemu zarządzającego windami oraz posiadającego funkcje automatyki budynkowej, rejestracji czasu pracy i rejestracji gości. Swoimi możliwościami przebija produkty konkurencji, może się poszczycić wieloma zadowolonymi użytkownikami z różnych branż i krajów. Dzięki zastosowaniu kart dostępu w najbezpieczniejszym standardzie Desfire, możemy być pewni, że niepowołane osoby nie dostaną się niezauważone na teren zabezpieczanego obiektu. Łącząc KD z SSWiN, ProtegeGX staje się spójnym produktem do kompleksowego zabezpieczenia budynku. Aby działał zgodnie z założeniami, nie można zapomnieć również o elementach detekcyjnych najwyższej jakości. Platforma ProtegeGX jest bardzo chętnie łączona z barierami podczerwieni i mikrofalowymi włoskiego producenta Mitech. Mimo że ProtegeGX działa w oparciu o serwer SQL, może pracować offline. Zatem w przypadku utraty komunikacji z serwerem nie staje się bezużyteczny. Cały czas zabezpiecza obiekt, przechodząc w tryb offline, a systemem zarządzają wówczas kontrolery.

Pełna synergia Arkiv i ProtegeGX umożliwia prawidłowe zabezpieczenie najważniejszych obiektów. Systemy komunikują się ze sobą, dzięki czemu można maksymalnie wykorzystać ich potencjał i jeszcze szybciej wykryć zagrożenia. System telewizji dozorowej, otrzymując informację o naruszeniu strefy w SSWiN, może skierować uwagę operatora, automatycznie pokazując np. obraz z kamery powiązanej z tą strefą lub wywołać odpowiedni preset kamery obrotowej mającej w zasięgu ww. strefę. ProtegeGX może z kolei pobierać materiał wideo z systemu Arkiv. Jest to bardzo wygodne rozwiązanie dla osoby obsługującej system ProtegeGX. Jeżeli w obiekcie nastąpi alarm lub siłowe otwarcie drzwi, operatorowi automatycznie zostaną wyświetlone najistotniejsze dla niego informacje. Dostanie precyzyjną informację, gdzie doszło do naruszenia systemu oraz obraz wyświetlony na żywo, natomiast w osobnym oknie zostanie pokazany film z chwili zdarzenia. Co istotne, zarówno Arkiv, jak i ProtegeGX są systemami skalowalnymi. Inwestycję można więc realizować etapami, nie ma potrzeby kupowania sprzętu od razu na cały projekt.
Ochrona infrastruktury krytycznej jest sprawą bezwzględnie ważną. Dzięki łącznemu zastosowaniu systemów Arkiv i ProtegeGX ten delikatny i skomplikowany system naczyń połączonych, jakim jest infrastruktura krytyczna, może być właściwie zabezpieczony i chroniony. Zaawansowana technologia Arkiv i ProtegeGX umożliwia szybką reakcję i pełną ochronę zasobów, obiektów, urządzeń czy instalacji mających podstawowe znaczenie dla prawidłowego i harmonijnego funkcjonowania gospodarki, państwa i życia jego obywateli. ▫

SSWiN dla obiektów infrastruktury krytycznej



Ustawa o zarządzaniu kryzysowym definiuje infrastrukturę krytyczną (IK) jako budynki, tereny, urządzenia, systemy oraz instalacje kluczowe dla bezpieczeństwa i funkcjonowania państwa. Ze względu na ich strategiczny charakter stosowane tam zabezpieczenia techniczne, w tym systemy alarmowe, powinny zapewniać wysoki stopień ochrony. Przy projektowaniu instalacji SSWiN należy więc sięgać po produkty spełniające rygorystyczne wymagania stopnia 3 (z ang. Grade 3) normy EN 50131.

Stopień 3 określa odporność systemu alarmowego na działania potencjalnych intruzów. Do obejścia takich zabezpieczeń potrzebna jest głęboka wiedza na temat ich działania i budowy, a także posiadanie i umiejętność korzystania ze specjalistycznych narzędzi.
System alarmowy spełniający wymogi Grade 3 musi mieć właściwości i funkcje wskazane przepisami, m.in. szyfrowanie danych oraz mechaniczną odporność na czynniki środowiskowe, akty wandalizmu czy sabotaż polegający na próbach demontażu jego elementów. W skład takiej instalacji SSWiN powinny wchodzić jedynie urządzenia stopnia 3 lub wyższego, gdyż o poziomie jej zabezpieczenia stanowi „najsłabsze ogniwo".

Zapewnienie ciągłości ochrony i natychmiastowej reakcji na niepożądane zdarzenia to podstawa w systemach bezpieczeństwa infrastruktury krytycznej.

System alarmowy i jego serce

Sercem systemu chroniącego obiekty IK może być jedna z zaawansowanych central rodziny INTEGRA Plus oferowanych przez SATEL. Oprócz wykrywania i informowania o próbach włamania rozwiązania te umożliwiają realizację funkcji kontroli dostępu oraz automatyki budynkowej. Najwyższy model serii – INTEGRA 256 Plus – obsługuje do 256 wejść (z możliwością programowania rezystancji parametrycznej oraz obsługą linii 3EOL) oraz wyjść.

Sterowanie systemem

Wśród modeli manipulatorów współpracujących z centralami INTEGRA Plus znajdują się zarówno nowoczesne, wyposażone w ekrany pojemnościowe manipulatory dotykowe (INT-TSI, INT-TSH i INT-TSG), jak również tradycyjne modele „klawiszowe" (INT-KLCD, INT-KLCDR, INT-KLFR). Pojedyncze strefy można obsługiwać z tzw. klawiatur strefowych INT-SCR.

Skuteczna detekcja

Zaawansowane dualne czujki OPAL Pro oraz AGATE, oprócz podwójnej ochrony sabotażowej, są wyposażone w aktywny antymasking IR (zgodny z EN 50131-2-4) – dzięki temu wszelkie próby ich unieszkodliwienia, polegające na zakryciu np. kartonem lub zamalowaniu lakierem bądź farbą, zostaną wykryte. Czujki te sprawdzą się w obiektach, w których panują niesprzyjające warunki środowiskowe, np. temperatura poniżej 0°C czy podwyższona wilgotność.

Pozostałe elementy

Ekspandery wejść i wyjść przewodowych: INT-E, INT-O oraz INT-PP służą do podłączania do centrali większej liczby urządzeń, niż wynika to z jej fizycznej konstrukcji. Moduły te można zasilić z posiadającego szereg zabezpieczeń oraz charakteryzującego się wysoką sprawnością zasilacza APS-612, również spełniającego wymogi Grade 3.
Centrala oraz współpracujące z nią moduły rozszerzeń i zasilacze powinny być umieszczone w obudowach zachowujących stopień zabezpieczenia całego systemu – tu za przykład mogą posłużyć: wykonana z tworzywa sztucznego obudowa OPU-3P czy metalowe modele serii OMI.

Zintegrowane zarządzanie bezpieczeństwem grupy obiektów

W przypadku zarządzania systemami bezpieczeństwa sieci obiektów strategicznym rozwiązaniem może okazać się specjalny program integrujący, taki jak INTEGRUM. To narzędzie stworzone przez inżynierów SATEL umożliwia wygodne kierowanie ochroną grupy placówek połączonych w jeden centralnie kierowany system. □

SATEL

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

Technologia radarowa sięga poza granice chronionego obiektu

Ze względu na duży zasięg detekcji i zdolność do działania w niesprzyjających warunkach atmosferycznych i w trudnym środowisku, włączenie radaru do systemu ochrony obwodowej może zapewnić operatorom obserwację na większą odległość, a przy tym oszczędności.

TEKST
Eifeh Strom

Technologie radarowe i lidarowe rozwijają się, rośnie też liczba ich zastosowań. Choć lidar jest znany przede wszystkim z zastosowań na rynku zaawansowanych systemów wspomagania kierowcy (ADAS – *advanced driver assistance system*) w pojazdach autonomicznych, to wykorzystuje się go również w takich branżach, jak obronność. Z kolei radar tradycyjnie cieszy się popularnością w zastosowaniach security i dozoru wizyjnego, szczególnie na lotniskach, w portach morskich, bazach wojskowych i ochronie granic.

Na światowym rynku w 2017 r. przewodził region Ameryki Płn. Z kolei do wzrostu w Europie przyczyniają się – wg najnowszego raportu Zion Market Research (ZMR) – bieżące programy rozwoju technologicznego oraz rozszerzania ochrony radarowej i dozoru wizyjnego. Region Azji i Pacyfiku (APAC) natomiast rósł najszybciej. Według szacunku ZMR globalny rynek technologii radarowych w zastosowaniach security i dozoru wizyjnego do 2024 r. osiągnie prawie 10,6 mld USD (wobec 7 mld USD w 2017r.). Wzrost wynika głównie z większej sprzedaży radarów nawigacyjnych, wykorzystywanych przez bezzałogowe statki powietrzne (UAV), a także rosnącego popytu na lżejsze i energooszczędne urządzenia.

Radar lepszy

W ochronie obwodowej można stosować zarówno radar, jak i lidar, jednak z kilku powodów ten pierwszy sprawdza się lepiej. Chociaż oba rozwiązania umożliwiają skanowanie w zakresie 360°, to ich możliwości i metody wykrywania są różne. Co więcej, także dane przez nie są dostarczane innej natury – radar może „widzieć" dalej, lidar ma lepszą rozdzielczość obrazu. W rezultacie ich cechy sprawiają, że jako rozwiązania do ochrony perymetrycznej nie są swoimi zamiennikami. Radar jest lepiej dostosowany do monitorowania rozległego obszaru ze względu na duży zasięg detekcji. Lidar natomiast działa na znacznie krótszym dystansie ze względu na wpływ warunków atmosferycznych i ograniczoną moc wyjściową. Oba rozwiązania są zwykle używane do wykrywania intruzów (zarówno ludzi, jak i pojazdów), ostatnio znalazły też zastosowanie w przechwytywaniu dronów.

Z perspektywy ochrony obwodowej radar jest lepszym wyborem. W porównaniu do tradycyjnych zabezpieczeń umożliwia detekcję po wewnętrznej stronie granicy, a także na zewnątrz chronionego obszaru. Daje pełen wgląd w zdarzenia mające miejsce na terenie obiektu i poza nim. Ma też znaczną przewagę nad lidarem i innymi technologiami ochrony obwodowej ze względu na zdolność do działania w niekorzystnych warunkach atmosferycznych i oświetleniowych. Na funkcjonowanie radaru nie mają wpływu żadne zmiany środowiskowe. Z kolei pracę lidaru może zakłócać pył, piasek i mgła, powodując spadek jego wydajności. Jest on również nieodporny na silne opady deszczu i śniegu.

Kolejną zaletą zastosowania radaru na dużych obszarach jest to, że jest on tańszy od tradycyjnych systemów ochrony obwodowej, takich jak ogrodzenia, zabezpieczenia mechaniczne, oświetlenie czy kamery dozorowe. Jeden radar może pokrywać detekcją obszar setek kilometrów kwadratowych, jest niezawodny, pracuje przy każdej praktycznie pogodzie w dzień i w nocy, bez obciążeń stałymi kosztami. A ponieważ jego zasięg jest większy, potrzeba mniej innych czujników do pokrycia zasięgiem tego samego obszaru. Zaletą dozorowania dużego obszaru jest to, że radar dostarcza operatorom ostrzeżenia z wyprzedzeniem, dzięki czemu mają więcej czasu na przechwycenie intruzów. Cały czas śledzi intruzów na chronionym terenie, więc operatorzy znają ich dokładną lokalizację. Tradycyjne metody są znacznie mniej precyzyjne i często mogą wykrywać intruza tylko przy ogrodzeniu, nie przekazując żadnych informacji, gdy się od niego oddali.

Nie oznacza to jednak, że radar jest rozwiązaniem idealnym. Technologie radarowa i lidarowa są nieodporne na przeszkody w polu widzenia. Przykładowo duże obiekty, takie jak budynki czy drzewa, mogą wpłynąć na skuteczność wykrywania. Instalując radary, należy upewnić się, czy mają one czyste pole widzenia, nie są bowiem w stanie „przenikać" obiektów. Ważne jest również, aby je lokalizować z dala od dużych obiektów, które mogą powodować odbicia o dużej części emitowanej energii, co ograniczy skuteczność rozwiązania. Jeśli z jakichś powodów instalacja musi znaleźć się blisko dużego obiektu, emisję można kontrolować – przy obrocie radaru, gdy trafi na przeszkodę, wiązka jest wyłączana, co eliminuje odbicia. Radar musi być instalowany wystarczająco wysoko nad ziemią – im dłuższy jego zasięg, tym wyżej powinien być zamontowany.

Najbardziej zainteresowani

Popyt na technologie radarowe i lidarowe stale rośnie. Jednym z tego powodów mogą być takie zdarzenia, jak niedawne wtargnięcia na tereny lotnisk, które spowodowały poważne zakłócenia w lotach, zaszkodziły reputacji portów

W porównaniu z tradycyjnymi zabezpieczeniami radar uważa się za rozwiązanie lepsze, ponieważ umożliwia detekcję zarówno wewnątrz obszaru chronionego, jak i na zewnątrz jego granicy .

KAMERA I RADAR – IDEALNA PARA

Jednym ze sposobów uzupełnienia niedostatków radaru w ochronie obwodowej jest powiązanie go z innym detektorem, np. kamerą dozorową.

Podobnie jak radar, same kamery nie są wystarczająco skutecznym rozwiązaniem zabezpieczającym chronione granice. Po zintegrowaniu obu rozwiązań operatorzy security będą uzyskiwać dostarczane przez radar dane o lokalizacji uzupełnione obrazem z kamer. Dzięki kamerom można dokonać weryfikacji „swój czy wróg", ale przekazują one obraz tylko z tego rejonu, który obserwują. Identyfikacja staje się trudniejsza, gdy cele są liczne lub znajdują się w większej odległości, kamera musi wtedy wykonać zbliżenie, przy którym jej pole widzenia znacznie się zmniejsza. Ograniczta to świadomość sytuacyjną. W tym czasie, gdy kamera skupia się na identyfikacji odległego intruza, inni, będący poza jej polem widzenia, mogą wejść do monitorowanej strefy. Radary z kolei wykrywają wszystkie cele o dowolnych rozmiarach bez konieczności zmiany pola widzenia: od tak małych, jak komercyjne drony, aż po statki wycieczkowe. Radar nieustannie skanuje przestrzeń 360°, szukając wszystkich celów, od których odbita energia powraca do radaru.

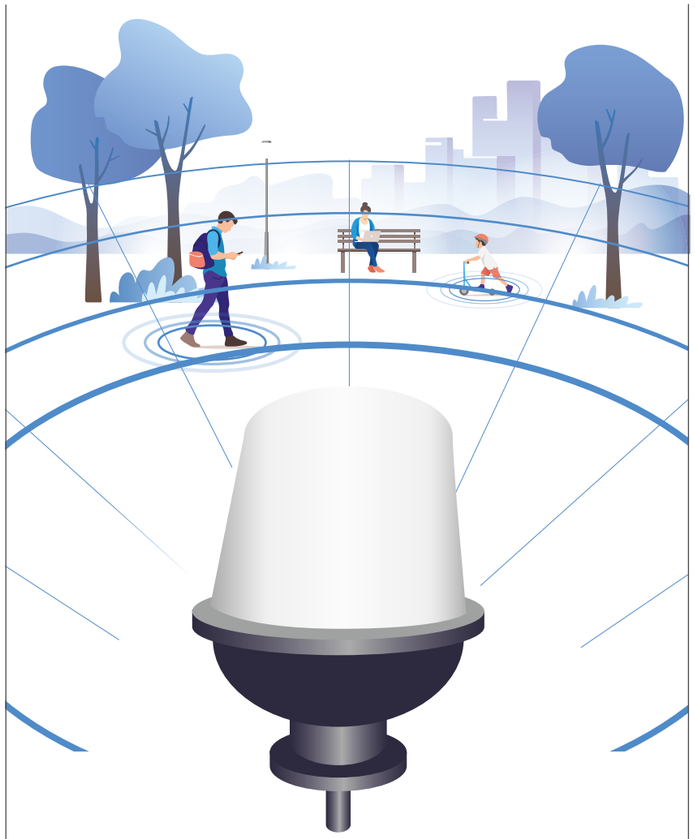
Idealne rozwiązanie ochrony obwodowej obejmuje radar, kamerę oraz oprogramowanie sterujące i zarządzające. Radar wykrywa cel, a oprogramowanie wydaje polecenie kamerze, aby skierowała się na niego w celu zidentyfikowania intruza.
Niektóre technologie radarowe można zintegrować z kamerami termowizyjnymi lub tradycyjnymi albo z siecią innych czujników w celu pełnego pokrycia obszaru, rozróżnienia celów i dostarczania informacji dotyczących ich prędkości, kierunku ruchu i rozmiaru.

i wymagały kosztownych działań PR w zarządzaniu kryzysowym. Z kolei w obiektach infrastruktury krytycznej dąży się do obniżenia kosztów ochrony i ograniczenia liczby fałszywych alarmów.

Lidar sprawdza się w ochronie obwodowej w zastosowaniach niewymagających dużego zasięgu detekcji, gdzie nie panują niekorzystne warunki atmosferyczne. Sprowadza się np. do hal przemysłowych i innych zastosowań wewnętrznych. Do ochrony dużych otwartych przestrzeniach idealną propozycją jest radar – odporne rozwiązanie, sprawdzające się w niekorzystnych warunkach meteorologicznych i trudnych środowiskach. Dzięki dużemu zasięgowi detekcji największe korzyści są osiągane w wykrywania intruzów na rozległych obszarach zarówno wewnątrz, jak i poza ich granicą zewnętrzną. Natomiast gdy obszar chroniony znajduje się pośrodku lasu i jest otoczony drzewami lub innymi wysokimi obiektami, radary nie będą najlepszym wyborem. Korzyści z ekonomicznego, stałego monitoringu zapewnianego przez radary odniosą obiekty działające na otwartej przestrzeni.
Dotyczy to infrastruktury krytycznej (ale nie ogranicza się tylko do niej), rezydencji, zapór, portów morskich i lotniczych, więzień, granic państwa, instalacji wojskowych, stadionów, budynków rządowych, elektrowni i podstacji. Stałe pokrycie, praca w dzień i w nocy w każdych warunkach atmosferycznych, niewielkie rozmiary, duży zasięg, efektywność kosztowa i względna niejawność działania przyczyniają się do akceptacji techniki radarowej.

Postępy w technologii radarowej

Jak twierdzi badająca rynek firma Zion Market Research, postęp technologiczny w systemach radarowych może w najbliższej przyszłości stworzyć nowe możliwości na rynku radarowej ochrony i dozoru. Wzrost popytu na technologie radarowe i lidarowe sprawił, że producenci pracują nad rozwiązaniami dostosowanymi do konkretnych potrzeb nabywców. Do coraz większego ich wykorzystania w ochronie obwodowej przyczynia się rozwój technologii, ulepszone algorytmy klasyfikowania celów, spadek cen oraz łatwość użycia.
Gdy do różnych zagrożeń dołączyły drony, radary trzeba było dostosować do wykrywania tych urządzeń. Tradycyjnie radary stosowane w ochronie obwodowej są naziemne i służą do wykrywania intruzów przy ziemi. Mają kąt wzniesienia (elewacji) wiązki 5 stopni lub mniejszy. Niedawno pojawiły się rozwiązania (np. serii FLIR



Tradycyjnie radary stosowane w ochronie obwodowej i służą do wykrywania intruzów przy ziemi. Niedawno pojawiły się rozwiązania służące również do wykrywania dronów.

Ranger) służące również do wykrywania zagrożeń powietrznych (takich jak drony), w których kąt wzniesienia wynosi od 20 do 60 stopni. Takie radary zapewniają niemal hemisferyczną detekcję zagrożeń zarówno na ziemi, jak i w powietrzu. Firma Navtech Radar z kolei ulepszyła swój system AdvanceGuard, który jest wysokiej rozdzielczości rozwiązaniem radarowym do monitoringu. Oferuje on teraz także opcję weryfikacji „swój czy wróg". System wykorzystuje detekcję opartą na regułach, działania legalne są odfiltrowywane, a poziom fałszywych alarmów ograniczony do minimum. System analizuje zachowania, rozróżniając zdarzenia dozwolone, takie jak uprawniony pojazd pracownika, od intruzów i zagrożeń. Zapewniając świadomość sytuacyjną całego zdarzenia, dostarcza operatorom informacje o dokładnej lokalizacji intruza w czasie rzeczywistym. Jego zdolność do wczesnego wykrywania ma kluczowe znaczenie na tak trudnym obszarze, jak lotniska, gdzie intruz musi być przechwycony, zanim naruszy bezpieczeństwo. Ogranicza to zakłócenia w funkcjonowaniu obiektów, które mogą być długotrwałe, kosztowne i niebezpieczne.

W nadchodzących latach powinien nastąpić sukcesywny rozwój technologii, producenci będą dokładać starań, by móc zaoferować klientom jak najlepsze rozwiązania. □

Automatyczne śledzenie PTZ

w AXIS Perimeter Defender Autotracking

NAJWAŻNIEJSZE KORZYŚCI:

- Szczegółowe informacje nt. obiektów powodujących alarmy bez ograniczania obszaru detekcji
- Automatyczne sterowanie kamerą PTZ
- Automatyczne utrzymywanie wszystkich podejrzanych obiektów w polu widzenia kamery PTZ
- Jeden program zarządzający umożliwiający skonfigurowanie funkcji analizy w kamerze stałopozycyjnej oraz aplikacji do automatycznego śledzenia w kamerze PTZ

AXIS Perimeter Defender zapewnia przewagę nad intruzem tam, gdzie powinna zaczynąć się ochrona obiektu, czyli już w strefie obwodowej. Ta aplikacja do analizy zawartości wizji, w połączeniu z kamerami sieciowymi Axis tworzy niezwykle skuteczny system, który automatycznie wykrywa osoby i pojazdy próbujące dostać się na chroniony teren obiektu, a następnie śledzi ich ruch.

Jest również elementem fizycznej kontroli dostępu stosowanej przy bramach i wejściach na teren obiektów, w których konieczne jest zapewnienie wysokiego stopnia bezpieczeństwa, takich jak zakłady chemiczne, elektrownie czy zakłady karne. W wyniku prac udoskonalających w oferowanym obecnie przez Axis Communications oprogramowaniu analitycznym AXIS Perimeter Defender wprowadzono aplikację służącą do automatycznego śledzenia PTZ. Aplikacja umożliwia płynną współpracę kamery stałopozycyjnej z kamerą PTZ, tworzac rozwiązanie zapewniające większą skuteczność ochrony obwodowej. Tradycyjna lub termowizyjna kamera stałopozycyjna z oprogramowaniem AXIS Perimeter Defender wykrywa osoby i pojazdy, a z chwilą wyzwolenia alarmu – przejmuje kontrolę nad kamerą PTZ w celu śledzenia i przybliżania obiektów, które spowodowały alarm.

Na obrazach nocnych pochodzących ze stałopozycyjnej kamery termowizyjnej (po lewej) i kamery PTZ (po prawej) przedstawiono efekt współpracy obu tych kamer z aplikacją AXIS Perimeter Defender PTZ Autotracking

Korzystając z aplikacji, kamera stałopozycyjna wysyła dane o lokalizacji obiektów-źródeł alarmu do kamery PTZ, sterując automatycznie jej kierunkiem patrzenia i stopniem zoomu, aby zapewnić widok wszystkich obiektów, które wywołały alarm, a także ewentualnych nowych obiektów pojawiających się w strefie detekcji kamery stałopozycyjnej. Dzięki tej aplikacji kamera stałopozycyjna zapewnia dozór na dużym obszarze, kamera PTZ natomiast automatycznie przybliża obraz w momencie wyzwolenia alarmu, aby zapewnić więcej szczegółów dotyczących podejrzanego obiektu. Operator może przejąć kontrolę nad kamerą PTZ i ręcznie nią sterować, np. gdy obserwowane obiekty opuszczą strefę detekcji kamery stałopozycyjnej, co powoduje zatrzymanie automatycznego śledzenia PTZ.

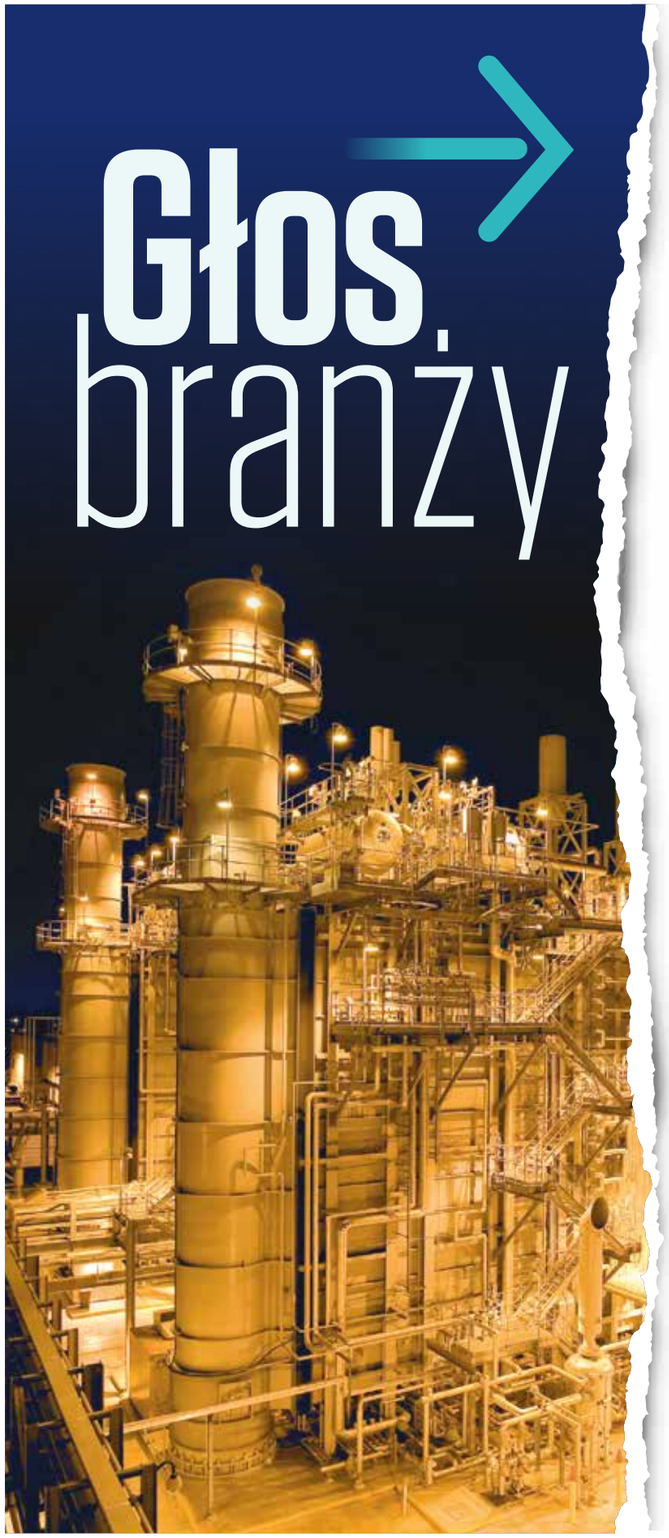
Aplikacja AXIS Perimeter Defender PTZ Autotracking jest zgodna z wybranymi modelami PTZ Axis i umożliwia współpracę jednej kamery stałopozycyjnej z jedną kamerą PTZ. Funkcja ta wymaga osobnej licencji w oprogramowaniu analitycznym AXIS Perimeter Defender. Początkowo aplikacja PTZ Autotracking będzie dostępna w Europie i Izraelu. W innych regionach zostanie wprowadzona w późniejszym terminie.

AXIS Perimeter Defender to aplikacja przeznaczona do wykrywania poruszających się ludzi i pojazdów. Wykorzystuje obraz 3D sceny, umożliwiając dokładną weryfikację obiektu – aplikacja klasyfikuje ludzi i pojazdy. Można wybrać, czy mają być wykrywane pojazdy, pojazdy i ludzie, czy tylko ludzie.
AXIS Perimeter Defender pozwala zminimalizować fałszywe alarmy na wiele sposobów. Aplikacja uczy się automatycznie różnicy między „dniem" a „nocą" i wykorzystuje te informacje do precyzyjnego dostrojenia algorytmu w celu uzyskania optymalnej skuteczności. Radzi sobie ze zmiennym oświetleniem i ignoruje ruch generowany przez np. kołyszącą się roślinność lub szybko przemieszczające się cienie. Zmniejsza również liczbę fałszywych alarmów powodowanych światłami reflektorów. Aplikacja obsługuje jednocześnie wiele scenariuszy detekcji, dzięki czemu można dostosować konfigurację do indywidualnych potrzeb. Wysoka skuteczność detekcji AXIS Perimeter Defender i niewielka liczba fałszywych alarmów, szczególnie w połączeniu z kamerami termowizyjnymi, umożliwiają utworzenie niezawodnego systemu.
Więcej informacji na https://www.axis.com/products/axis-perimeter-defender

Axis Communications Poland

ul. Domaniewska 44
bud. 4
02-672 Warszawa
www.axis.com/pl

Głos branży



OBIEKTY I SYSTEMY INFRASTRUKTURY KRYTYCZNEJ POWINNY BYĆ ZABEZPIECZONE PRZED ZAGROŻENIAMI ZARÓWNO FIZYCZNYMI, JAK I CYBERNETYCZNYMI. BEZPIECZEŃSTWO IK STANOWI JEDEN Z PRIORYTETÓW PAŃSTWA.

Maciej Pietrzak

Technical Team Leader,
Dahua Technology Poland

Wyzwania współczesności

Szybki postęp technologiczny i rozwój otwiera przed nami wiele nowych możliwości. Wystarczy prześledzić historię ostatnich lat, żeby zobaczyć, czego już dokonaliśmy. Nie bez powodu mówi się, że jesteśmy świadkami kolejnej rewolucji przemysłowej, określanej jako Przemysł 4.0, której głównymi filarami są Internet Rzeczy, rozwój algorytmów sztucznej inteligencji oraz *big data*.

Czy społeczeństwo jest już gotowe na tak duży postęp technologiczny? Głównym celem rozwoju technologicznego jest zwiększenie wydajności i niezawodności. Tymczasem wg ekspertów ludzie wykorzystują zaledwie kilka procent możliwości dostępnej technologii. Wynika to przede wszystkim z rozbudowanej funkcjonalności i braku dostatecznej wiedzy. Jej brak ma również ogromne znaczenie dla bezpieczeństwa. Według danych Głównego Urzędu Statystycznego z 2018 r. w Polsce stały dostęp do Internetu posiada 84,7% społeczeństwa. Coraz więcej osób ma konto na portalu społecznościowym, korzysta z bankowości elektronicznej, dokonuje transakcji internetowych – wartość płatności internetowych w 2018 r. wyniosła 626 mld USD. Razem z benefitami wynikającymi z rozwoju pojawiły się również zagrożenia. Straty spowodowane cyberatakami wynoszą 1%. Ryzyko potencjalnego cyberataku znajduje się na drugim miejscu pod względem szkodliwości. Co ciekawe, 33% strat powstałych w przedsiębiorstwie nie wynika z ataku na pracowników, a mimo to tylko 3% spółek deklaruje pełne przygotowanie w zakresie cyberbezpieczeństwa (źródło: https://www.pwc.pl/pl/pdf/publikacje/2018/cyber-ruletka-po-polsku-raport-pwc-gsiss-2018.pdf).

Jakie grzechy popełniamy najczęściej? Mimo częstych kampanii informacyjnych nadal wiele osób nie przestrzega podstawowych zasad tworzenia i przechowywania haseł dostępu. Administratorzy mogą wywierać wpływ na pracowników i dbać o to, aby hasła były bezpieczne i zmieniane odpowiednio często, ale nadal zagrożenie istnieje chociażby w wyniku ataku wykorzystującego inżynierię społeczną. Badania pokazują, że to najskuteczniejsza metoda zdobywania informacji. Brak czujności pracowników prowadzi najczęściej do ujawnienia informacji, które nie powinny trafić do osoby postronnej.

Producenci systemów informatycznych stale podnoszą jakość stosowanych zabezpieczeń, np. wprowadzając szyfrowanie danych. Niestety bardzo często opracowywane poprawki nie są wykorzystywane w praktyce, ponieważ administratorzy nie wykonują aktualizacji. Wniosek, jaki się nasuwa, jest taki, że nieważne jak duże nakłady poniesiemy na zabezpieczenia sprzętowe i oprogramowanie, zawsze na końcu pojawia się użytkownik i to on jest najsłabszym ogniwem całego systemu. Konieczne są kampanie podnoszące świadomość zagrożeń wynikających z cyberataków. Dobrą praktyką, jaka powinna być stosowana w przedsiębiorstwach, jest organizowanie obowiązkowych szkoleń dla wszystkich pracowników nt. zagrożeń i sposobów ochrony przed nimi. Warto też rozważyć wprowadzenie procedur, które należy postrzegać nie jako utrudnienie życia pracownika, ale jako sposób ochrony zarówno pracownika, jak i danych firmy.

> Bez względu na zabezpieczenia sprzętowe i oprogramowanie zawsze na końcu pojawia się użytkownik i to on jest najsłabszym ogniwem całego systemu.

Ireneusz Pawłowski

dyrektor zarządzający,
Biuro Bezpieczeństwa i IT,
Polski Holding Obronny

Krwiobieg bezpieczeństwa

Infrastruktura krytyczna stanowi szczególny fragment systemu organizacji państwa. Nazwałbym ją krwiobiegiem bezpieczeństwa kraju. To niezwykle istotna i wrażliwa materia, podatna na różne ryzyka. Problem dodatkowo komplikuje fakt, że niestety duża część infrastruktury znajduje się w rękach prywatnych. W związku z tym właściwe organy i agendy administracji państwa starały się wypracować formułę współpracy z biznesem.

Oceniając branżę ochrony, ze szczególnym uwzględnieniem ochrony infrastruktury krytycznej, uprawniony jest wniosek, że regulacje dotyczące bezpieczeństwa IK wymagają istotnych zmian legislacyjnych. W przestrzeni publicznej często słyszymy o profesjonalizacji, korzystaniu z nowoczesnych technologii w realizacji usług bezpieczeństwa. To wszystko prawda, ale niewiele mówi się o najważniejszym, a jednocześnie (w rozumieniu bezpieczeństwa) newralgicznym ogniwie systemu, czyli pracowniku ochrony.

Niestety rzeczywistość pokazuje nam, że w tym zakresie pożądane są bardziej restrykcyjne wymagania w stosunku do wykonawców świadczących usługi ochrony IK. Dobrze przeszkolony, odpowiednio wynagradzany pracownik jest gwarantem, że będzie solidnym aktywem w systemie zabezpieczeń.

Takie standardy wprowadza Polski Holding Obronny. Nie stosujemy powszechnych w tej branży formuł zatrudnienia pracowników na podstawie umowy o pracę i umowy zlecenia w innej spółce z grupy kapitałowej. Dzięki temu nie mamy dużej rotacji pracowników, co zapewnia szczelność informacji. Przede wszystkim zaś odprowadzamy wszystkie należne Skarbowi Państwa zobowiązania. To szczególnie istotne wobec pojawiających się nowych kategorii zagrożeń. Poza tym uważamy, że równie ważne są systemy weryfikacji dostawców oparte na certyfikatach, np. poświadczenia bezpieczeństwa przemysłowego czy zabezpieczenie operacji solidnymi polisami ubezpieczeniowymi. Głęboko wierzymy, że sygnalizowane nowelizacje aktów prawnych dotyczących ochrony infrastruktury krytycznej będą uwzględniały i te aspekty.

Piotr Kiliszek

dyrektor Biura Bezpieczeństwa,
Jastrzębska Spółka Węglowa

Działać zgodnie z RODO...

Największym problemem w ochronie infrastruktury krytycznej jest – moim zdaniem – pogodzenie interesu ochrony z obostrzeniami nakładanymi przez RODO. Dzięki rozwojowi technologicznemu widzimy więcej, dalej i w każdych warunkach. Możemy analizować zachowania, rozpoznawać twarze, kontrolować pojazdy i ich kierowców, ale tematem wielu dyskusji jest styk możliwości technologicznych z prawami osób objętych działaniem monitoringu wizyjnego.

Poważnym problemem jest wyważenie interesu pracodawcy i praw osoby, która znajduje się na terenie obiektu. Ale tutaj kontekst jest szerszy, bo dotyczy obserwacji również otoczenia takich obiektów. Gdzie leży granica? Jak daleko ma sięgać dozór wizyjny wokół obiektów?

Takich pytań jest dużo. Każdy z praktyków na podstawie własnych doświad-

czeń ma inne zdanie i to jest cenne, natomiast prawdziwą sztuką będzie doświadczenia te zebrać, skategoryzować i dopasować do ram prawnych. Myślę, że należałoby stworzyć przy udziale instytucji rządowych pewnego rodzaju zestawienie wytycznych, które jednoznacznie wyznaczą kierunki wymagań i zgód w zakresie zabezpieczenia tak ważnych obiektów dla gospodarki państwa. Mimo że Polska jest krajem spokojnym, nie możemy popełnić grzechu zaniechania. Każda odpowiedzialna osoba ma świadomość, że balansujemy między niedopełnieniem obowiązków a przekroczeniem uprawnień. Mając dokument stanowiący choćby wytyczne, znajdziemy wsparcie do realizacji stawianych nam zadań. Wtedy, jako osoby odpowiedzialne za bezpieczeństwo, będziemy mogli użyć dostępnego potencjału technologicznego bez narażania się na zarzut naruszania np. RODO.

Sytuacja będzie również komfortowa dla producentów sprzętu – znając wymagania i wprowadzone ograniczenia, uwzględnią je w swojej ofercie. Liczę na to, że takie rozwiązania zostaną wprowadzone jako działanie wyprzedzające, a nie w reakcji na wydarzenie lub kosztowne postępowanie sądowe. Reasumując, myślę, że wyzwaniem, którego musimy opanować, jest stworzenie ram, które pozwolą wykorzystać wszelkie nowinki techniczne, a jednocześnie nie będziemy naruszali praw, co jako odpowiedzialni za bezpieczeństwo powinniśmy czynić w pierwszym rzędzie.

Witold Skomra

Rządowe Centrum Bezpieczeństwa

Zarządzanie bezpieczeństwem

Wdrożenie technologii Internetu Rzeczy (IoT) i Przemysłu 4.0 jest ciągle przed

Sprawy związane z bezpieczeństwem muszą stać się „elementem DNA" firmy. Trzeba je włączyć do wszystkich procesów biznesowych.

nami, ale już obecnie pewne elementy z nimi związane dotykają szeroko rozumianego bezpieczeństwa organizacji i obiektów, którymi te organizacje zarządzają. Krótko mówiąc, IoT to bezpośredni przepływ danych z czujnika do urządzenia wykonawczego, natomiast przemysł 4.0 to połączenie hardware'u i software'u w urządzeniu pozostającym w interakcji z innymi urządzeniami i człowiekiem. W obu przypadkach jednym z większych wyzwań jest zbudowanie systemu, który by kontrolował, czy autonomiczne systemy i urządzenia pracują poprawnie.

Ten problem, choć oczywiście w mniejszej skali, występuje już dziś. Coraz bardziej rozbudowywane systemy ochrony fizycznej, przeciwpożarowej i zarządzania infrastrukturą budynku wymagają narzędzi do monitorowania poprawności ich funkcjonowania i zarządzania sytuacjami awaryjnymi. Powstające aplikacje i systemy zarządzania infrastrukturą (BMS – *Building Management Systems)* to nic innego, jak właśnie systemy zarządzające innymi systemami.

Trzeba zaznaczyć, że coraz częściej w nowoczesnych systemach sterowania korzysta się z analiz behawioralnych. Ich stosowanie pozwala na łatwiejsze administrowanie całą infrastrukturą obiektu i ogranicza koszty obsługi, a jednocześnie identyfikuje nowe rodzaje zagrożeń, np. możliwość przechwycenia przesyłanych danych z systemów wizyjnych i kontroli dostępu, czy zagrożenia związane z możliwością ataku hakerskiego. Dlatego muszą one być brane pod uwagę jako elementy podatności przy opracowywaniu planu ochrony czy planu ciągłości działania przedsiębiorstwa. Jest to szczególnie ważne, gdy mamy do czynienia z infrastrukturą krytyczną – krytyczną z punktu widzenia państwa i w rozumieniu utrzymania celu działania dowolnej organizacji.

Jednym z problemów do rozwiązania przy określaniu standardu bezpieczeństwa dla systemów zarządzania infrastrukturą obiektu jest brak ich właściwej kwalifikacji. O ile początkowo te systemy jedynie obrazowały stan pracy urządzeń i były zaliczane do systemów informatycznych (IT), o tyle obecnie coraz częściej same posiadają urządzenia wykonawcze, co kwalifikuje je do obszaru sterowania przemysłowego (OT). Być może rozwiązaniem tego dylematu jest wprowadzenie i zdefiniowanie pojęcia, które obrazowałoby cele i zadania systemu zajmującego się wyłącznie poprawnością i bezpieczeństwem funkcjonowania innych systemów.

Janusz Syrówka

Country Security Chair,
innogy Polska S.A.
Dział Bezpieczeństwa,

Nowe przepisy, nowe wyzwania

Rok 2019 dla firm związanych z szeroko rozumianą infrastrukturą krytyczną będzie z pewnością kojarzony z wejściem w życie ustawy o krajowym systemie cyberbezpieczeństwa. Nie chciałbym skupiać się na przepisach, a w zasadzie na kontrowersjach ich dotyczących. Uważam, że mimo wszystko ustawa to krok w dobrym kierunku i jej wdrożenie przyniesie duże korzyści. Nowe przepisy są doskonałą okazją, żeby spojrzeć na firmę pod trochę innym kątem. Zazwyczaj najważniejszym elementem jest rentowność prowadzonej działalności. Dzięki ustawie element zapewnienia ciągłości świadczenia usługi znacząco się wzmacnia. Nie oznacza to, że pojęcie ciągłości jest czymś nowym we współczesnym biznesie.

Nowość polega na kompleksowym podejściu i stworzeniu samoregulującego się mechanizmu opartego na szacowaniu ryzyka i zarządzaniu nim. Aby tak się stało, sprawy związane z bezpieczeństwem muszą stać się „elementem DNA" przedsiębiorstwa. Słowo „bezpieczeństwo" rozumiem jako określenie stanu rzeczy, bez odniesień do rozwiązań strukturalnych czy też firm świadczących usługi bezpieczeństwa. Zapewnienie ciągłości usługi to swego rodzaju zagwarantowanie klientowi bezpieczeństwa poprzez nieprzerwane dostarczanie wody, prądu, gazu, usług komunikacyjnych itp. Jedyną drogą, aby to osiągnąć, jest włączenie kwestii bezpieczeństwa do wszystkich procesów biznesowych w firmie oraz zaangażowanie ogółu pracowników. Szczególnie istotna jest świadomość i zaangażowanie kadry zarządzającej. Oczywiście znajdą się liczne elementy systemu bezpieczeństwa możliwe do outsourcingu. Nie da się tego jednak zrobić całkowicie poza organizacją, chociażby ze względu na kwestie zarządzania ryzykiem i odpowiedzialności.

Nowe regulacje prawne mogą wymusić pewne zmiany organizacyjne. Istnieje też możliwość, że wymuszą dodatkowe koszty. Największym jednak wyzwaniem będzie właściwe zrozumienie istoty zmian i nowego, całościowego spojrzenia na bezpieczeństwo. Bezpieczeństwo fizyczne, cyberbezpieczeństwo, bezpieczeństwo informacji, ciągłość działania i zarządzanie kryzysowe tworzą kompleksową sferę ochronną dla firmy, jej pracowników i klientów. Odporność tej sfery wcześniej czy później zostanie zweryfikowana przez zagrożenia, które brutalnie pokażą, czy została zbudowana z papieru zapisanego pobożnymi życzeniami, czy też ma mocniejsze fundamenty.

Jakub Sobek

Linc Polska

Świadomość zagrożeń

Zabezpieczenie techniczne infrastruktury krytycznej jest tematem na tyle złożonym, że bez dobrego planu i schematu działania praktycznie trudno zrealizować to zadanie dobrze. Nie można patrzeć na dany obiekt przez pryzmat tylko jednego, wybranego problemu i od niego rozpoczynać tworzenie globalnej koncepcji ochrony. Tak samo nie można zaczynać od wyboru konkretnego produktu i do niego dobudowywać pozostałe elementy systemu.

Często brak sprecyzowanych wymagań po stronie użytkownika końcowego sprawia, że kryterium cenowe staje się pretekstem do opracowania wymagań stawianych przed danym systemem. Takie podejście jest zazwyczaj także pewną wymówką przed przygotowaniem bardziej przemyślanej koncepcji. W efekcie tworzony system nie jest zgodny z zasadami sztuki, dobrymi praktykami ani obowiązującymi standardami.

Zagrożenia dla infrastruktury krytycznej ciągle się zmieniają i na początku należy postawić sobie zasadnicze pytanie, czy jestem świadomy wszystkich zagrożeń. Podstawowym, często popełnianym błędem jest uwzględnianie tylko tych zagrożeń, które wcześniej wystąpiły lub które udało się nam zaobserwować. O wielu atakach i zagrożeniach jednak nie wiemy dopóty, dopóki nie zaczniemy ich monitorować. Tak jest m.in. w przypadku ataków w cyberprzestrzeni. Jeśli jakiegoś fragmentu naszej sieci i infrastruktury nie monitorujemy pod kątem określonych zagrożeń, to teoretycznie zakładamy, że one się nie pojawią. To jednak kardynalny błąd logiczny.

Kolejnym nowym zagrożeniem, jakie może wystąpić w obszarze zabezpieczenia infrastruktury krytycznej, są nadlatujące nad obiekty drony. Świadomość tego zagrożenia jest znikoma. Nawet jeśli uda się zaobserwować pojedyncze przeloty dronów nad obiektami, nadal często uznajemy ten problem za marginalny. Dopiero gdy na terenie obiektu uruchomimy specjalistyczny radar pozwalający na monitorowanie nieba, uświadamiamy sobie, o jak wielu incydentach nie wiedzieliśmy. Właśnie dlatego, że wcześniej obszar ten nie był monitorowany.

Od czego zatem powinniśmy zacząć tworzenie koncepcji systemu zabezpieczenia technicznego? Przede wszystkim od postawienia sobie kilku podstawowych pytań. Co może się wydarzyć w obiekcie i czy na pewno jestem świadomy wszystkich zagrożeń? Jakich zagrożeń nie monitoruję i czy zatem mogę mieć pewność, że one nie występują? Jak oceniam ryzyko potencjalnych zagrożeń? W jakim celu chcę stworzyć systemem zabezpieczeń? Jak złożony ma być system i jak ma być zrealizowana jego integracja oraz kto za nią będzie odpowiadał? Wszystkie własne oceny dobrze byłoby poddać weryfikacji przez podmioty zewnętrzne, które pomogą w zrealizowaniu kompleksowego audytu bezpieczeństwa. Pozwala to na porównanie własnych wizji i wyobrażeń z chłodną i obiektywną oceną osób z zewnątrz.

Marcin Walczuk

BCS

Sprawny system bezpieczeństwa

W codziennym życiu, mając dostęp do wszelkich udogodnień nowoczesnego świata, najczęściej nie zdajemy sobie nawet sprawy z istnienia infrastruktury krytycznej, nie mówiąc już o tym, jak wiele systemów wchodzi w jej skład. Wystarczy jednak, że z powodu awarii sieci komórkowej stracimy dostęp do Internetu w smartfonie, a płatność telefonem lub wypłata gotówki bez karty płatniczej będą niemożliwe. A gdybyśmy

długotrwale stracili dostęp do usług znacznie ważniejszych, takich jak energia elektryczna, woda pitna, środki komunikacji i transportu czy wszelkiego rodzaju metody łączności?
Aby uniknąć wybuchu paniki i destabilizacji wewnętrznej kraju, jednym z priorytetów, jakie stawia przed sobą państwo, jest zapewnienie bezpieczeństwa i odpowiedniego poziomu ochrony wszystkich systemów wchodzących w skład infrastruktury krytycznej. Tego typu struktury w dużej mierze należą do sektora prywatnego i to w jego interesie leży tworzenie odpowiednich mechanizmów i procedur bezpieczeństwa, które sprostają potrzebom zabezpieczenia danej gałęzi infrastruktury krytycznej.
Ważną w tym rolę odgrywają producenci i dostawcy rozwiązań związanych z szeroko pojętą branżą security. I nie chodzi tylko o zabezpieczenia techniczne. Do obsługi wszystkich systemów zabezpieczeń potrzebny jest wykwalifikowany operator, a także pracownicy ochrony fizycznej, którzy niejednokrotnie stanowią pierwszą linię reagowania na pojawiające się zagrożenia.
Dopiero połączenie wszystkich tych elementów pozwoli na stworzenie sprawnie działającego systemu bezpieczeństwa, który nie tylko będzie reagować na już powstałe zagrożenia, ale też, a może przede wszystkim zawczasu wyeliminuje sytuacje niebezpieczne dla ciągłości działania stacji uzdatniania wody i wodociągów, elektrowni i linii przesyłowych, gazociągów czy szpitali lub budynków administracji publicznej. Nie wolno zapominać, że zachowanie wspomnianej ciągłości jest konieczne w czasie całego okresu użytkowania danego systemu. Stąd niezmiernie istotne są odpowiednia konserwacja i serwisowanie, co oczywiście leży po stronie dostawcy danego rozwiązania technicznego.
BCS, jako wiodący producent urządzeń i rozwiązań z zakresu telewizji dozorowej, dokłada wszelkich starań, aby proponowane produkty były przede wszystkim niezawodne oraz oferowały najnowocześniejsze rozwiązania techniczne. Zastosowanie rejestratorów i kamer z funkcjami zaawansowanej analizy obrazu pozwoli na dokładniejsze określenie charakteru wykrywanych zagrożeń, minimalizując w ten sposób liczbę fałszywych alarmów, co z kolei powinno się przełożyć na efektywniejszą pracę działu bezpieczeństwa danego obiektu.
Możliwość integracji naszych urządzeń z rozwiązaniami innych producentów pozwoli w łatwy sposób wdrożyć proponowane rozwiązania do istniejących już instalacji lub w oparciu o nie tworzyć nowe struktury zabezpieczeń.

Wieloletnie zaniechania i pozorne oszczędności skutkowały obniżeniem poziomu bezpieczeństwa obiektów IK. Pozornym rozwiązaniem problemu było wykorzystanie ochrony fizycznej.

Tomasz Goljaszewski

Hikvision Poland

Bezpieczeństwo obiektów infrastruktury krytycznej

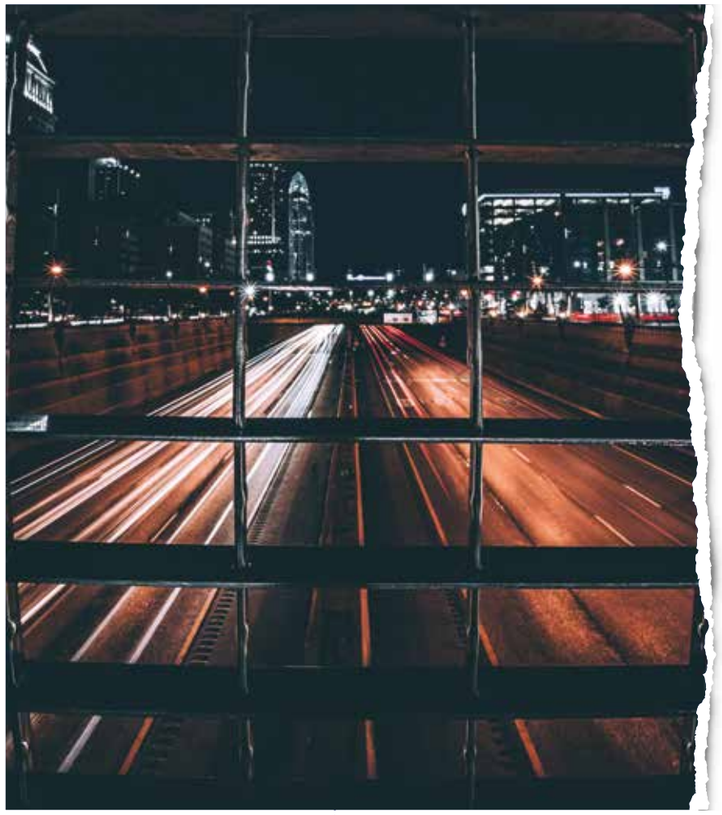
Nakłady ponoszone na ochronę infrastruktury krytycznej w Polsce są ciągle niskie w stosunku do jej znaczenia. Infrastruktura krytyczna to obiekty, systemy czy instalacje o strategicznym znaczeniu dla funkcjonowania społeczeństwa i państwa. Na przestrzeni lat, w okresie gorszej koniunktury gospodarczej, namnożyły się wieloletnie zaniechania i pozorne oszczędności, które skutkowały obniżeniem poziomu bezpieczeństwa tych obiektów – rozwiązaniem problemu było wykorzystanie ochrony fizycznej. Jednak ochrona fizyczna pozbawiona dobrych narzędzi wczesnego wykrywania zagrożenia oraz systemu powiadamiania nie jest w stanie skutecznie i odpowiednio szybko reagować.
Wraz ze wzrostem świadomości zagrożeń coraz częściej mówi się o znaczącym podniesieniu poziomu bezpieczeństwa obiektów infrastruktury krytycznej. Jak wiemy, system CCTV jest kluczowym elementem technicznego systemu zabezpieczeń ważnych obiektów. I tu pojawia się rola firmy Hikvision. Rozwój systemów i produktów w branży CCTV, a w szczególności w ofercie Hikvision nadąża za stale rosnącymi oczekiwaniami klientów w kierunku zwiększania poziomu bezpieczeństwa.
Nasza firma w ciągu kilku ostatnich lat bardzo rozwinęła dwie unikatowe technologie związane z jakością obserwacji w nocy: technologię DarkFigther opartą na dużym przetworniku obrazu o specjalnej światłoczułej konstrukcji oraz technologię DarkFighterX opartą na rozwiązaniu dwuprzetwornikowym – jeden przetwornik odpowiada wyłącznie za rozpoznanie kształtów, drugi za rozpoznanie kolorów. Obie technologie zapewniają bardzo dobrej jakości obraz w warunkach nocnych, przy minimalnym poziomie oświetlenia (np. światło gwiazd), przy czym technologia DarkFighterX koncentruje się przede wszystkim na odwzorowaniu obrazu w kolorze. Nowością w tym roku są kamery w technologii DarkFighter 4 Mpix i 8 Mpix.
W ochronie perymetrycznej obiektów IK nie powinno też zabraknąć kamer termowizyjnych z zaawansowaną analizą wizji. Firma Hikvision oferuje pełną gamę kamer termowizyjnych w rozdzielczościach CIF, 4CIF i 1 Mpix (poprzez cyfrowe przeskalowanie). Mają one prędkość wyświetlania do 50 kl./s, co jest istotne dla skuteczności działania algorytmów analizy wizji.
Pod koniec ubiegłego roku nasza firma opracowała też nowy firmware do kamer termowizyjnych rozpoznający automatycznie w obrazie powstanie pożaru oraz ingerencję w chronioną strefę człowieka lub pojazdu. Taka funkcjonalność skutecznie podnosi wykrywalność niebezpiecznych zdarzeń oraz ogranicza lub eliminuje fałszywe alarmy. Jest to możliwe dzięki nowej technologii *Deep Learning*. Technologia ta uczy się i tworzy różne wzorce rozpoznawanych obiektów czy zdarzeń. Wparcie przez *Deep Learning* mamy również w nowych kamerach linii 7. oraz systemach rejestracji Hikvision. Urządzenia te mają algorytmy analizy wzorców i potrafią filtrować alarmy pod kątem wykrycia człowieka czy pojazdu. Istotne jest to, że taka detekcja człowieka wynika nie z określenia wielkości obiektu czy prędkości jego poruszania się (co jest najczęściej spotykane i niestety mało skuteczne), ale właśnie poprzez rozpoznawanie wzorca.
Firma Hikvision opracowała również nową, w pełni profesjonalną platformę klient-serwer HikCentral, która skutecznie scentralizuje w jeden system wszystkie obiekty IK na bardzo dużym obszarze, ponieważ oprogramowanie to umożliwia zarządzanie niemal nieograniczoną liczbą lokalnych systemów.

Bogumił Szymanek

Axis Communications

Zintegrowane zabezpieczenie przed wtargnięciami

Aby zabezpieczyć obiekty przed wtargnięciem intruzów, należy chronić cały teren – od ogrodzenia po wnętrze budynków. Rozwiązania Axis przeznaczone do ochrony infrastruktury o kluczowym znaczeniu umożliwiają uporanie się – za pomocą jednego efektywnego kosztowo systemu – z takimi głównymi zagrożeniami, jak wtargnięcia intruzów, przerwanie pracy czy urazy pracowników. Obejmują one bogate portfolio sieciowych kamer, urządzeń kontroli dostępu i systemów audio, a wszystko to działające w ramach aplikacji Axis Perimeter Defender.
Zarejestrowany materiał bez analizy obrazu ma jednak niewielką wartość, bo takie rozwiązania wymagają żmudnego wyszukiwania niezbędnych informacji i są nieefektywne. Nasze rozwiązania obejmują zaawansowane funkcje analizy materiału wizyjnego, które przetwarzają i pomagają zrozumieć zgromadzone dane i obrazy. Dane analityczne wspierają podejmowanie właściwych decyzji.
Z kolei analiza zawartości obrazu na żywo skutecznie wspiera operatorów w ich reakcji na zdarzenia, co znacząco zmniejsza koszty obsługi fałszywych alarmów. Co więcej, wbudowane funkcje analizy umożliwiają gromadzenie danych w celu przewidywania długoterminowych trendów i planowania konserwacji.
Dzięki takiemu zintegrowanemu systemowi można nie tylko zabezpieczyć obiekt, ale także poprawić poziom bezpieczeństwa i zadbać o zdrowie pracowników. Można się upewnić, czy personel prawidłowo stosuje środki ochrony indywidualnej, np. kaski. Rozwiązanie umożliwia ponadto efektywne zarządzanie sytuacjami kryzysowymi, takimi jak ewakuacja, w bardziej elastyczny sposób.
Rozwiązania oferowane przez Axis są przyszłościowe i skalowalne, można je łatwo zintegrować z innymi systemami. Co ważne, umożliwiają one zdalne monitorowanie wielu obiektów z jednej sterowni. □



Jednym z priorytetów, jakie stawia przed sobą państwo, jest zapewnienie bezpieczeństwa i odpowiedniego poziomu ochrony wszystkich systemów wchodzących w skład infrastruktury krytycznej.

Co nowego w kontroli dostępu

Użytkownicy oczekują większej wygody i poczucia bezpieczeństwa, dlatego zastosowanie nowych technologii na rynku kontroli dostępu powinno rosnąć.

Jak wynika z badania przeprowadzonego przez firmę Memoori, światowy rynek produktów kontroli dostępu w 2018 r. powiększył się o 8 proc., osiągając sprzedaż na poziomie 7,5 mld USD. Miały w tym udział produkty sieciowe, kontrola dostępu jako usługa (ACaaS), czytniki biometryczne i narzędzia do zarządzania uprawnieniami. Analitycy spodziewają się dalszego wzrostu związanego z integracją innych systemów bezpieczeństwa fizycznego oraz systemów automatyki budynkowej (BAS).

TEKST
Eifeh Strom
a&s International

Zamki bezprzewodowe i systemy oparte na potwierdzaniu tożsamości coraz popularniejsze

Od szerszego wykorzystania zamków bezprzewodowych po integrację uwierzytelniania i zarządzania dostępem – przedstawiciele branży kontroli dostępu komentują obecne trendy na rynku.

Tempo, w jakim rynek kontroli dostępu dostosowuje się do najnowszych trendów technologicznych, nie jest duże. Jednym z powodów wolniejszego wprowadzania innowacji jest to, że firmy nie aktualizują systemów kontroli dostępu (KD) tak regularnie, jak inne rozwiązania, np. telefony komórkowe. Tradycyjna kontrola dostępu pozostaje nawet 10 lat w tyle za innymi sektorami.
Na szczęście rośnie obecnie świadomość korzyści związanych z bezpieczeństwem i zainteresowanie nowszymi technologiami dostosowanymi do zaostrzonych przepisów. W ciągu roku czy półtora użytkownicy powinni mieć już pełną świadomość poważnego ryzyka związanego z użytkowaniem starszych platform, w tym kart zbliżeniowych lub Mifare CSN w krytycznych lokalizacjach. Zaakceptują wtedy konieczność aktualizacji technologii w celu tworzenia bezpiecznego środowiska.

W tym roku można oczekiwać sporego wzrostu wykorzystania zamków bezprzewodowych. Tego typu zamek to nie tylko połączenie czytnika i blokady w jednym urządzeniu. Jego montaż jest dużo łatwiejszy i tańszy, ponieważ nie wymaga położenia dodatkowego okablowania. Przykładem jest sektor hotelarski od kilku lat podążający w tym kierunku. Branże komercyjne i przemysłowe również szybko nadrabiają dystans. Bezprzewodowe zamki to także sposób na szybkie tworzenie tymczasowych środowisk KD, które równie łatwo można zdemontować lub przenieść do innej lokalizacji.
Większe znaczenie będzie też miała KD oparta na tożsamości użytkownika w jego interakcjach w sferze zarówno fizycznej, jak i cyfrowej. Przyszłość będzie należała do kompleksowych platform kontroli dostępu, które – zamiast pojedynczo analizować każdą transakcję dostępu w środowisku, gdzie poszczególne systemy kontroli dostępu opierają się na odmiennych systemach autoryzacji – pobierają do identyfikacji dane z różnych systemów tożsamości (AD dla aplikacji firmowych, bazy danych fizycznego dostępu i biometryczne itp.) i podejmują „inteligentne" decyzje oparte na globalnej polityce dostępu. Wykorzystują przy tym zarówno fizyczne, jak i cyfrowe informacje kontekstowe.
Należy się również spodziewać, że w ciągu najbliższych kilku lat przyspieszy integrowanie uwierzytelniania i zarządzania dostępem ze względu na konieczność ograniczania ryzyka, a także zmniejszania obciążeń użytkowników końcowych, którzy muszą logować się do wielu aplikacji. Wynika to z ciągłej potrzeby zapewnienia bezpiecznego dostępu na poziomie aplikacji ze względu na stale rosnący obszar i poziom zagrożeń. Powiększanie się obszaru zagrożeń wynika z większego wykorzystania chmury i Internetu. Z kolei o tym, że poziom zagrożeń rośnie, świadczą przykłady naruszeń bezpieczeństwa ujawnione w ciągu ostatnich kilku lat i ich konsekwencje.
Można też wymienić inne trendy: ciągły rozwój rozwiązań sieciowych opartych na IP, stanowiących wyzwanie dla tradycyjnej architektury wykorzystującej łącza RS-485; zwiększające się zapotrzebowanie na rozwiązania hosto-

wane w chmurze kosztem tradycyjnych rozwiązań wdrażanych lokalnie; coraz większą inteligencję w urządzeniach brzegowych – za sprawą postępu w zarządzaniu mocą obliczeniową i tańszych platform obliczeniowych; mobilny dostęp oraz jego zdolność do dalszej konwergencji bezpieczeństwa fizycznego i logicznego; zastosowania zaawansowanego uczenia maszynowego i sztucznej inteligencji; wzrost znaczenia biometrii.

Dostęp mobilny zastępuje uwierzytelnianie oparte na kartach

Choć autoryzacja przy użyciu karty stanowi od dawna jeden z filarów branży kontroli dostępu, to użytkownicy końcowi oczekują metod bezpieczniejszych i wygodniejszymi. Jedną z technologii mających być odpowiedzią na ich żądania jest dostęp mobilny.

Przedstawiciele branży są zgodni: dostęp mobilny znajdzie się w tym roku w centrum uwagi. Do komunikacji z czytnikami coraz częściej będą wykorzystywane takie technologie, jak Bluetooth i PIR, a użytkownik uzyska dostęp już po machnięciu ręką w pobliżu czytnika, bez wyciągania telefonu z kieszeni. Firma analityczna IHS Markit przewiduje spore wzrosty na rynku dostępu mobilnego w ciągu najbliższych pięciu lat. Z jej raportu wynika, że średnia roczna stopa wzrostu w tym segmencie wyniesie w latach 2017-2022 ponad 100 proc. Przewiduje się też, że do 2022 r. ok. 20 proc. już zainstalowanych czytników kontroli dostępu będzie zdolnych do obsługi mobilnej.

Na niektórych rynkach komercyjnych, przemysłowych i nieruchomości będą nadal używane karty jako element autoryzacji wieloelementowej, ale będzie też widoczny trend odchodzenia od kart na rzecz wykorzystania smartfonów jako głównego narzędzia uwierzytelniania. Dzisiaj dostęp mobilny jest już nie tylko kolejną ciekawostką, ale także zyskuje uznanie ze względu na wygodę i dodatkowe bezpieczeństwo. Urządzenia mobilne przynoszą niezaprzeczalne korzyści, takie jak możliwość wykorzystania w wielu lokalizacjach oraz zdalnego poświadczania danych przez Internet. To wielka zaleta dla klienta w administrowaniu – pozbywa się drukowania kart, katalogowania ich i dbania o to, by znajdowały się we właściwych rękach. Gdyby smartfony stały się głównym narzędziem identyfikowania i uwierzytelniania użytkowników, a także inicjowania żądań dostępu (fizycznego lub cyfrowego), to łatwiejsze stałoby się tworzenie globalnych polityk dostępu i podejmowanie decyzji dotyczących dostępu na podstawie całościowej interakcji użytkownika.

Coraz więcej klientów pyta też o aplikacje mobilne, w których system kontroli dostępu wysyła w trybie *push* na telefon komórkowy przekaz wideo do weryfikacji.

Powszechność smartfonów daje wyraźną przewagę nad kartami dostępu. Zastanówmy się, ile osób zawraca, gdy w drodze do pracy stwierdzi, że kartę dostępu zostawili w domu? Praktycznie nikt. Jednak większość wróci po pozostawiony telefon komórkowy – ludzie używają smartfonów do płacenia za towary, przechowywania biletów do kina czy rezerwacji w restauracji. Dlaczego więc nie wyposażyć go w funkcjonalność otwierającą im drzwi, do których uzyskali dostęp, tym bardziej że coraz więcej użytkowników końcowych oczekuje sposobu na połączenie telefonów komórkowych z pewnymi poziomami dostępu w swojej organizacji. W dzisiejszym świecie smartfon jest stałym elementem, więc naturalne jest to, że firmy postrzegają go jako narzędzie integrujące dostęp mobilny w biurach na różnych poziomach.

Technologie dostępu mobilnego są już na większą skalę stosowane w sektorze ***smart home*** i, jak pokazują badania, także niektóre duże organizacje mające wielu użytkowników kupują nowe czytniki dostosowane do obsługi identyfikatorów mobilnych. Z szacunków wynika, że takie czytniki mogą do 2020 r. stanowić 10 proc. sprzedaży w tej kategorii urządzeń.

Telefon komórkowy jest również używany do kontroli dostępu w sposób wykraczający poza otwarcie drzwi. Działy bezpieczeństwa wykorzystują rozwiązania mobilne do zdalnego monitorowania, ustawiania alarmów i wprowadzania danych nowych pracowników do systemów. Rozwiązania mobilne oddają w nasze ręce większą kontrolę funkcjonalną nad systemem, który jest opracowywany i wdrażany, a cel funkcjonalny jest akceptowany i dostosowywany. Takie wdrożenia pojawiają się na uczelniach i w różnych sektorach gospodarki, zwłaszcza tam, gdzie są obiekty zdalne, np. na rynku energetycznym i mediów użytkowych.

Zalety i wady dostępu mobilnego

Wykorzystanie dostępu mobilnego ma się zwiększać w tym roku i kolejnych latach. Dlatego warto przyjrzeć się zarówno korzyściom, jak i wyzwaniom, które należy uwzględniać przy wdrażaniu tego rodzaju rozwiązań.

Wygoda jest jednym z podstawowych powodów postępującej konwersji dostępu mobilnego. W przypadku tradycyjnego rozwiązania dochodzi też problem odpadów, zwłaszcza gdy stosuje się wiele kart, np. w środowisku hotelowym. Inne korzyści to niemal natychmiastowa autoryzacja, szybszy i wygodniejszy dostęp oraz mniejszy całkowity koszt posiadania (TCO) w autoryzacji wieloelementowej.

Sposób uwierzytelniania został udoskonalony, zmalały koszty czytników. W rezultacie coraz więcej firm jest skłonne rozważyć dostęp mobilny w kontekście realizacji nowych projektów. Dostęp mobilny jest wygodny, ale należy wziąć pod uwagę to, czy dane zapisywane w logach będą przechowywane na urządzeniu mobilnym, czy na serwerze w chmurze. Koszt wdrożenia wirtualnego uwierzytelniania w porównaniu z tradycyjnymi kartami fizycznymi także trzeba mieć na względzie. W przypadku rozwiązań niektórych dostawców taka inwestycja może być znacząca.

Żeby dostęp mobilny mógł skutecznie wyprzeć istniejące czytniki kart i czytniki zbliżeniowe, szybkość i pojemność czytników dostępu mobilnego musi być co najmniej na poziomie zastępowanych urządzeń. Jednym z wyzwań w środowisku biurowym jest to, że nadal wymaga się tam od personelu posiadania fizycznego identyfikatora ze zdjęciem, który odróżnia pracowników od gości i kontrahentów. Mimo to dostęp mobilny i w tym scenariuszu wciąż ma wyraźną przewagę – jest wygodny i bezpieczniejszy (smartfony są zwykle chronione hasłem).

Kolejnym wyzwaniem jest duża liczba różnych platform, na których są tworzone te programy. Nie każdy używa tego samego typu smartfonu. Trzeba też sobie poradzić z gośćmi i podwykonawcami, którzy mogą wymagać krótko- lub długoterminowego dostępu do obiektu. Konieczne jest także rozwiązanie problemów dotyczących prywatności, np. jeśli pracownik ma korzystać z osobistego telefonu w celu uwierzytelniania się, to jaki dostęp do tego urządzenia mógłby uzyskać pracodawca. Dochodzą również kwestie związane z cyberbezpieczeństwem. Granica pomiędzy użyciem telefonów komórkowych w celach zawodowych i prywatnych coraz bardziej się zaciera. Z tego powodu urządzenia przenośne stają się dla cyberprzestępców bardzo atrakcyjnym celem ataku. Ze wszystkimi takimi wyzwaniami trzeba sobie poradzić, zanim firma będzie mogła wdrożyć tego rodzaju rozwiązania.

Użytkownicy powinni być świadomi zagrożeń i ostrożni, jeśli chodzi o instalowanie aplikacji, a firmy powinny przeznaczyć więcej zasobów na ochronę punktów końcowych i zabezpieczanie dostępu w kontekście urządzeń mobilnych. Dlatego też na znaczeniu będą zyskiwać mechanizmy bezpieczeństwa utrzymujące wysoki poziom zaufania, przy założeniu że telefon komórkowy jest urządzeniem nie w pełni bezpiecznym (podejście *zero trust*).

Kolejne problemy wiążą się z ograniczonym czasem pracy baterii telefonu, tym bardziej że większość opartych na łączności Bluetooth rozwiązań dostępu mobilnego będzie wymagała, aby ta funkcjonalność była przez cały czas włączona.

Postępująca integracja systemów VSS i KD

Użytkownicy końcowi poszukują bezproblemowo działających rozwiązań obejmujących różne funkcjonalności na pojedynczej platformie. Dlatego można się spodziewać dalszego integrowania systemów dozoru wizyjnego (VSS) z systemami kontroli dostępu.

Integracja systemów VSS z kontrolą dostępu trwa od lat. Producenci systemów KD twierdzą, że będzie kontynuowana w ramach szerszego trendu integracji. Integracja będzie miała kluczowe znaczenie zarówno dla producentów KD, jak i komponentów dozoru wizyjnego, takich jak kamery i systemy zarządzania. Producenci, którzy uczynią z integracji kluczowy element swojej oferty, będą odnosić większe sukcesy niż ci, którzy tego nie zrobią.

Każdy podmiot dysponujący centrum NoC lub SoC natychmiast odczuje korzyści wynikające z połączenia wszystkich krytycznych funkcjonalności na zunifikowanej platformie – dozoru wizyjnego, kontroli dostępu, systemów zabezpieczeń i dwukierunkowej komunikacji. Wyższy poziom integracji zapewnia bezpieczeństwo i zarządzanie operacyjne oraz pełną świadomość sytuacyjną, dzięki czemu można np. koordynować działania osób niosących pierwszą pomoc czy tych, które są chronione, dostarczając im informacje niezbędne w sytuacjach wyjątkowych. Specjaliści coraz częściej są zainteresowani wyższym poziomem integracji systemowej pozwalającej na konsolidowanie operacji i łączenie odrębnych wcześniej możliwości systemowych w ramach platformy zunifikowanej.

Obraz z kamery to prosty sposób wizualnej weryfikacji zdarzenia kontroli dostępu, kontrola dostępu natomiast dostarcza dodatkowych danych, które można wykorzystać w dochodzeniu opartym na dozorze wizyjnym. Zakres integracji zależy od tego, w jaki sposób użytkownik końcowy wykorzystuje swój system. Jednak w sytuacji, gdy kamery znajdują się w pobliżu punktów kontroli dostępu, brak integracji byłby marnotrawstwem w inwestycji. Zarówno zarejestrowane obrazy, jaki i przekaz na żywo wciąż będą miały dużą wartość, popularność zaczną zyskiwać rozwiązania, wykorzystujące obraz do poprawy bezpieczeństwa, np. rozpoznawanie twarzy w strumieniu wizji.

Rozwiązania oferujące zarówno kontrolę dostępu, jak i zarządzanie wizją realizowane w chmurze są – ze względu na cenę i wybór usług – wybierane przez małe i średnie przedsiębiorstwa. Wśród innych sektorów, które mogą skorzystać na integracji, są te, dla których obraz jest kluczowym elementem kontroli dostępu. Należą do nich ochrona zdrowia, edukacja, usługi finansowe, szkolnictwo wyższe, kasyna czy hotelarstwo.

Można się też spotkać ze zdaniem przeciwnym, np. że integracja VSS z KD jest bardziej efektem działań chcących się wyróżnić producentów i dostawców niż wynikiem potrzeb i oczekiwań rynku. Nie jest ona konieczna w każdej aplikacji i powinna ograniczyć się jedynie do przypadków indy-

widualnych. Integracja dozoru wizyjnego może nie być ani praktyczna, ani opłacalna, gdy np. wymagałaby dużo większej liczby operatorów monitorujących obrazy przy ogromnej przepustowości systemu kontroli dostępu. Przykładem są szpitale i edukacja – miesięcznie milion otwarć drzwi!

Bezkontaktowy dostęp na podstawie cech biometrycznych

Wykorzystanie biometrii w systemach kontroli dostępu to od dawna ważny trend. Teraz w centrum uwagi są technologie bezkontaktowe.

W najbliższym czasie na rynku kontroli dostępu można się spodziewać wzrostu udziału bezkontaktowej identyfikacji na podstawie cech biometrycznych, przede wszystkim dzięki dokładniejszym i bardziej zaawansowanym technologiom. Według raportu Markets and Markets światowy rynek systemów biometrycznych ma do 2023 r. osiągnąć wartość 41,8 mld USD. Sprzedaż będzie się zwiększać co roku średnio o 20 proc. (CAGR).

Podobnie jak analityka, która od ponad dekady próbuje stać się sprzedażowym hitem – biometria wciąż czeka na swój wielki moment w kontroli dostępu. Postęp technologiczny, w którego wyniku obniżyły się koszty i poprawiła wydajność praktycznie wszystkich metod biometrycznych, znacząco przybliżyły jego nadejście. Do zwiększonego wdrażania rozwiązań biometrycznych przyczyni się powszechna akceptacja użytkowników dla wykorzystania biometrii w smartfonach przy logicznej kontroli dostępu i płatnościach elektronicznych.

Stworzenie systemu kontroli dostępu, który nie wymagałby szczególnej współpracy użytkownika, od dawna było piętą achillesową bezkontaktowych systemów biometrycznych. Dzieje się tak, gdyż te rozwiązania zazwyczaj wymagają, aby obiekt znalazł się w ściśle określonym miejscu, zanim system go rozpozna i uwierzytelni. Ponieważ są już technologie, które potrafią rozpoznać tęczówkę oka lub twarz widziane pod różnymi kątami, ta bariera wydaje się do pokonania. W połączeniu z systemami tak zaprojektowanymi, by zapobiegać wejściu intruza z autoryzowaną osobą, technologia ta może zrewolucjonizować punkty kontrolne.

Niedawno firma Gemalto zapowiedziała wspólny pilotażowy program ze znaną linią lotniczą, dotyczący wdrażania biometrycznego boardingu pasażerów na pokład samolotu. Test ma potwierdzić, czy w porównaniu z tradycyjną kartą pokładową rozpoznawanie twarzy odpowiada na potrzeby i oczekiwania pasażerów. Okaże się też, czy są spełnione wymogi amerykańskiej ochrony celnej i granicznej, agencji CBP (*Customs and Border Protection*).

Administracja i instytucje bezpieczeństwa publicznego przestaną być podstawowymi i niemal jedynymi inwestorami, którzy wykorzystują technologie biometryczne. Dojdą do nich edukacja i ochrona zdrowia, które w coraz większym stopniu będą wdrażać kontrolę dostępu. W obiektach ochrony zdrowia aplikacje przyczynią się do usprawnienia przepływu pracy (zwiększając efektywność pracy personelu i dostarczania wyników pacjentów), zachowania higieny dzięki implementacji bezkontaktowej, skuteczniejszego weryfikowania tożsamości przy uzyskiwaniu dostępu do informacji o pacjentach i innych danych. Biznes również powinien znacząco zwiększyć wykorzystanie biometrii w logicznej kontroli dostępu – wg prognoz nawet do 90 proc. w roku 2020.

Przykładem miejsc, gdzie bezstykowa biometryczna kontrola dostępu może być korzystna, są place budowy. W takim środowisku system rozpoznawania dłoni lub twarzy staje się wyjątkowo praktycznym rozwiązaniem dla pracowników. Posługiwanie się tokenem jest niewygodne, a odciski palców robotników mogą być trudne do odczytania z powodu warunków pracy. Kolejnym miejscem, w którym taki system świetnie by się sprawdził, są boiska sportowe i stadiony. Zawodnicy muszą uzyskać dostęp do strzeżonych stref, a najczęściej nie dysponują kieszeniami bądź torbami do noszenia identyfikatorów.

Kolejną bezstykową techniką biometryczną, która zaczyna zdobywać uznanie, jest identyfikacja oparta na głosie osoby. Ma o tym świadczyć dwucyfrowy wzrost wykorzystania asystentów głosowych. Uwierzytelnianie przy użyciu głosu może być pomostem między bezpieczeństwem fizycznym i cyfrowym oraz stanowić w razie potrzeby dodatkową warstwę ochrony.

Wciąż jednak istnieją poważne bariery wdrażania rozwiązań biometrycznych, głównie ze względu na ochronę danych osobowych od czasu wprowadzenie rozporządzenia RODO/GDPR. Ludzie są zaniepokojeni tym, że „robi się im zdjęcia", nie wiedząc „do czego potem mogą być wykorzystane". Wyjaśnienie, że system dokonuje pomiarów pewnych charakterystycznych punktów ich twarzy i dołącza je do algorytmicznego obrazu, nie ma dla nich znaczenia. Z tego samego powodu nie przyjęły się 20 lat temu skanery w bankomatach. Ostatecznie jednak, ze względu na wygodę użytkownika, trend ten będzie przybierać na sile, tym bardziej że technologie staną się doskonalsze, co – w połączeniu z edukowaniem konsumentów – pozwoli ograniczyć czynnik lęku.

Rozpoznanie twarzy przyspiesza rozwój biometrii bezkontaktowej

Postęp w rozpoznawaniu twarzy i większa akceptacja tej technologii przyczyniają się do wzrostu jej wykorzystania jako bezkontaktowej biometrycznej metody kontroli dostępu.

Choć technologia rozpoznawania twarzy na początku napotykała opór użytkowników, dziś cieszy się rosnącą popularnością i przeciera szlak zastosowaniom bezkontaktowej biometrycznej kontroli dostępu. Jej implementacja w najpopularniejszych na rynku smartfonach radykalnie poprawiła krzywą uczenia się. Szersza obecnie akceptacja w społeczeństwie jeszcze bardziej przyspieszy jej wdrażanie w większej liczbie aplikacji, w tym kontroli dostępu. Szacuje się, że światowy rynek rozpoznawania twarzy osiągnie do 2022 r. wartość prawie 7,8 mld USD, przy średniej rocznej stopie wzrostu (CAGR) 13,9 proc. (dane z raportu Markets and Markets). Wzrost przypisuje się zwiększonemu zapotrzebowaniu na dozór wizyjny i monitoring w miejscach publicznych oraz rosnącemu zastosowaniu tej technologii w administracji publicznej. Podobnie jak w przypadku uwierzytelniania mobilnego, użytkownicy szukają elastyczności. Czytnik biometryczny może ułatwić osiągnięcie tego celu, oferując jednocześnie dodatkową warstwę bezpieczeństwa w ochronie organizacji.

I choć stale pojawiają się kolejne nowe technologie, to najpopularniejsze systemy autoryzacji biometrycznej zwykle wykorzystują metody dobrze już znane i praktyczne, takie jak rozpoznawanie twarzy i tęczówki. W ostatnich kilku latach można zaobserwować szybki rozwój czytników twarzy. Zaczynają one wypierać czytniki linii papilarnych lub dłoni, ponieważ są wygodne i bezpieczne. Zwiększa się w nich pojemność wzorców twarzy, która może wynosić nawet 10 000, co umożliwia obsługę dużej liczby osób, wymaganą w niektórych zastosowaniach.

Technologia rozpoznawania twarzy została w znacznym stopniu udoskonalona i jest już dokładniejsza od rozpoznawania tęczówki. Przykładem skutecznej implementacji rozpoznawania twarzy – technologii pierwotnie opracowanej przez firmę Aurora Computer Services – może być kontrola paszportowa na lotniskach. Jednak nawet w tak ściśle kontrolowanych środowiskach wskaźnik „trafień" nie zawsze jest do zaakceptowania. Problem jest związany z ograniczeniami kamery, która zasięgiem nie jest w stanie objąć każdej osoby, np. o wzroście ponad 190 cm, gdyż trudno znaleźć kamerę ustawioną tak wysoko. Z kolei w przypadku osób na wózku kamera musiałaby być zamontowana poniżej 120 cm.

W regionie Azji i Pacyfiku oprogramowanie do rozpoznawania twarzy zdobywa rynek nie tylko jako narzędzie do bezkontaktowej biometrycznej kontroli dostępu, ale także do rozwijania możliwości analitycznych. Uwagę zwraca znaczny wzrost inwestycji związanych z rozpoznawaniem twarzy, zwłaszcza w Chinach. Dzieje się tak, ponieważ dostawcy uznają kombinację rozpoznawania twarzy i sztucznej inteligencji (AI) jako czynnik pobudzający rynek. Badania pokazują, że inwestycje typu venture capital w biometrię przekroczyły w ciągu ostatnich dwóch lat 4 mld USD – około połowy tej kwoty trafiło do chińskich firm zajmujących się rozpoznawaniem twarzy.

Więcej chmury i świadomości w obszarze cyberbezpieczeństwa

Gdy pamięć masowa w chmurze staje się coraz bardziej przystępna cenowo, migracja kontroli dostępu do tego środowiska powinna się zwiększyć.

Można się spodziewać większej akceptacji użytkowników dla realizowanych w chmurze kontroli dostępu i zarządzania wizją – branża wskazuje na rosnącą otwartość klientów na korzystanie z produktów chmurowych. Choć większość nadal zamierza inwestować w bardziej tradycyjne rozwiązania kontroli dostępu, to korzyści z chmury – np. krótszy czas instalacji, automatyczne aktualizacje oprogramowania, elastyczność i mobilność, zarządzane usługi oraz większe cyberbezpieczeństwo – kuszą użytkowników. Hostowana w chmurze kontrola dostępu stwarza resellerom nowe możliwości zarabiania, a wielu małym i średnim klientom daje szansę na ekonomiczne wdrożenie bardziej zaawansowanego rozwiązania. W rezultacie będziemy obserwować dalszą ewolucję opartej na chmurze oferty kontroli dostępu – z coraz większą liczbą funkcji i integracji.

Przeniesienie kontroli dostępu do chmury ma sens z wielu powodów, wśród których można wymienić łatwość zarządzania i większe bezpieczeństwo. Powstaje w ten sposób system o niemal nieskończonej skalowalności, nieobciążony wymogiem instalowania kolejnych paneli w środowisku lokalnym. Obecny stan to podejście hybrydowe, z chmurą jako mózgiem systemu i fizyczną lokalizacją w charakterze *backupu*. Producenci nadal przenoszą większość funkcjonalności systemu KD do urządzeń brzegowych (mostki i czytniki), ale to chmura może stać się atrakcyjniejszą opcją.

Analitycy z IHS Markit przewidują, że rynek kontroli dostępu jako usługi (ACaaS) do 2022 r. osiągnie wartość 950 mln USD. Skorzystają z niej przede wszystkim małe i średnie przedsiębiorstwa – w 2017 r. odpowiadały one za 21 proc. przychodów na tym rynku. Przeniesienie kontroli dostępu do chmury zapewnia użytkownikom końcowym większe bezpieczeństwo, bez konieczności inwestowania w kosztowną infrastrukturę informatyczną. Wygląda na to, że kontrola dostępu w formie usługi będzie solidnym i szybko rosnącym segmentem rynku w obszarze małych i średnich projektów (do 50 przejść kontrolowanych). Nie jest to bowiem jeszcze rozwiązanie, które sprawdzi się przy większych projektach.

Co ciekawe, w sytuacji, gdy kontrola dostępu jako usługa staje się nowym paradygmatem dla dostawców, powinni pojawiać się nowi graczy na rynku. Oznacza to większą konkurencję, więc interesująca będzie reakcja branży oraz to, jak dostawcy poradzą sobie z nowymi wyzwaniami.

Wobec spodziewanego przeniesienia kontroli dostępu do chmury i rosnącego wykorzystania rozwiązań opartych na protokole IP ważną kwestią staje się cyberbezpieczeństwo.

Większa świadomość cyberzagrożeń jest siłą napędową rozwoju technologicznego w obszarze kontroli dostępu, szczególnie w aspekcie wymogów RODO/GDPR, a częściowo także uwierzytelniania mobilnego. Zapewnienie cyberbezpieczeństwa jest dużym problemem widocznym już na coraz wyższym poziomie. Firmy międzynarodowe, korporacje czy tak specyficzne sektory jak bankowość i finanse chcą się stosować do rządowych regulacji, mając pewność, że wszystko co podłączone do ich sieci, nie będzie ułatwiać hakerom włamania przez systemy kontroli dostępu lub dozoru wizyjnego.

W przypadku Internetu Rzeczy (IoT) odporność na cyberzagrożenia można obecnie osiągnąć dzięki systemom spełniającym globalne standardy, takie jak brytyjski CAP (*Cyber Assurance Products*), amerykański FIPS czy australijski Type 1. Przykładowo w Wielkiej Brytanii tylko nieliczni z około 40 producentów mogą zaoferować taki poziom zgodności ze standardami oraz odporność na cyberataki. W przypadku małych i średnich przedsiębiorstw, w których poziom kompetencji i zasobów jest niższy, użytkownicy muszą być przekonani, że ich sieć jest odporna. Dlatego należy zadbać, by inwestycja w bezpieczeństwo była przyszłościowa i odporna na cyberzagrożenia.

Inteligentne budynki, chmura, technologie mobilne oraz Internet Rzeczy (IoT) to tylko niektóre kierunki rozwoju w świecie kontroli dostępu. Aby zapewnić sukces firmie, a tym samym jej wzrost, producenci rozwiązań kontroli dostępu muszą nadążać za innowacjami i zmieniającym się otoczeniem.

Światowe trendy w kontroli dostępu

Marcus Handels, Chief Technology & Innovation Oficer firmy SALTO Systems, ocenia zmiany mające znaczący wpływ na sektor kontroli dostępu.

CO JEST WYZNACZNIKIEM INTELIGENTNYCH BUDYNKÓW?

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

TECHNOLOGIA CLOUD JEST CORAZ POWSZECHNIEJSZA NA RYNKU KONTROLI DOSTĘPU. JAKIE SĄ JEJ ZALETY?

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

CO Z INTEGRACJĄ Z INNYMI APLIKACJAMI W CHMURZE OPRÓCZ KONTROLI DOSTĘPU?

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

TECHNOLOGIA MOBILNA ROZWIJA SIĘ NA RYNKU KONTROLI DOSTĘPU. CZY TO JUŻ WIDOCZNY TREND?

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

JAKIE ZALETY DLA UŻYTKOWNIKÓW WYNIKAJĄ ZE STOSOWANIA MOBILNEGO DOSTĘPU?

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

CZY KONTROLA DOSTĘPU W INTERNECIE RZECZY MA PRZYSZŁOŚĆ?

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

CZY SYSTEMY KONTROLI DOSTĘPU BĘDĄ ODGRYWAĆ ROLĘ W ROZWOJU INTELIGENTNEGO DOMU?

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

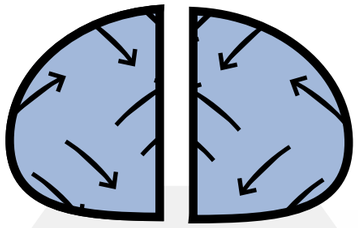
SALTO Systems Sp. z o.o.
Oddział w Polsce

ul. 17 Stycznia 45 A, Warszawa
tel. +48 609 017 777
info.pl@saltosystems.com
www.saltosystems.com

Znajdź odpowiednią kontrolę dostępu w 5 krokach

Firma Nedap Security Management opracowała jeden z pierwszych systemów kontroli dostępu opartych na oprogramowaniu – AEOS. Anna Twardowska, Country Manager Poland w Nedap, przedstawia najważniejsze kwestie, jakie należy uwzględnić przy wyborze systemu.

System kontroli dostępu to nie tylko ważna inwestycja długoterminowa, to także rozwiązanie, które odpowiednio dobrane zapewni pełen wachlarz korzyści komercyjnych. Zalecamy wdrażanie go krok po kroku.



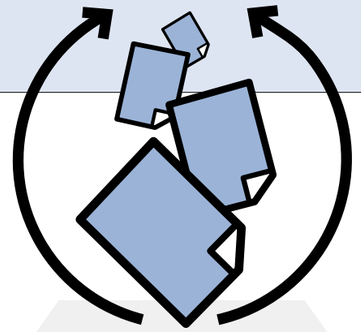
KROK 1.

PRZEPROWADŹ ANALIZĘ RYZYKA

System kontroli dostępu może chronić nie tylko aktywa i pracowników, ale także procesy biznesowe. Pierwszym krokiem w doborze odpowiedniego do potrzeb systemu jest rozpoznanie czynników ryzyka oraz określenie, które z nich stanowią największe zagrożenie.

Na tym etapie zastanów się:

- → co wymaga zabezpieczenia – czy chcesz chronić wrażliwe informacje lub urządzenia równie dobrze, jak ludzi i budynki;
- → które procesy będą miały wpływ na obroty firmy, gdyby doszło do ich naruszenia, np. produkcja lub logistyka;
- → jakich zagrożeń należy uniknąć i w jakim obszarze, np. włamania lub nieuprawnionego dostępu;
- → co należy zrobić, aby zminimalizować szkody, gdy dojdzie do takiej sytuacji.



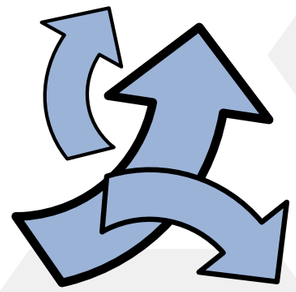
KROK 2.

PRZYJMIJ PERSPEKTYWĘ DŁUGOTERMINOWĄ

Wiele może się zmienić w kolejnych latach działania dobrego systemu kontroli dostępu. Zastanów się, jakie mogą być twoje długoterminowe potrzeby, aby dostosować do nich rozważany system i pomóc w maksymalizacji zwrotu z inwestycji.

Pomyśl np. o:

- → stosowaniu kart dostępu zamiast kluczy w celu zwiększenia bezpieczeństwa i umożliwienia sprawnej współpracy pomiędzy oddziałami firmy;
- → kierunku, w jakim mogą się w przyszłości zmienić przepisy i regulacje;
- → współpracy z innymi działami, np. HR, IT i administracji budynku, by uwzględnić ich sugestie dotyczące systemu kontroli dostępu;
- → nowych technologiach, np. biometrii, która jest coraz częściej stosowana w kontroli dostępu w celu weryfikacji tożsamości osób za pomocą ich cech fizycznych. Najpopularniejsze obecnie rozpoznają twarz, tęczówkę, odciski palców, geometrię ręki lub układ żył.



KROK 3.

ROZWAŻ DOSTĘPNE MOŻLIWOŚCI

Aby optymalnie wykorzystać inwestycję, oszacuj wszystkie korzyści oferowane przez dany system, oprócz samej funkcji kontroli dostępu.

Przykładowo dobry system kontroli dostępu stanowi cenną pomoc, zapewniając jednocześnie:

- → bardziej wydajne użytkowanie budynku lub innych przestrzeni,
- → optymalizację procesów biznesowych,
- → przyjazne przywitanie gości,
- → większą wygodę dla pracowników.

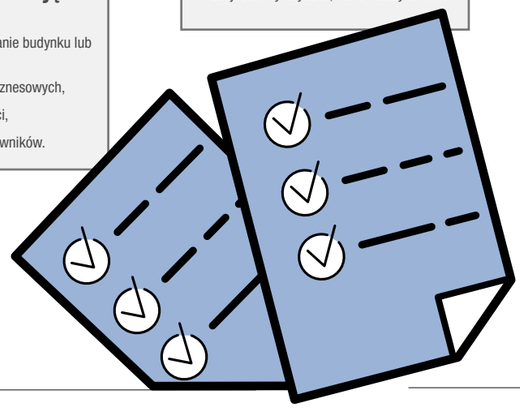
KROK 4.

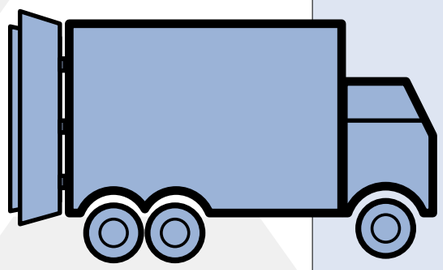
SPORZĄDŹ LISTĘ WYMAGAŃ

Po wykonaniu kroków 1., 2. i 3. dopilnuj, aby twoje potrzeby zostały jasno określone na liście wymagań dotyczących systemu kontroli dostępu.

Określ jak najdokładniej potrzeby:

- → wyjaśnij, dlaczego chcesz wymienić swój dotychczasowy system;
- → opisz zalety dotychczasowego systemu, z których nie chcesz zrezygnować;
- → sprecyzuj, czego oczekujesz od nowego systemu, oraz jakich problemów chcesz uniknąć;
- → określ, w jaki sposób system ma poprawić wydajność, produktywność, elastyczność i skalowalność, i w jaki sposób będziesz to mierzyć;
- → ustal, w jaki sposób użytkownicy mają korzystać z systemu, jakie zadania powinien wykonywać recepcjonista, kto będzie monitorować alarmy, w jaki sposób zarządca budynku będzie korzystać z raportów dotyczących dostępu;
- → określ szczególnie ważne dla twojej organizacji obiekty fizyczne, które należy chronić.





KROK 5.

ZNAJDŹ ODPOWIEDNIEGO DOSTAWCĘ

Mając już listę wymagań, możesz podzielić się nią z producentami, instalatorami oraz wdrożeniowcami. Każdy z nich zaproponuje coś innego. Producent może np. doradzić w kwestiach trendów technologicznych i zaproponować wybór rozwiązań odpowiadających Twoim potrzebom. Instalatorzy i wdrożeniowcy powinni zapewnić prawidłowe wdrożenie i utrzymanie systemu. Zastanów się, czego oczekujesz po współpracy z nimi. Weź pod uwagę to, czy wybrany system będzie, i na jakich warunkach, przez nich aktualizowany i usprawniany w przyszłości.

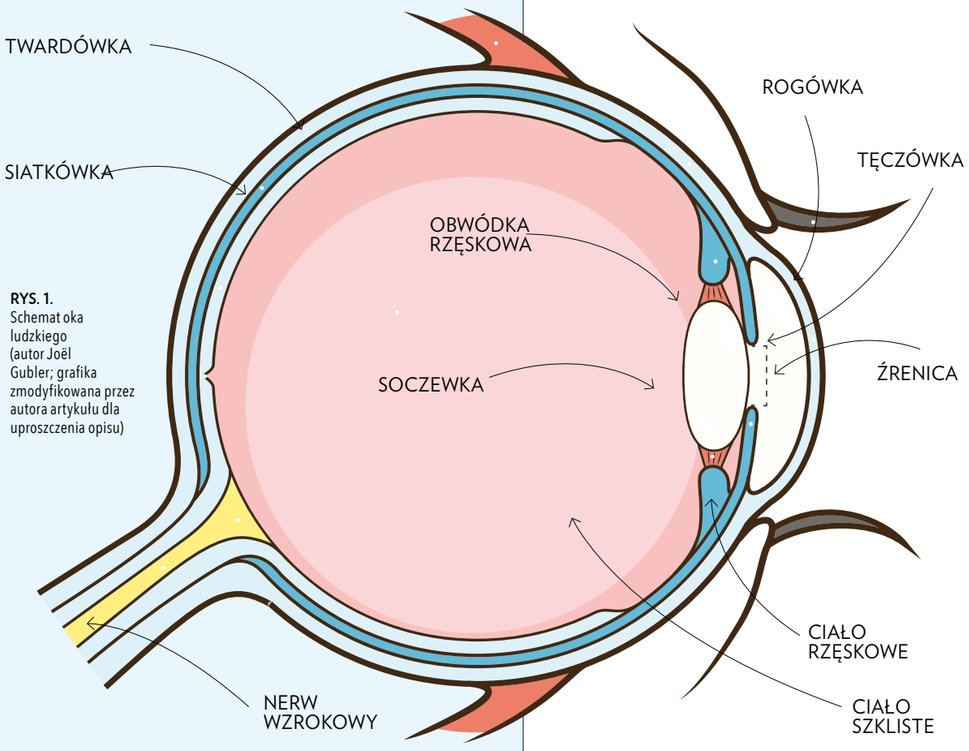
W firmie Nedap stale inwestujemy w badania i rozwój, aby użytkownicy AEOS mieli gwarancję, że system kontroli dostępu będzie dostosowany do określonego celu i aktualny bez okresu ważności. Takie działania w ostatnim czasie doprowadziły do modyfikacji i adaptacji 30% bazy kodów AEOS oraz ponownego napisania ponad 3 milionów wierszy kodu oprogramowania w celu osiągnięcia znacznego usprawnienia wydajności.

Weź również pod uwagę złożoność projektu systemu i instalacji oraz zastanów się, kto ma największe kompetencje, aby zarządzać całością. Oferujemy klientom program globalny, który pomaga firmom międzynarodowym w szybszym i łatwiejszym usprawnianiu kontroli dostępu. System wdrażania projektów zapewnia efektywną kosztowo i wydajną strukturę ramową, umożliwiającą standaryzację bezpieczeństwa we wszystkich obiektach firmy na całym świecie. To z kolei zapewnia większą elastyczność i skalowalność, umożliwiając powstawanie globalnego systemu kontroli dostępu przygotowanego na przyszłe wyzwania. Po wyborze dostawcy zdecydujcie wspólnie, w jaki sposób będzie określana sprawność systemu, aby można go było udoskonalać w kolejnych latach. □

Więcej informacji na temat korzyści oferowanych przez system kontroli dostępu Nedap znajduje się na stronie **www.nedapsecurity.com/pl**

Nedap Security Management

Al. Niepodległości 18,
02-653 Warszawa
www.nedapsecurity.com/pl



RYS. 1. Schemat oka ludzkiego (autor Joël Gubler; grafika zmodyfikowana przez autora artykułu dla uproszczenia opisu)

Optyka dla każdego

Część II

TEKST
Piotr Rogalewski

W artykule rozpoczynającym cykl omówiłem podstawowe pojęcia związane ze światłem. Wiedza ta przyda się nam w tej i kolejnych jego częściach. Dziś poznamy ogólnie działanie ludzkiego oka i soczewek oraz zjawisko dyfrakcji, a także podstawowe pojęcia z zakresu optyki geometrycznej.

Oko to bez wątpienia jedno z najbardziej niezwykłych osiągnięć natury. Ze swoją pojedynczą soczewką i w porównaniu z obecnymi zdobyczami techniki np. w dziedzinie rozdzielczości, czułości czy prędkości przetwarzania obrazu czasem wypada „blado" w bezpośrednich zestawieniach parametrów. Jednak dzięki niesamowitym zdolnościom naszego mózgu do generowania wizji w trzech wymiarach i do kompensacji niedoskonałości anatomicznych układu optycznego człowieka zestaw oko plus mózg można uznać za najlepszą kamerę na świecie.

Ale dlaczego warto znać szczegóły anatomiczne naszych naturalnych „kamer"? Odpowiedź nasuwa się sama: wiedza o tym, jak zbudowane jest oko, pozwala zrozumieć m.in. działanie przysłony obiektywu, a także to, dlaczego większość stosowanych obecnie technologii obrazowania elektronicznego opiera się na trzech kolorach składowych: czerwonym, zielonym i niebieskim (RGB). Z indywidualnych cech charakterystycznych budowy oka korzystają także niektóre biometryczne systemy identyfikacji i kontroli dostępu.

Budowę ludzkiego oka przedstawiono na *rys. 1*. Dla zachowania czytelności obrazu wiele elementów anatomicznych nie zostało tam uwzględnionych, są jedynie te, dla których można znaleźć analogię do urządzeń telewizji dozorowej. Pominę mechanizmy fizjologiczne działania oka, skupiając się na kwestiach najistotniejszych z punktu widzenia optyki. Dla ułatwienia w tabeli zestawiono elementy anatomiczne człowieka z odpowiadającymi im elementami kamer i układów optycznych.

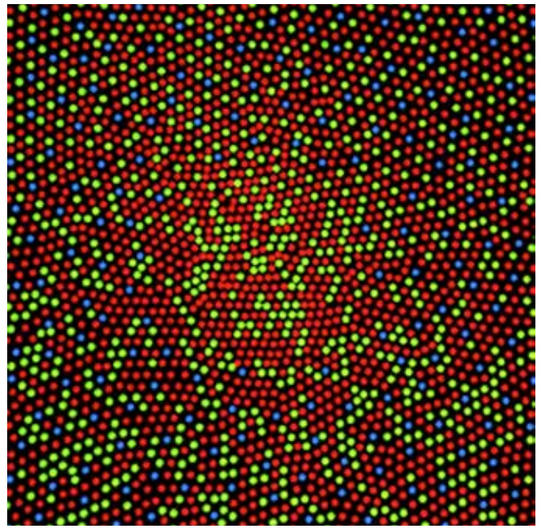
CZŁOWIEK	KAMERA PLUS OBIEKTYW
twardówka	obudowa obiektywu
tęczówka	przysłona
źrenica	otwór przysłony
soczewka i rogówka	soczewki
siatkówka	przetwornik CMOS lub CCD (dawniej analizująca lampa obrazowa)
nerw wzrokowy	linie sygnałowe: z przetwornika CCD/CMOS do przetwornika A/C
mięśnie rzęskowe	silnik ostrości
mózg	przetwornik A/C + procesor sygnałowy (DSP)

Rozważania zacznę od pojęcia źrenicy. Przyjęło się nieco błędne określenie, że źrenica rozszerza się lub zwęża. Źrenica to jedynie otwór w tęczówce prowadzący w głąb oka. O ilości wpadającego do oka światła decyduje tęczówka, czyli błona naczyniowa, dzięki której można też mówić o różnych kolorach oczu. Tęczówka za pomocą delikatnych włókienek mięśniowych modyfikuje kształt, zmieniając średnicę swojego otworu [1]. Przysłona obiektywu kamery działa w bardzo podobny sposób. Konstruując obiektyw, człowiek nie pierwszy raz zaadaptował sprawdzone rozwiązanie ze środowiska naturalnego. Listki przysłony w obiektywie to odpowiednik tęczówki, a zamiast włókienek mięśniowych są tam cewki galwanometru albo miniaturowy silnik krokowy (w obiektywach typu P-Iris). Przy okazji mała dygresja językowa. Według dostępnych słowników języka polskiego w zasadzie obie formy: „przesłona" i „przysłona" są poprawne i powszechnie używane. Jednak „przesłona" występuje w większej liczbie znaczeń i może to być np. „element uszczelniający podłoże zapory wodnej" [2], a także pojęcie używane w grze w szachy i oznaczające postawienie bierki na linii działania dalekosiężnej figury tego samego koloru [3]. W odniesieniu do elementu układów optycznych przyjęło się stosowanie formy „przysłona". Wracając do naszych naturalnych „kamer", układ naczyń, wybarwień i fałd w tęczówce jest niepowtarzalny dla każdego oka (każdy człowiek ma dwie zupełnie różne tęczówki) i nie zmienia się z wiekiem. Cechy te zostały wykorzystane przez branżę zabezpieczeń w biometrycznych skanerach tęczówki. Stosuje się je dziś nawet w smartfonach wyższej klasy do odblokowywania urządzenia za pomocą spojrzenia. Kolejną istotną funkcją oka jest zdolność do uzyskania ostrego obrazu. W jaki sposób jesteśmy w stanie czytać książkę, a za chwilę wypatrywać na horyzoncie obiekty odległe nawet o kilkanaście kilometrów? Zawdzięczamy to mechanizmowi akomodacji oka, czyli zdolności do ostrego widzenia w zakresie od bliży do dali. Punkt bliży wzrokowej człowieka, czyli minimalna odległość, dla której oko ludzkie jest w stanie uzyskać ostry obraz, znajduje się 10–11 cm od soczewki oka. Maksymalna odległość, przy której kończy się zdolność akomodacji, wynosi 6–7 m. Powyżej tej odległości oko już się nie „dostraja" i można mówić o zakresie dali wzrokowej od 6 m do nieskończoności [1].

Mięśnie rzęskowe na obwodzie oka mogą pogrubiać i rozciągać soczewkę, modyfikując tym samym jej ogniskową, dzięki czemu możemy „przestawiać" się z widzenia dalekiego na bliskie, i odwrotnie. Odpowiednikiem mięśni rzęskowych w obiektywach z ręczną regulacją jest pierścień ostrości, a w obiektywach z regulacją mechaniczną – silnik ostrości, bo geometrie soczewek w obiektywach się nie zmieniają. Dla ścisłości, bardzo ważny udział w ostrym widzeniu bierze także rogówka, czyli przednia przezroczysta część oka. Niejednokrotnie uszkodzenie lub inne wady rogówki nie pozwalają na prawidłowe widzenie pomimo pełnej sprawności soczewki, tęczówki i pozostałych elementów oka.

Widzenie barwne

Siatkówka oka ludzkiego zawiera średnio 100 mln komórek fotoreceptorowych, tzn. czułych na światło widzialne. Od 90 do 95 mln z nich to pręciki, czyli receptory odpowiedzialne za tzw. widzenie skotopowe, czyli w niekorzystnych warunkach oświetleniowych (np. w nocy). Dzienne (fotopowe) widzenie barwne jest możliwe dzięki czopkom – drugiemu rodzajowi fotoreceptorów, których w oku jest ok. 5 mln [1]. I teraz najciekawsze: czopki występują w trzech odmianach, czułych na trzy różne zakresy długości fal z widma widzialnego: czerwonej, z pogranicza żółtej i zielonej oraz niebieskiej. Mózg, odpowiednio miksując sygnały z poszczególnych rodzajów czopków, generuje wrażenie koloru. Największe zagęszczenie czopków znajduje się w tzw. plamce żółtej, czyli strefie najostrzejszego widzenia, zlokalizowanej mniej więcej w centrum siatkówki oka. Orientacyjny rozkład czopków w tzw. dołku środkowym, czyli centrum plamki żółtej, przedstawiono na *rys. 2*. Co ciekawe, w tym obszarze pręciki praktycznie nie występują.



RYS. 2. Orientacyjny rozkład czopków w dołku środkowym siatkówki oka ludzkiego (fot. Mark Fairchild, Rochester Institute of Technology)

Ten temat jest ważny ze względu na sposób generowania obrazu w urządzeniach telewizji dozorowej, będący niejako odwrotnością procesu percepcji tego obrazu przez nasze oczy. Tak jak w siatkówce występują trzy rodzaje czopków, tak w przetwornikach obrazowych występują subpiksele czułe na zakres koloru czerwonego (R – red), zielonego (G – green) i niebieskiego (B – blue). W monitorach obraz barwny powstaje na skutek „zapalania" w odpowiednich proporcjach poszczególnych barw składowych w pikselach RGB. Włączenie np. piksela czerwonego i zielonego daje w efekcie kolor żółty, niebieskiego i czerwonego – purpurowy, a wszystkich pikseli jednocześnie – kolor biały. Proces ten opisuje trójchromatyczna teoria Younga-Helmholtza [4], a RGB jest obecnie najpowszechniej stosowanym systemem generowania obrazu kolorowego w telewizji dozorowej.

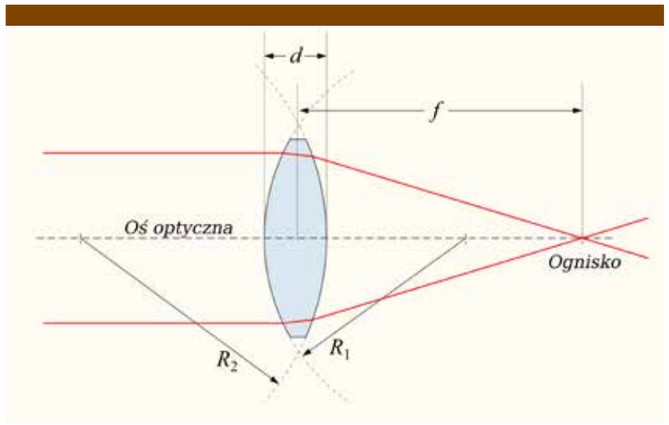
Optyka geometryczna

W pierwszym artykule (1/2019 „a&s Polska") została opisana optyka falowa i cząsteczkowa (kwantowa). W tym potrzebna będzie jeszcze jedna interpretacja, a mianowicie optyka geometryczna, w której jednym z podstawowych pojęć jest promień. Promień świetlny to model optyczny, analogiczny do pojęcia prostej w matematyce. To idealna, nieskończenie wąska forma światła, rozchodząca się po liniach prostych. Promienie mogą zmieniać swój kierunek w wyniku odbicia lub refrakcji. W warunkach świata rzeczywistego rodzajem światła najbliższego definicji promienia świetlnego jest światło lasera i właśnie dlatego wiele elementarnych doświadczeń z zakresu optyki wykonuje się przy użyciu laserów. Innym ważnym pojęciem jest wiązka światła, czyli wiele promieni rozchodzących się w tym samym lub zbliżonym kierunku. Wiązka może być skolimowana (promienie są równoległe do siebie), zbieżna (promienie dążą do punktu wspólnego) lub rozbieżna (promienie wychodzą z punktu wspólnego w różnych kierunkach). Skoro znamy już podstawowe pojęcia optyki geometrycznej, czas na omówienie urządzeń optycznych.

Soczewka

Jednym z najprostszych urządzeń optycznych jest soczewka. To jednocześnie jeden z najistotniejszych elementów naszych oczu, a także obiektywów w kamerach telewizji dozorowej. Najczęściej spotykanym typem jest soczewka sferyczna, czyli taka, której co najmniej jedna powierzchnia jest wycinkiem sfery. Soczewka może być wypukła z jednej lub obu stron, z jednej strony wklęsła, z drugiej wypukła itd. Jej podstawowym zadaniem jest skupianie lub rozpraszanie światła względem swojej osi optycznej. W przypadku soczewki skupiającej punkt, w którym zbiegają się promienie (światło jest skupiane), jest nazywany ogniskiem soczewki, a odległość ogniska od geometrycznego środka soczewki podawana w milimetrach to ogniskowa, oznaczana małą literą *f*. To jeden z podstawowych parametrów optycznych, z którym spotkamy się w każdej karcie katalogowej obiektywu lub kamery zintegrowanej z obiektywem (np. kopułkowej czy w obudowie cylindrycznej).

Soczewka skupiająca



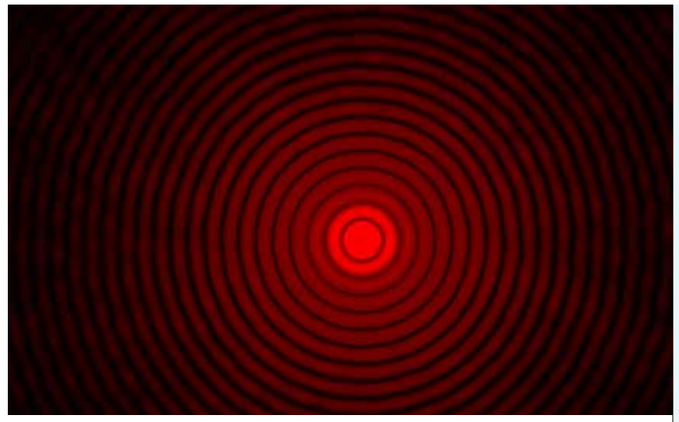
RYS. 3. Działanie dwuwypukłej soczewki skupiającej: ***d*** – grubości soczewki, ***f*** – ogniskowa, (Źródło: www.wikipedia.org)

Działanie soczewki z *rys. 3* można opisać poniższym wzorem:

$$\frac{1}{f} = \frac{2}{R}(n-1) \qquad (1)$$

gdzie ***f*** – ogniskowa soczewki, ***R*** – promień krzywizny soczewki (dla uproszczenia na rysunku promienie R_1 i R_2 są identyczne i oznaczone we wzorze jako ***R***), ***n*** – współczynnik załamania materiału, z jakiego wykonana jest soczewka. Przykładowo, dla szkła kwarcowego współczynnik *n* wynosi ok. 1,46. Po podstawieniu do wzoru (1) tej wartości i przykładowych wartości promieni krzywizny (np. 20 mm) otrzymamy ogniskową o wartości dodatniej, co oznacza soczewkę skupiającą. Zależności wynikające ze wzoru są bardzo proste: im większy współczynnik załamania i im mniejszy promień krzywizny soczewki, tym krótsza ogniskowa soczewki. Ogniskowa może mieć wartość ujemną (w soczewkach rozpraszających, np. dwuwklęsłej).

Oprócz ogniskowej jednym z najistotniejszych parametrów układów optycznych, niestety bardzo często pomijanych w prasie branżowej, jest rozdzielczość optyczna podawana w parach linii na milimetr (lp/mm lub lppm). Jej zrozumienie pozwoli wyjaśnić dlaczego do kamery megapikselowej potrzebny jest dobrej jakości obiektyw, a także jaki wpływ ma przysłona na jakość obrazu. Zanim jednak do tego przejdziemy, należy poznać pojęcie dyfrakcji.



FOT. 1. Rezultat dyfrakcji – plamka Airy'ego wraz z pierścieniami. Obraz rzeczywisty, uzyskany w wyniku przejścia wiązki lasera czerwonego przez otwór kołowy o średnicy 90 µm (fot. Markus Bautsch)

Dyfrakcja, czyli niesforne światło

Wyobraźmy sobie źródło światła skierowane na płytę, pośrodku której znajduje się kołowy otwór. Za płytą umieszczono ekran, na którym obserwujemy przechodzące przez otwór światło. Zgodnie z logiką (i optyką geometryczną także) zmniejszanie średnicy otworu w płycie powinno powodować zmniejszanie średnicy obrazu (koła) obserwowanego na ekranie – i do pewnego momentu tak się właśnie dzieje. Okazuje się jednak, że im bardziej średnica otworu zbliża się do długości fali światła[1], które przez ten otwór przechodzi, obraz na ekranie zaczyna zachowywać się odwrotnie do oczekiwanych efektów. Średnica koła na obrazie, zamiast maleć, zaczyna rosnąć, a wokół koła pojawiają się naprzemiennie jasne i ciemne pierścienie otaczające środek. Centralne koło to plamka Airy'ego[2] (lub dysk Airy'ego), a całość (plamka plus pierścienie) to krążek Airy'ego, czasami określany też jako krążek dyfrakcyjny, gdyż powstaje on na skutek dyfrakcji światła.

Dyfrakcja światła to zjawisko z fizyki falowej, polegające na ugięciu fali elektromagnetycznej (czyli np. światła) na krawędziach szczeliny lub otworu, przez który fala przechodzi. Dyfrakcja to niesforna manifestacja falowej interpretacji światła[3] (niezgodnej z prawami optyki geometrycznej). Jej definicja wynika wprost z zasady Huygensa[4], której analiza nie jest konieczna dla dalszych rozważań, a matematyczny opis wymaga analizy różniczkowych równań falowych.

Nam wystarczy wiedza, że dyfrakcja ma poważny wpływ na rozdzielczość i ostrość obserwowanego obrazu, a im wyższa rozdzielczość przetwornika obrazowego w kamerze, tym większe znaczenie mają skutki dyfrakcji. Dlaczego tak się dzieje? Wróćmy do plamki Airy'ego. Będziemy rozpatrywać przejście światła przez otwór kołowy, bo taki (w każdym razie bardzo zbliżony do koła) występuje w obiektywach stosowanych w kamerach dozorowych. **Miarę kątową plamki Airy'ego można obliczyć z prostego przybliżonego wzoru:**

$$\theta = 1{,}22 \cdot \frac{\lambda}{D} \qquad (2)$$

gdzie **λ** – długość fali elektromagnetycznej (w tym przypadku światła widzialnego), ***D*** – średnica otworu, przez który przechodzi fala.

Dla ścisłości, wzór (2) określa miarę kątową do pierwszego ciemnego pierścienia otaczającego plamkę, a nie samej plamki. Ponieważ wartości te są bardzo zbliżone, takie uproszczenie można przyjąć. Ze wzoru można wysnuć bardzo prosty i zarazem niezwykle istotny wniosek: im mniejsza jest średnica otworu *D*, tym większa plamka Airy'ego. Tu nasuwa się pytanie: skoro długości fal elektromagnetycznych z zakresu światła widzialnego są na poziomie setek nanometrów, a po pobieżnych obliczeniach już widać, że plamka Airy'ego będzie miała średnicę rzędu mikrometrów, to czy jest sens przejmować się tym zjawiskiem? Długość boku pojedynczego piksela w megapikselowych przetwornikach obrazowych jest rzędu pojedynczych mikrometrów, więc odpowiedź brzmi: zdecydowanie tak.

Ten wątek zostanie poruszony w kolejnej części, w której zajmę się m.in. obiektywami, przysłoną, głębią ostrości i rozdzielczością optyczną. □

Wiedza o tym, jak zbudowane jest oko, pozwala zrozumieć m.in. działanie przysłony obiektywu, a także dlaczego większość technologii obrazowania elektronicznego opiera się na trzech kolorach składowych: czerwonym, zielonym i niebieskim (RGB).

Piotr Rogalewski

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

[1] Więcej o falach el-mag w cz. 1. niniejszego cyklu
[2] Zjawisko to jako pierwszy opisał w 1835 r. George Biddell Airy, angielski astronom, fizyk i matematyk
[3] Dla pełnego zrozumienia polecam lekturę cz. 1. niniejszego cyklu artykułów, w szczególności fragment dotyczący dualizmu korpuskularno-falowego.
[4] Dla zainteresowanych zgłębieniem zagadnienia: F. Crawford: „Fale", Wydawnictwo Naukowe PWN, Warszawa 1973.

LITERATURA

[1] Bochenek, M. Reicher: „Anatomia człowieka", t. V, „Układ nerwowy obwodowy. Układ nerwowy autonomiczny. Powłoka wspólna. Narządy zmysłów". Wyd. Lekarskie PZWL, W-wa 1989.
[2] Praca zbiorowa: „Ilustrowany leksykon techniczny", WN-T, wyd. III zmienione, Warszawa 1994.
[3] Praca zbiorowa: „Słownik języka polskiego", Wyd. Naukowe PWN, W-wa 2007.
[4] L.M. Hurvich, D. Jameson: „*Helmholtz and the Three-Color Theory: An Historical Note*". The American Journal of Psychology, vol. 62, nr 1, styczeń 1949.

Nowe funkcje kamer serii equIP®

sieciowych rejestratorów i oprogramowania zarządzającego Honeywell MAXPRO™

Firma Honeywell wprowadziła na rynek zmodernizowaną serię kamer equIP®, nowe rejestratory NVR MAXPRO oraz oprogramowanie do zarządzania obrazem VMS MAXPRO z rozbudowanymi możliwościami. Zaprojektowano je do ochrony złożonych inwestycji, jednocześnie z myślą o ułatwionej obsłudze systemu przez operatorów i obniżeniu całkowitych kosztów operacyjnych.

Algorytmy analizy zawartości wizji i rozszerzona funkcjonalność ochrony prywatności to jedne z najważniejszych funkcji, które firma Honeywell dodała do nowej serii kamer equIP®, sieciowych rejestratorów (NVR) i systemu zarządzania obrazem (VMS) MAXPRO™. Technologie zaimplementowane w kamerach i nowe oprogramowanie analityczne we wszystkich modelach obejmują: analizę trasy przemieszczania się osoby/obiektu, strefy alarmowe, pojawienie i zniknięcie obiektu. Z kolei kamery z funkcją pracy przy słabym oświetleniu (*LowLight*) zostały wyposażone również w funkcje analizy behawioralnej (aktywności), śledzenia oraz klasyfikacji ludzi i pojazdów podczas przemieszczania się w scenie – algorytmy *Xtralis LoiterTrace, Smart Impressions* oraz zliczanie osób. Nowe kamery, rejestratory i oprogramowanie VMS do zarządzania obrazem pomagają również klientom spełnić wymogi RODO.
Zarówno MAXPRO NVR, jak i MAXPRO VMS zostały zaktualizowane, aby móc obsługiwać najnowsze kamery serii equIP i nowe funkcje dla szerszych zastosowań.

Aktualizacje obejmują:

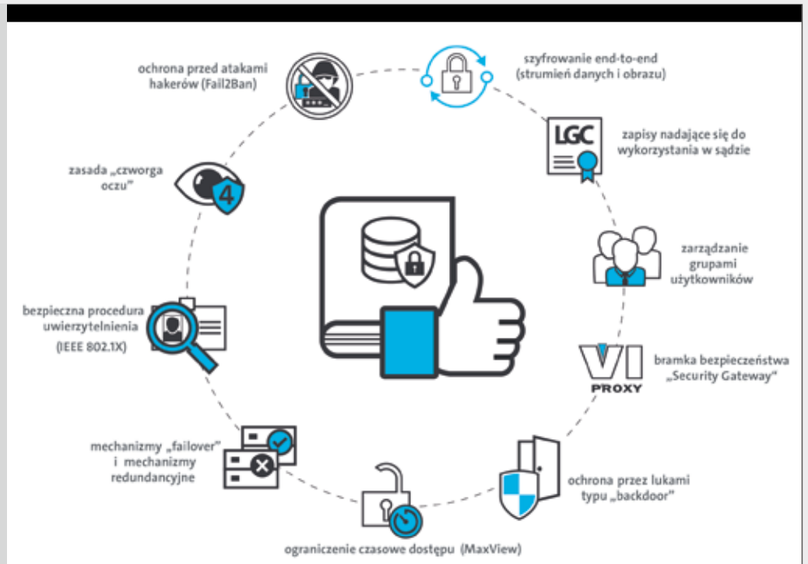
- zastosowanie nowych przełączników PoE (HPOE3X) i AUX w celu zmniejszenia kosztów instalacji i konserwacji oraz zasobów pamięci masowej do rejestracji nagrania,
- dzięki zastosowaniu kompresji wideo H.265 koszty pamięci masowej i wymagana przepustowość również zostały zmniejszone (nawet o 40%),
- zastosowanie w MAXPRO VMS R500 pikselizacji osób lub ich rozmycia w trybie podglądu na żywo obrazów z nowych modeli kamer equIP w celu jak najlepszej ochrony prywatności (RODO).

Nowe wersje urządzeń ulepszają powiększającą się linię produktów CCTV firmy Honeywell, zapewniając skalowalne rozwiązania wysokiej jakości na potrzeby zastosowań biznesowych. Ponadto rozwiązania serii equIP oraz MAXPRO współpracują z różnorodnymi produktami Honeywell, w tym m.in. z systemami kontroli dostępu PRO-Watch®, zapewniając kompleksową platformę zarządzania budynkiem. □

Honeywell

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

Nie tylko bezpieczeństwo cybernetyczne – firma Dallmeier, niemiecki producent systemów dozoru wizyjnego z Ratyzbony przedstawia kompleksowe podejście do bezpieczeństwa w systemach dozoru wizyjnego. W swoim pakiecie informacyjnym zawierającym konkretne zalecenia dotyczące postępowania omawia, na co w obszarze strategii bezpieczeństwa powinni zwracać uwagę użytkownicy. Elementy tej strategii wykraczają poza klasyczne instrumenty bezpieczeństwa cybernetycznego.



Funkcje bezpieczeństwa danych połączonych modułów ochrony i bezpieczeństwa danych firmy Dallmeier

Ochrona i bezpieczeństwo danych

Liczba cyberataków na urządzenia IoT, a więc także na systemy dozoru wizyjnego, bardzo szybko rośnie. Osoby odpowiedzialne za bezpieczeństwo wielu banków w różnych krajach mogły być zaskoczone, gdy w 2013 r. rosyjskie grupy hakerów w trakcie kampanii „Carbanak" ukradły im środki o wartości kilkuset milionów dolarów. Ataki przeprowadzono w drodze przejęcia kontroli nad kamerami monitoringu w instytucjach finansowych, by móc szpiegować treści wyświetlane na ekranach i dane wprowadzane z klawiatury, a także identyfikować pracowników (np. na podstawie tabliczek z nazwiskiem lub legitymacji pracowniczych) jako cele tzw. *spear phishingu*. Jak wykazały znane ataki Mirai i Persirai, systemy dozoru wizyjnego są również podatne na ataki typu *Denial-of-Service*.

Od planowania po zaufanie do producenta

Każda firma, chcąc się skutecznie chronić przed cyberatakami, musi zastosować kompleksową strategię bezpieczeństwa. Dallmeier wskazuje pięć istotnych aspektów bezpieczeństwa, które są ze sobą powiązane: • uwzględnianie ich już na etapie planowania • włączanie do strategii IT • funkcje bezpieczeństwa cybernetycznego w systemach • ochrona danych, a także • wiarygodność producenta.

Planowanie powinno w niezbędnym zakresie uwzględniać wymogi bezpieczeństwa, np. w inteligentny sposób wykorzystując technologię *3D Planning* (pozycjonowanie GDPR). Inwestycja powinna się wpisywać w strategię IT przedsiębiorstwa, coraz częściej bowiem całkowitą odpowiedzialność za istotne zasoby, takie jak wydajność serwerów czy nawet cały system zabezpieczeń, ponosi dział IT. Dla obszaru zasadniczego – właściwego „bezpieczeństwa cybernetycznego" – ważne jest, by systemy miały wszystkie niezbędne funkcje „bezpieczeństwa IT", począwszy od wzmocnionych systemów operacyjnych, przez możliwość rozdzielania sieci, aż po techniki szyfrowania i możliwości wykrywania ataków. Aspekt czwarty – uwzględnienie ochrony danych osobowych od chwili wejścia w życie RODO powinien być sprawą niemal oczywistą. Klienci powinni zwracać szczególną uwagę także na producenta: sprawdzać, jakie rozwiązania systemowe i sprzętowe zostały przyjęte na etapie projektowania i produkcji w celu zabezpieczenia systemów, a także kwestie wzajemnej współpracy oraz integracji z systemami zewnętrznymi w kontekście wszystkich aspektów bezpieczeństwa.

Zadaniem pakietu informacyjnego producenta jest dostarczenie odpowiedzi na te i wiele innych pytań. Ponadto w jego części *Best Practice Guide* zawarto obszerny zbiór praktycznych informacji i wskazówek dotyczących konfiguracji dla pracowników działów IT i bezpieczeństwa oraz administratorów. Pakiet obejmuje również najnowsze wydanie Video Extra oraz broszurę firmy Dallmeier zawierającą informacje z zakresu ochrony i bezpieczeństwa danych. □

Osoby zainteresowane znajdą pakiet informacyjny (w języku angielskim) pod adresem: https://www.dallmeier.com/ls/cybersecurity

Dallmeier electronic

Bahnhofstr. 16, 93047 Regensburg,
Niemcy
tel +49 151 58204199
www.dallmeier.com

Śmieci, czyli... płonie śmietnisko na polu

TEKST
Zbigniew Morawski
Security Solution Engineer
Hikvision Poland

Po licznych pożarach wysypisk śmieci, które dały się we znaki społecznościom lokalnym i stanowiły pożywkę dla mediów, odpowiednie władze postanowiły zobowiązać właścicieli wysypisk do wprowadzenia dodatkowych środków technicznych podnoszących bezpieczeństwo na placach składowych.

Zgodnie z ustawą z 20 lipca 2018 r. o zmianie ustawy o odpadach po upływie 6 miesięcy weszło w życie rozporządzenie definiujące szczegóły systemów dozoru wizyjnego VSS. Nabrało ono mocy prawnej 22 lutego 2019 r. Warto przyjrzeć się zapisom aktu zarówno wyższego, jak i niższego rzędu pod kątem wymagań technicznych dla systemów VSS.

W ustawie mamy następujące zapisy:
- prowadzący magazynowanie odpadów lub zarządzający składowiskiem odpadów jest obowiązany do prowadzenia wizyjnego systemu kontroli miejsca magazynowania lub składowania odpadów,
- czas przechowywania materiału to jeden miesiąc (praktycznie 31 dni),
- wizyjny system kontroli miejsca magazynowania lub składowania odpadów prowadzi się przy użyciu urządzeń technicznych zapewniających przez całą dobę zapis obrazu i **identyfikację** osób przebywających w tym miejscu.

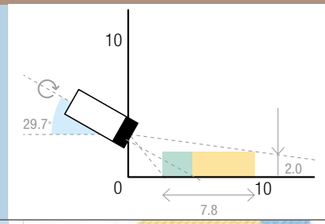
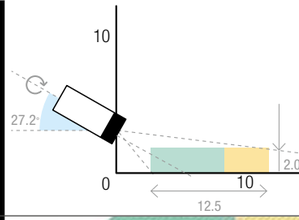
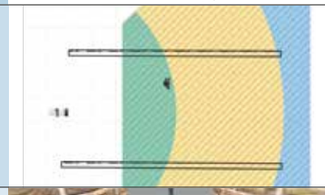
Warto zwrócić uwagę na słowo „identyfikacja", gdyż niesie ono poważne następstwa techniczne odnoszące się do zastosowanego sprzętu oraz sposobu podejścia projektowego do systemów VSS.

Obecnie możemy się również zapoznać z tekstem rozporządzenia. Przytoczmy główne i znaczące dla sposobu zabezpieczenia zapisy, które się tam znajdują:
- monitorowana będzie cała powierzchnia magazynowanych śmieci, łącznie z drogami dojazdowymi oraz okalającym pasem zewnętrznym o szerokości 5 m,
- dla składowisk większych niż 2 ha – pas o szerokości 15 m od zewnątrz składowiska do wewnątrz,
- zarejestrowany obraz z systemu będzie dostępny online dla wojewódzkich inspektorów ochrony środowiska,
- obraz będzie przechwytywany za pomocą kamer dzień/noc,
- opuszczono rozwiązania rejestracji w chmurze, po warunkiem że łączny czas wyłączenia instalacji w ciągu roku nie może być dłuższy niż 2 dni.

W rozporządzeniu powołano się na zastosowanie normy PN-EN-62676-4:2015-06 w zakresie wymaganych parametrów technicznych urządzeń. Jest to nieporozumienie, gdyż wymieniona seria norm zajmuje się bardziej definiowaniem funkcji systemów VSS, a nie parametrów poszczególnych urządzeń. Pośrednio można się zgodzić, że na podstawie takich danych, jak planowany zasięg, funkcja, ukształtowanie terenu czy warunki oświetleniowe można określić minimalne warunki techniczne dla urządzeń, jednak wymaga to indywidualnego podejścia. Koreluje to z procesem projektowania zalecanego przez normę, w której projektując instalację VSS, pierwszym i podstawowym dokumentem jest tzw. OR, czyli „Wymagania użytkowe".

Wróćmy jednak do wcześniej wyróżnionego terminu „identyfikacja". Jest to cel funkcjonalny obrazu, umożliwiający identyfikację osoby ponad wszelką wątpliwość. Aby ten cel zrealizować, trzeba zapewnić kadr, w którym obiekt będzie rejestrowany z rozdzielczością pionową równą co najmniej 250 pikseli/m, a także
- instalację kamer na wysokości głowy człowieka, gdyż instalacja znacznie powyżej może nie zapewnić pełnego widoku twarzy,
- oświetlenie powinno umożliwiać obserwację szczegółowych cech obiektów, takich jak kolor ubrania. Ponadto na potrzeby identyfikacji należy zapewnić oświetlenie twarzy celu.

Sprawdźmy, jak od strony praktycznej wygląda spełnienie wg PN-EN-62676-4 wymogu zapewnienia identyfikacji przez kamery dla osoby o wzroście 180 cm.

KAMERA 2 MPIX O ROZDZIELCZOŚCI 1080P Z PRZETWORNIKIEM OBRAZU 1/1,8" (NAJCZĘŚCIEJ STOSOWANA).		KAMERA 8 MPIX O ROZDZIELCZOŚCI 4K Z PRZETWORNIKIEM OBRAZU 1/1,8".
Sposób instalacji kamery: • wysokość instalacji – 3 m, • ogniskowa obiektywu – 2,8 mm o kącie H = 92° • identyfikacja – kolor zielony • rozpoznanie – kolor żółty		 Sposób instalacji kamery: • wysokość instalacji – 3 m, • ogniskowa obiektywu 2,8 mm o kącie H = 96° • identyfikacja – kolor zielony • rozpoznanie – kolor żółty
Przedstawienie długości obszaru celu funkcjonalnego kamery dla wymaganej szerokości pasa zewnętrznego 5 m		 Przedstawienie długości obszaru celu funkcjonalnego kamery dla wymaganej szerokości pasa zewnętrznego 5 m
Przykładowy widok z kamery w pasie 5 m		 Przykładowy widok z kamery w pasie 5 m
Kamera 2 Mpix jest w stanie zagwarantować funkcję identyfikacji na obszarze o długości ok. 2 m.		Kamera o rozdzielczości 4K jest w stanie zapewnić funkcję identyfikacji na długości ok. 7,5 m przy zastosowaniu obiektywu o ogniskowej 2,8 mm. Użycie obiektywów o innych ogniskowych nie wydłuży sektora funkcji, może ją jedynie przesunąć w osi X.

Z powyższego wynika, że chcąc spełnić oczekiwania ustawodawcy, w systemach VSS trzeba stosować urządzenia o wysokich rozdzielczościach i dużej czułości. Należy też korzystać z oświetlenia zewnętrznego na poziomie gwarantującym pracę systemu w trybie kolorowym, gdyż identyfikacja wymaga rejestracji wszelkich unikalnych szczegółów. Można pokusić się o szybką symulację, ile kamer będzie potrzeba, żeby zabezpieczyć płaski obiekt typu składowisko o wymiarach 20 x 50 m z 5-metrowym pasem przyległym, zapewniając identyfikację.

Zabezpieczenie składowiska 20 x 50 m.

Analizując tylko wymagany teren wokół hałdy, otrzymujemy minimalną liczbę kamer wynoszącą 20 szt. Ponadto musimy zapewnić monitoring całego terenu składu. Taka liczba kamer wysokiej rozdzielczości generuje potrzebę stosowania profesjonalnych urządzeń sieciowych oraz – zakładając niewielkie parametry strumienia 3072 Kb/s (kodek H.265, profil średni, 6 fps) – potrzebę stosowania pamięci masowych o pojemności 2 TB kamerę dla zapisu 31 dni.
Zasadne jest pytanie, dlaczego potrzeba tylu kamer, skoro można by zastosować kamery PTZ zapewniające identyfikację wspartą inteligentną analityką kamer stacjonarnych? Zapewne można do tego zagadnienia podejść w ten sposób (i jest to jak najbardziej poprawne), ale w rozporządzeniu pada magiczne słowo „w sposób ciągły" – co wymaga zastanowienia się, jakie intencje przyświecały ustawodawcy chcącemu zapewnić identyfikację osób przebywających w sposób ciągły.

Na koniec zestawiłbym koszty, jakie podano w mediach. Są to szacunkowe kalkulacje Ministerstwa Środowiska. „Gazeta Prawna" podaje w artykule z 19.08.2018 r., że koszt instalacji 16 kamer z rejestratorem wyniesie ok. 16 tys. zł. Najtańsze kamery 8 Mpix (o słabych parametrach) to koszt w granicach 1,5 tys. zł, co przy liczbie 20 sztuk znacznie przewyższa koszty szacunkowe. Do całości należy doliczyć budowę systemu rejestracji, infrastruktury kablowej ziemnej, instalację słupów, oświetlenia, systemu zasilania i transmisji.
Biorąc pod uwagę tak dokładnie opisane wymogi monitorowania składowisk, kluczowe w procesie inwestycyjnym będzie odpowiednie podejście inwestora do rozwiązania problemu. Nie można zakładać, że postawienie kilku słupów z najtańszymi kamerami spełni wymogi formalne. W przypadku jakiegokolwiek zdarzenia niepożądanego należy się spodziewać, że odpowiednie służby poproszą o materiał z chwili zdarzenia i sprawdzą, czy spełnia wymogi formalne.

Wśród rozwiązań poprawnych technicznie znajdą się systemy zarówno oparte na kamerach stacjonarnych, jak i z automatyczną detekcją, a funkcję identyfikacji zapewnią wysokiej jakości kamery PTZ. □

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

Wdrożenie GEMOS w Kompanii Piwowarskiej

CASE STUDY

Podstawową funkcjonalnością systemu GEMOS jest integracja i analiza wszelkich zdarzeń mających miejsce w obiekcie. Zaimplementowane procedury działań filtrują wszystkie sygnały z budynku, aby wybrać spośród nich tylko istotne dla operatora. Dzięki temu może on szybko i precyzyjne analizować różnego typu zdarzenia, np. alarm pożarowy czy włamaniowy, stan przejść kontroli dostępu, awarie automatyki budynkowej itp.

Każde zdarzenie może być inaczej interpretowane w systemie. Dozwolone przejście nie musi angażować uwagi operatora, jednak próba forsowania lub pozostawienia drzwi otwartych mogą wywołać interakcje. ***GEMOS automatycznie poinformuje operatora o danym zdarzeniu, na planie budynku wskaże lokalizację drzwi oraz dzięki integracji z systemem CCTV pokaże obraz z kamery i nagranie przed wystąpieniem zdarzenia. Takich integracji może być wiele, wszystko zależy od charakterystyki budynku i tego, co chcemy osiągnąć. Możliwości są nieograniczone*** – mówi Maciej Nowacki, GEMOS Product Manager w Ela-compil.

Jedną z firm, która zdecydowała się skorzystać z możliwości, jakie daje GEMOS, jest Kompania Piwowarska. Lider rynku piwa w Polsce zapewnienie bezpieczeństwa w miejscu pracy traktuje priorytetowo. Jest ono jednym z filarów strategii firmy, co pociąga za sobą nieustanne inwestowanie w rozwiązania wspierające eliminowanie i ograniczanie czynników ryzyka. Kładąc nacisk na podnoszenie poziomu bezpieczeństwa, Kompania Piwowarska wyposażyła w system GEMOS dwa z trzech swoich browarów – Lech Browary Wielkopolski w Poznaniu i Browar Dojlidy w Białymstoku. To w nich warzone są najchętniej wybierane przez Polaków piwa, m.in. Żubr, Tyskie, Lech, Dębowe, Redd's czy kolekcja specjalności Książęcego.

Jak większość zakładów jesteśmy wyposażeni w szereg systemów istotnych dla zapewnienia bezpieczeństwa – wyjaśnia Paweł Żółtowski, szef kontroli ryzyka w Kompanii Piwowarskiej. – ***Do niedawna nie były one jednak tak użyteczne, jak byśmy sobie tego życzyli. Brak współpracy między systemami, trudna obsługa czy ograniczone możliwości raportowania przekładały się na długi okres wdrażania pracowników, ograniczenia w wykrywaniu incydentów i opóźnienia w reakcjach na alerty. Szukając rozwiązania, postawiliśmy na integrację. Wybraliśmy GEMOS ze względu na bardzo duże zdolności integracyjne, aprobatę CNBOP i wsparcie techniczne ze strony Ela-compil. Nie bez znaczenia była też bardzo dobra relacja jakości do ceny. GEMOS połączył systemy różnych producentów w dobrze zgraną całość. Zyskaliśmy jeden intuicyjny interfejs użytkownika, błyskawiczny dostęp do rozproszonych wcześniej informacji i dodatkowe benefity płynące z synergii. Wdrażanie pracowników stało się prostsze, wykrywanie problemów skuteczniejsze, a podejmowane działania są szybsze i bardziej adekwatne. Jesteśmy zadowoleni z efektu*** – dodaje Paweł Żółtowski. Każdy zakład produkcyjny ma specyficzne warunki, do których należy dopasować funkcje systemu integrującego. W GEMOS-ie opracowano szereg procedur i instrukcji dla operatora na wypadek różnych zdarzeń, dzięki czemu może on natychmiast zweryfikować zagrożenie. Plan budynku jest drukowany automatycznie z zaznaczeniem miejsca wzbudzenia alarmu oraz uruchamiany podgląd z najbliższej kamery. Wybrane osoby zostają powiadomione o zagrożeniu za pomocą wiadomości SMS.

Prace wdrażania systemu GEMOS rozpoczęto od opracowania koncepcji i dokumentacji projektowej, w której zawarto wszystkie wymagania użytkownika. Ustalono, że realizacja inwestycji odbędzie się etapami. W pierwszym zainstalowano interfejs komunikacyjny do systemu ppoż., redundancję serwerów oraz moduł SMS do powiadamiania kierowników zmiany o zagrożeniach, opracowano dedykowany interfejs kontroli dostępu. W drugim etapie rozbudowano system o interfejs do systemu telewizji dozorowej oraz ochrony obwodowej obiektu. Wszystkie prace zakończyły się w terminie – podkreśla Mariusz Bernat, kierownik projektu w Ela-compil odpowiedzialny za wdrożenie GEMOS w Kompanii Piwowarskiej. □

Branża systemów zabezpieczeń przeżywa intensywny rozwój w zakresie oprogramowania zarządzającego obrazem wideo. Przyczyniają się do tego zmiany w prawie (RODO) oraz unifikacja rozwiązań. Wdrażane są pomysły podpatrzone na rynkach ościennych, w tym technologii IT, dotyczące zwłaszcza rozwiązań mobilnych.

T E K S T
Radomir Dębek

T E K S T
Jan T. Grusznic

Ciągły wzrost funkcjonalności systemów do zarządzania obrazem wideo (**VMS** – *Video Management System*, *Video Management Software*) nie ułatwia jednak decyzji osobom, które muszą zdecydować o wyborze rozwiązania spośród dziesiątek istniejących na rynku. Jak bowiem ocenić system, który tylko nagrywa i wyświetla obrazy z kamery, od takiego, który ponadto zapewnia nadmiarowość zapisu, obsługę urządzeń wielu producentów, analizę obrazu, integrację z systemami uzupełniającymi (np. kontroli dostępu, sygnalizacji włamania)? Czy ten drugi system jest na pewno lepszy, a pierwszy niewystarczający? A może w ogóle VMS to za mało i potrzeba czegoś więcej? Czy zagubieni w liczbie możliwych rozwiązań potrafimy właściwie zidentyfikować własne potrzeby i poprawnie wybrać typ systemu?

Telewizja w standardzie analogowym, czyli jak to się zaczęło

Początki rozwiązań systemów wizyjnych były skromne, zwłaszcza od strony zarządzania, ale jednoznacznie zainspirowały i nadały kierunek rozwoju oprogramowania dzisiaj określanego akronimem VMS. Zanim jednak rozłożymy wspomniany skrót literowy na czynniki pierwsze, sięgnijmy do rozwiązań, dzięki którym osiągnęliśmy obecny stan technologiczny.

Czasy technologii VHS to zupełny brak komunikacji pomiędzy rejestratorami w zakresie ich zasobów, a co za tym idzie również brak nadzoru ich stanu za pomocą jakiegokolwiek oprogramowania. Pierwszy krok do większych zmian umożliwiło wprowadzenie na rynek rejestratora cyfrowego, który na dalszym etapie swojego rozwoju – oprócz zamiany taśmy na dyski twarde i możliwości automatycznego nadpisywania najstarszych nagrań – został także wyposażony w interfejs komunikacji sieciowej. Bardzo szybko zaczęto oferować oprogramowanie (tzw. CMS – *Central Management System*) zarządzające kilkoma, często nawet kilkunastoma rejestratorami. Operator systemu nareszcie mógł otrzymać w jednym miejscu informację z konkretnego rejestratora o awarii dysku lub informację o zalogowaniu się użytkownika do urządzenia. Otrzymał narzędzie, które w sposób ustrukturalizowany prezentowało zasoby systemowe, a jednocześnie znacząco ułatwiało prace związane z przetwarzaniem obrazu (np. eksport nagrań), czy tak banalnym zadaniem, jak aktualizacja oprogramowania układowego rejestratorów. Trzeba jednak wyraźnie zaznaczyć, że ten jakże ważny moment tylko uchylił drzwi do procesu udoskonalania rozwiązania. Szybko ujawniły się braki w zakresie możliwości zaawansowanej kontroli dostępu użytkowników do systemu czy rozbudowanego dziennika zdarzeń działania usług składowych systemu, nie wspominając o potrzebie posiadania większej przestrzeni dyskowej rejestratorów i większej liczby podłączonych kamer. Na przeszkodzie stała jeszcze analogowa budowa samego systemu opartego na rejestratorach. Dopiero boom na rynku kamer IP stał się punktem zwrotnym dla najważniejszego elementu systemu dozoru wizyjnego, czyli oprogramowania VMS.

> Boom na rynku kamert IP stał się punktem zwrotnym dla najważniejszego elementu systemu dozoru wizyjnego – oprogramowania VMS.

Etymologia terminu VMS

Kluczowym elementem wspomnianego skrótu jest „Video" nierozerwalnie połączone z obsługą strumieni wizyjnych skompresowanych w technologiach wspieranych zarówno przez kamerę, jak i wybrany system rejestracji. Niektórzy rozwijają go też jako Video Management Software. Dopóki w rozwinięciu pojawia się słowo kluczowe „Video", dopóty nie trzeba będzie udowadniać, co jest filarem systemów VMS. Dla wielu producentów od początku XXI wieku skrót VMS oznacza kluczowe możliwości obsługi i zarządzania kamerami sieciowymi oraz ich zapisem na sieciowych zasobach dyskowych. Technologie zapisu wyewoluowały do rozwiązania popularnie określanego rejestratorem sieciowym – NVR – pracującym jako usługa oraz rozwiązań wspierających macierze z wykorzystaniem np. protokołu iSCSI. Szczególnie ważny jest rozwój standardów otwierających homogeniczną strukturę systemu VMS w zakresie wspierania różnych producentów kamer IP – tutaj z pomocą przycho-

dzi profil S standardu Onvif. W obecnych czasach i to okazuje się niewystarczające, szczególnie jeśli uwzględnić kamery nagrywające na nośniku lokalnym. Wówczas sięgnięcie do nagrań z poziomu aplikacji klienckiej systemu VMS będzie oznaczało konieczność kompatybilności z kolejnym profilem Onvif, tym razem profil G, który nie jest jeszcze rozpowszechniony w takim zakresie, jakiego życzyliby sobie użytkownicy. Z kolei o funkcjonalnościach z zakresu wpływania na ustawienia obrazu, zdarzeń z detekcji ruchu, przesyłu metadanych czy obsługi dwukierunkowego audio traktuje nowo wprowadzony profil T standardu. Podobnej wszechstronności należy oczekiwać od rozwiązań dedykowanych do obsługi nagrań. Na szczęście w tym zakresie jest nieco łatwiej ze względu na mniejszą liczbę dostępnych technologii.

Z perspektywy użytkownika cały *back-end* (część najbardziej oddalona od klienta, sposób działania [przyp. red.]) systemu nie jest jednak aż tak istotny, gdy w grę wchodzi środowisko pracy, czyli interfejs graficzny użytkownika (tzw. GUI) oraz wszystkie dostępne narzędzia wpływające na bardziej efektywną pracę operatora. Zaawansowane zarządzanie wyświetlaniem układów podziału obrazu na 4 czy nawet 8 ekranach stacji operatorskiej to najbardziej widoczne efekty działania systemu VMS. Najnowsze rozwiązania bardzo często korzystają już z interfejsu projektowanego pod kątem obsługi za pomocą dotyku. Od maja 2018 r. funkcjonalność rozszerzono o dodatkowe wymogi bezpieczeństwa (RODO) w zakresie ograniczania dostępu do materiałów eksportowanych czy „hasłowania" wykonywanych ujęć z kamer. Od systemu VMS teraz oczekuje się także wsparcia połączeń szyfrowanych, szyfrowania samego zapisu czy szczegółowego logowania każdego działania operatora. Funkcjonalność alarmowania wszelkich stanów dotyczących wszystkich komponentów systemu czy możliwość budowania zaawansowanych harmonogramów działania są dostępne w niemal wszystkich proponowanych na rynku rozwiązaniach.

VMS+, czyli jeszcze więcej możliwości

Współczesność, szczególnie w zakresie funkcjonalnym, jest równoznaczna z mobilnością. Rozpisywanie się o aplikacjach na smartfon byłoby nietaktem, zwłaszcza w 2019 r. – teraz mają je nawet pralki automatyczne, a powoli są używane w ramach autoryzacji dostępu do auta. Użytkowników głodnych nowoczesnych rozwiązań

Filarem systemów VMS jest słowo kluczowe – Video.

zainteresuje odmienne wykorzystanie wspomnianego smartfona. Jeżeli spojrzymy na niego jak na urządzenie oferujące grupę interfejsów komunikacyjnych oraz obiektyw, możemy nadać mu zupełnie nową funkcjonalność. Po zainstalowaniu aplikacji umożliwiającej „wypychanie" obrazów wideo (tzw. *video-push*) może się on stać mobilnym punktem kamerowym strumieniującym do systemu VMS z dowolnego miejsca pokrytego zasięgiem sieci 3G/LTE. Do tego dochodzi możliwość wysłania współrzędnych GPS do systemu w celu prezentacji pozycji na mapie. A przecież nie trzeba się ograniczać do smartfona, kiedy system Android pracujący w tandemie z kamerą, modemem LTE i GPS-em są dostępne w formie okularów, hełmu czy drona. Mobilność przez duże M można by rzec.

Wymagania funkcjonalne operatorów są dzisiaj znacznie większe niż jeszcze kilka lat wstecz. Temat komunikatora tekstowego wbudowanego w interfejs przewija się od lat, a jednak nie doczekał się znaczącej popularyzacji. Tego typu rozwiązania były popularne w świecie aplikacji na komputery klasy PC z końcem XX wieku i miały ciekawe możliwości współdzielenia zasobów czy udostępniania linków. Cały czas współczesne systemy VMS są oparte na globalnym nadawaniu uprawnień i administrator systemu nie może dynamicznie przydzielić jednorazowych uprawnień użytkownikowi do wybranych zasobów (np. kamer w danej lokalizacji). Jedno jest pewne, GUI systemów VMS nie oferuje jeszcze wszystkiego, co jest potrzebne w zakresie narzędzi ułatwiających codzienną pracę. Przykładem tak trywialna i z pozoru prosta funkcjonalność wywoływania kilku kamer do podglądu bez nadmiaru czynności. Widoki ulubione wyczerpały formułę i aż prosi się, by można było wskazać grupy kamer, choćby ruchem kolistym myszy na mapie, i wywołać tę grupę z danego obszaru. Jeśli przyjrzeć się dostępnym dla użytkownika narzędziom przeznaczonym do przeszukiwania nagrań, okazuje się, że tylko nieliczni producenci pozwalają na wskazanie obiektu w materiale nagranym i przeszukanie aktualnych strumieni w celu odnalezienia podobnego obiektu.

Od kilku lat można zaobserwować stopniową rozbudowę funkcjonalności systemów VMS w bardzo „chwytliwym" zakresie, jakim jest integracja. Jeśli ma ona ścisły związek z obsługą urządzeń strumieniujących, takich jak rozpoznawanie twarzy czy czytanie tablic rejestracyjnych (tzw. ANPR), często jest uznawana za nieodłączny element systemu zarządzania sygnałem wizyjnym. Do grona nieformalnych wyróżników już dawno trafił standard komunikacji z wykorzystaniem serwera OPC, a obecnie dochodzi do nich także system SCADA. Szczególnie ten pierwszy otwiera duże możliwości integrujące dla systemów korzystających z tego standardu, a są to systemy sygnalizacji włamania i napadu, systemy sygnalizacji alarmu pożarowego, systemy kontroli dostępu, dźwiękowe systemy ostrzegawcze czy systemy przyzywowe. Tak bogate możliwości integracji wpływają na charakter systemu VMS, wymuszają redefinicję jego możliwości czy wręcz wskazują nową drogę, którą powinien wybrać projektant lub użytkownik.

Od kilku lat obserwujemy stopniową rozbudowę funkcjonalności VMS w zakresie integracji.

PSIM, czyli dlaczego VMS to za mało

Możliwość integracji różnych systemów, tworzenie obrazu sytuacji opartego na dopływających danych i dostarczanie operatorom narzędzia pozwalającego na skuteczne reagowanie to główne powody wyboru oprogramowania typu PSIM[1]. Niemal nieograniczone możliwości integracji sprawiają, że często PSIM jest wykorzystywana jako platforma do zarządzania całym obiektem, a nawet przedsiębiorstwem, nie ograniczając się tylko do systemów zabezpieczania technicznego.

Światowy rynek oprogramowania PSIM nieprzerwanie rośnie, choć nie jest to wzrost dynamiczny. Głównymi ograniczeniami są poziom cen i pobieżna wiedza na temat tych rozwiązań. Ponadto popularyzacja PSIM jest hamowana przez systemy VMS, wdrażane z powodzeniem w niewielkich i mało skomplikowanych rozwiązaniach, które są poza zasięgiem wysokiej klasy platform PSIM ze względu na ich wysoką cenę.

PSIM jest platformą programową, która gromadzi informacje z różnych urządzeń zabezpieczających i systemów informatycznych oraz zarządza nimi, a następnie przedstawia je, dając wspólny obraz sytuacji. Tymi urządzeniami mogą być tradycyjne „czujniki" systemu zabezpieczeń, np. kamery dozorowe, urządzenia kontroli dostępu, detektory ruchu, a także „niekonwencjonalne" systemy nadzorujące pracę sieci komputerowych i systemów automatyki budynkowej BMS, systemy monitorujące zagrożenia cybernetyczne, a nawet kanały pogodowe. Rzetelny producent PSIM nie preferuje konkretnych dostawców urządzeń, pozostawiając użytkownikom dowolność wyboru przy integracji starszych systemów i nowoczesnych technik pojawiających się na rynku.

Coraz większy wybór funkcji oferowanych przez systemy VMS, coraz mocniejsza reprezentacja oprogramowania do wizualizacji stanów systemów pożarowych (które również są sprzedawane pod postacią PSIM) rodzi pytania, czym rzeczywiście jest PSIM, jakie są różnice w porównaniu z innymi systemami wspomagającymi bezpieczeństwo, które oferują własne możliwości integracji.

Główną zaletą oprogramowania PSIM są jego prawie nieograniczone możliwości integracji, współpracy z istniejącymi i planowanymi systemami, bez „blokowania" konkretnych dostawców. Zwykle systemy oferowane przez producentów, którzy produkują rozwiązania sprzętowe, ograniczają się do produktów z portfolio właśnie tego dostawcy. Integracja z pozostałymi systemami dostępnymi na rynku jest na poziomie podstawowym i jeśli w ogóle jest wykonywana, to na bazie dostępnych otwartych protokołów. W takich przypadkach system można rozszerzyć głównie z użyciem produktów tego tylko producenta. Integracja z istniejącym systemem od innego dostawcy może okazać się trudna, wręcz wymuszać czasami wymianę istniejących już systemów.

PSIM to rozwiązanie oparte na analizie napływających danych. Gromadzenie i korelacja informacji z różnych źródeł oznacza, że alarmy są wyzwalane tylko w przypadku istotnych zdarzeń. Identyfikowanie zachodzących wydarzeń i efektywne nimi zarządzanie wpływa na ograniczanie ryzyka. To właśnie zdolność do aktywnego zarządzania wydarzeniami pozwala zwiększyć wydajność operacyjną. Korzystając z takich adaptacyjnych przepływów zadań, operator wie, co się dzieje, gdzie się dzieje i co należy z tym zrobić. PSIM pozwala opracować plany działań krok po kroku, aby uwzględnić różne sytuacje. Dodatkowo dynamiczne przepływy zadań mogą się zmieniać w zależności od pory dnia, poziomu zagrożenia oraz liczby i rodzajów alarmów w systemie.

Brak aktywnego zarządzania zdarzeniami powoduje całkowite uzależnienie się od doświadczenia operatora, jego dyspozycyjności i stanu psychofizycznego. To właśnie sprawia, że rozwiązanie PSIM jest systemem opartym na inteligencji, a nie listą zadań, które należy wykonać (jak w przypadku systemów VMS).

Korzyści te w połączeniu z rozproszoną liczbą stanowisk odbiorczych zmieniają sposób działania korporacji. PSIM pozwala na bardziej scentralizowane sterowanie i kontrolę, bez konieczności przebywania w konkretnym obiekcie. Utarł się zwyczaj, że monitorowanie stanów systemów wspomagających bezpieczeństwo jest wykonywane w miejscu instalacji. Dzisiaj jednak coraz popularniejszy staje się dozór zdalny.

PSIM jest platformą programową, która gromadzi informacje z różnych urządzeń zabezpieczeń technicznych i systemów informatycznych oraz przedstawia je na wspólnym obrazie sytuacji.

[1] PSIM – Physical Security Information Management, odpowiada polskiemu określeniu Zarządzanie Informacją Bezpieczeństwa Fizycznego.

Kto powinien przemyśleć inwestycję w PSIM?

Z technicznego punktu widzenia rozwiązanie PSIM jest przeznaczone do zintegrowania różnych systemów. Zatem ma sens, jeśli w obiekcie działa kilka systemów, z których sygnały muszą być połączone w celu lepszego zarządzania całością, a także gdy konieczne jest powiększenie istniejących już rozwiązań o nowe produkty lub systemy.

PSIM najczęściej stosuje się w lokalizacjach o znaczeniu krytycznym dla przedsiębiorstwa lub państwa, charakteryzujących się rozległym obszarem i wieloma wdrożonymi systemami. Z tego względu dotyczy głównie infrastruktury krajowej, dużych korporacji, budynków rządowych lub transportu masowego. Coraz częściej PSIM pojawia się jako platforma wspomagająca koncepcję *smart city*. Łącząc informacje pochodzące z analizy obrazów z kamer monitorujących przestrzeń publiczną i systemów zarządzania ruchem, tworzy jednolity obraz sytuacji w czytelnym interfejsie użytkownika.

Chociaż korzyści zapewnione przez PSIM wydają się oczywiste i logiczne, nadal istnieje wiele barier dla jej przyjęcia. Niektóre z nich wynikają z braku aktywnego zaangażowania się stron, które nie chcą rezygnować z kontroli nad swoimi systemami i informacjami; niektóre są wynikiem wcześniejszych niepowodzeń. Dotychczas jednym z największych wyzwań stojących przed rynkiem była dostępność doświadczonych konsultantów i partnerów handlowych.

Wpływ nowych technologii na rozwój PSIM

Popularyzację PSIM w dość szczególny sposób napędza technologia IoT, która w założeniu opiera się na wymianie informacji między wieloma produktami. Oczywiście do tego potrzebna jest platforma zarządzająca. Dzięki otwartej architekturze i technologii PSIM opartej na przeglądarce platforma oprogramowania może szybko łączyć się z niemal każdym urządzeniem, aplikacją i systemem IP przy użyciu otwartych standardów i protokołów, takich jak XML, SOAP, HTTP, SMTP i inne. Platformy PSIM, podobnie jak VMS, obejmują integrację z urządzeniami mobilnymi, umożliwiając podgląd zdarzeń i wpływanie na stany urządzeń i systemów. Rozwiązania takie jak PSIM mogą wykraczać poza zarządzanie zdarzeniami i analizowanie przebiegu zdarzenia post factum. Wykorzystanie analizy w ramach *big data* daje PSIM zdolność predykcyjną, a także strategiczną przewagę w przewidywaniu i przygotowywaniu się na przyszłe incydenty.

> PSIM jest systemem opartym na inteligencji, a nie listą zadań do wykonania, jak w przypadku VMS.

> Wykorzystanie analizy big data daje PSIM zdolność predykcyjną.

PSIM oferuje holistyczne zarządzanie

Korzyści płynące z oprogramowania PSIM, a zwłaszcza jego zdolność do wykorzystania danych z systemów niezwiązanych z bezpieczeństwem sprawiają, że platformy te wykraczają poza bezpieczeństwo fizyczne i zapewniają kompleksowe zarządzanie informacjami. Dobrym przykładem jest zarządzanie w logistyce. System PSIM zapewnia szybką obsługę ruchu kołowego dzięki korelacji danych z systemu rozpoznawania tablic rejestracyjnych z danymi biometrycznymi kierowcy. Kontenery są identyfikowane przez system odczytu numerów na nich, a proces rozpakowywania jest rejestrowany za pomocą kamer – obraz z kamer jest łączony z danymi pochodzącymi z czytników kodów kreskowych. Ponieważ wszystko jest objęte kontrolą systemu, centrum logistyczne ma możliwość dokładniejszego rozliczania klientów, wiedząc, jak długo towar był przechowywany, zanim został wysłany. Takie zastosowania pokazują, jak PSIM pozwala połączyć te różne przepływy pracy w jedną historię.

Zatem VMS czy PSIM?

Nie ma jednoznacznej odpowiedzi na tak postawione pytanie. Wybór zależy bowiem od potrzeb i przyjętych planów bezpieczeństwa obiektu. Należy pamiętać, że VMS stanowi oprogramowanie skoncentrowane na przetwarzaniu danych wizyjnych. I choć obecne systemy VMS realizują wiele dodatkowych funkcji umożliwiających stworzenie czegoś na wzór zintegrowanej platformy zarządzania bezpieczeństwem, to jednak nie będzie to jeszcze PSIM z prawdziwego zdarzenia. Platforma do Zarządzania Informacją Bezpieczeństwa Fizycznego opiera się przede wszystkim na analizie wpływających danych, opracowanych scenariuszach i przepływie pracy dla operatorów. W niektórych przypadkach VMS może być systemem wystarczającym, w innych tylko PSIM. A jeszcze w innych mogą współistnieć oba systemy – VMS jako podsystem PSIM. □

BIO

Jan T. Grusznic

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

Radomir Dębek

Inżynier systemów dozoru wizyjnego z kilkunastoletnim doświadczeniem zdobytym u czołowych europejskich producentów rozwiązań z branży systemów zabezpieczeń. Zrealizował szereg audytów systemów CCTV i wdrożył wiele złożonych ich konfiguracji. Wspiera użytkowników systemów VMS, prowadząc doradztwo projektowe.

LITERATURA

[1] Biuletyn informacyjny Stowarzyszenia „Polalarm", 2/2015.
[2] Israel Gogol: Understanding "Real" PSIM, a&s International, 2014/10/15.
[3] „Bezpieczeństwo dzięki integracji systemów", http://aspolska.pl/bezpieczenstwo-dzieki-integracji-systemow/, 02/04/2019.

Alnet: NetStation Enterprise

NetStation Enterprise to zintegrowana platforma VMS do zarządzania i nadzoru systemów VSS/CCTV, alarmowych, pożarowych, kontroli dostępu oraz innej infrastruktury technicznej obiektu, w tym IoT.

Dane generowane z infrastruktury bezpieczeństwa są rejestrowane w czasie rzeczywistym i udostępniane wszystkim użytkownikom systemu NetStation Enterprise. Duża skalowalność ułatwia jej wdrażanie w obiektach o dowolnej wielkości. NetStation Enterprise jest kompleksowym rozwiązaniem dla sieci sklepów, stacji benzynowych, centrów biurowych, rozległych zakładów przemysłowych czy innych obiektów o znaczeniu krytycznym. System może pracować jako rozwiązanie scentralizowane, obsługujące do 4096 kamer na serwer, albo jako system rozproszony, mający wiele stacji monitoringu o precyzyjnie określonych zadaniach i funkcjach. Jednym z istotnych elementów struktury jest CMS HUB – system oparty na bazie danych SQL, który zbiera wszystkie dane i udostępnia je użytkownikom.

CMS HUB to aplikacja serwerowa przeznaczona do akwizycji danych generowanych przez serwery VMS NetStation oraz systemy alarmowe, pożarowe lub inne współpracuje z serwerami VMS NetStation. Aplikacja pracuje w formie usługi systemowej Windows i obsługuje bazę danych MSSQL. Dane gromadzone w CMS HUB są udostępniane i wizualizowane w aplikacji klienckiej CMS Professional, stanowiącej kombinację intuicyjnej obsługi z wieloma możliwościami konfiguracyjnymi. Elastyczny i modyfikowalny design pozwala na łatwe dostosowanie konfiguracji zarówno do niewielkich, jak i bardzo złożonych instalacji z tysiącami kamer rozmieszczonych w wielu lokacjach. NetStation został również wyposażony w język skryptowy umożliwiający tworzenie zaawansowanych reguł alarmowych. Oprogramowanie NetStation Enterprise ma pełną, dwukierunkową integrację m.in. z systemami Satel, Polon oraz Roger. Dostępne są również dodatkowe moduły NetPOS (monitorowanie kas fiskalnych) i VCA (analityka wideo).

Systemy z minimum 8 kamerami zawierają ANPR (rozpoznawanie numerów tablic rejestracyjnych) w cenie. Dogodną, dalszą rozbudowę systemu umożliwia licencjonowanie na kanał wideo.

Axis Camera Station

Oprogramowanie do zarządzania dozorem wizyjnym Axis Camera Station to idealne rozwiązanie do skutecznego dozoru w małych i średnich instalacjach, takich jak sklepy, hotele, szkoły czy zakłady produkcyjne. System doskonale współpracuje z innymi sieciowymi produktami firmy Axis i wykorzystuje ich funkcje, zapewniając optymalną niezawodność. Oprogramowanie najlepiej sprawdza się w instalacjach do 64 kanałów, których łączne pasmo nie przekracza 512 Mb/s.

Dostępna jest jedna wersja serwerowa oprogramowania, w której zawarte są wszystkie dostępne funkcjonalności. Połączenie z serwerem może być realizowane przez aplikację klienta zainstalowaną na komputerze PC lub na urządzeniu mobilnym opartym na systemie Android lub iOS. Istnieją dwa rodzaje licencji: Core – dla urządzeń Axis oraz Universal – dla urządzeń firm trzecich podłączanych z wykorzystaniem protokołu ONVIF Profil S. Licencje są wydawane na urządzenie, niezależnie od liczby strumieni, jakie generuje. Tak więc kamera 4-przetwornikowa, mimo iż generuje strumienie wideo z czterech niezależnych przetworników obrazu, wymaga tylko jednej licencji. Każde urządzenie można podłączyć do oprogramowania Axis Camera Station na okres testów do 60 dni.

W celu ochrony zapisanych danych użytkownika oprogramowanie Axis Camera Station wspiera architekturę RAID macierzy dyskowych i zasobów sieciowych.

Możliwe jest tworzenie zaawansowanych reguł alarmowych przekazywanych między urządzeniami systemu. Na przykład aktywacja czujnika wstrząsów kamery może wyzwolić nagrywanie alarmowe, ruch sąsiedniej kamery PTZ na pozycje alarmującej kamery, komunikat głosowy z pobliskiego głośnika, blokadę drzwi i włączenie oświetlenia danego regionu. Również informacje z aplikacji analizy zawartości obrazu zainstalowanych bezpośrednio w kamerze, takie jak przekroczenie linii, licznik osób lub rozpoznawanie tablic rejestracyjnych są w stanie wygenerować akcje na dowolnym urządzeniu w systemie oraz wysyłanie komunikatów HTTP do urządzeń firm trzecich i serwerów działających w sieci.

Oprogramowanie Axis Camera Station można uruchomić na wszystkich 64-bitowych systemach Windows, począwszy od Windows 7.

Axxon: Axxon Next

Axxon Next to rozwiązanie VMS w pełni otwarte. Idealnie sprawdzi się tam, gdzie mamy do czynienia z wieloma różnymi markami kamer lub nie chcemy wiązać się z jednym producentem sprzętu: w miejskich systemach monitoringu wizyjnego czy w modernizowanych obiektach przemysłowych i użyteczności publicznej.

Integracja bezpośrednia z kamerami, obsługa protokołu Onvif (profile S, G i T) oraz RTSP zapewniają, że obsłużymy strumienie z niemal każdego urządzenia wideo. Axxon Next posiada zaawansowaną analitykę wideo oraz funkcję inteligentnego przeszukiwania archiwum, umożliwiającą szybkie odnalezienie poszukiwanego nagrania.

Dzięki trzem wersjom licencjonowania produkt jest dopasowany cenowo i skalowalny do wszelkich zastosowań: od najmniejszych systemów po rozbudowane instalacje. Axxon Next Start jest ograniczony do 64 kanałów. Wersja Professional nie ma ograniczeń co do liczby podłączonych kanałów i dodatkowo, za opłatą może być wyposażona w funkcje analityczne: kompresor czasu; rozpoznawanie LPR, detekcja twarzy i Moment Quest. Natomiast wersja Axxon Next Universe, bez ograniczeń co do liczby kamer, oferuje w cenie licencji funkcje: LPR, detekcję twarzy i wyszukiwanie Moment Quest, a ponadto replikację archiwów na kamerach, redundancję serwerową, zarządzanie ścianą wideo i monitoring wielodomenowy.

Axxon Next nie ma limitów pod względem liczby obsługiwanych kamer (oprócz ograniczeń wynikających z licencji). Kalkulator sprzętowy AxxonSoft umożliwia optymalny dobór mocy obliczeniowej dla serwera i stacji roboczej. Oprogramowanie oferuje nadmiarowość zapisu poprzez równoległe strumieniowanie do osobnych archiwów w ramach lokalnego serwera – zapis lokalny do dowolnej liczby archiwów (wraz z zapisem w archiwum zdalnym) oraz zapis lokalny do dowolnej liczby archiwów (wraz z zapisem na serwerze redundantnym). Dostępna jest również automatyczna replikacja nagrań poprzez protokół Onvif-G z pamięci wbudowanych w kamery. Operatorzy systemu sterują kamerami PTZ i zarządzają alarmami wg nadanych priorytetów. Ponadto Axxon Next dzięki kreatorowi makr zapewnia tworzenie zaawansowanych reguł alarmowych w ramach systemu.

Axxon Next wspiera systemy operacyjne: MS Windows Server 2016, MS Windows Vista SP2, MS Windows 10, Linux Debian w wersji 9 lub wyższej.

BCS Manager

Systemy CCTV w ostatnich latach ewoluowały, stając się dostępne nawet dla prywatnych użytkowników. Duża różnorodność oferowanych na polskim rynku rozwiązań często przyprawia instalatorów o ból głowy.

Aplikacja BCS Manager to rozwiązanie dedykowana do obsługi głównie urządzeń marki BCS, ale nie tylko. Obsłuży zarówno małe instalacje składające się z kilku kamer, jak i duże powyżej kilkuset kanałów. Liczba obsługiwanych w systemie kamer zależy od mocy komputera, na którym aplikacja jest zainstalowana. Można wyświetlić jednocześnie nawet kilkanaście ekranów podglądu z dowolnym podziałem. Aplikacja wykorzystuje drugi strumień o niższej rozdzielczości w podglądzie wielu kanałów, a dopiero po zbliżeniu lub wywołaniu jednego okna wyświetla pełną rozdzielczość kanału. W przypadku obsługi urządzeń BCS nie ma ograniczenia co do liczby dodawanych kanałów czy urządzeń. Dodanie urządzenia innego producenta natomiast wymaga odpowiedniej licencji. Licencje aplikacji BCS Manager są związane również z dodatkowymi funkcjami, które aplikacja oferuje. Są wśród nich m.in. obsługa kamer rozpoznających numery tablic rejestracyjnych, moduł porównywania pojazdów czy też wspomagający reklamacje w systemach magazynowych (WMS – *Warehouse Management Systems).*

Odtwarzanie nagrań odbywa się z dedykowanych rejestratorów, w aplikacji natomiast można włączyć funkcję szybkiego odtwarzania, która nagrywa w ustawionym przedziale czasowym strumienie wyświetlane przez użytkownika. Pozwala to bardzo szybko sprawdzić z poziomu podglądu, co działo się w obiekcie kilka minut wcześniej. Przydatną funkcjonalnością jest możliwość tworzenia sekwencji podglądu oraz zadań uruchamianych w dowolnym momencie przez użytkownika. Sekwencje widoków i zadania pozwolą skonfigurować aplikacje tak, aby po uruchomieniu włączyła tylko te kanały, które dany operator chce lub może oglądać. Nadzorowanie alarmów z podłączonych urządzeń pozwala tworzyć scenariusze reakcji na konkretne zdarzenia, wywoływanie podglądu z dowolnych kamer systemu, aktywację wyjść przekaźnikowych w innych urządzeniach, a wszystko może działać zgodnie z ustawionym harmonogramem.

Aplikacją można sterować z poziomu klawiatury sieciowej BCS-P--KN. Jest ona dostępna w wersji x64 i x86 na systemy operacyjne Windows 10, Linux, MacOS.

Bosch Video Management System

Bosch Video Management System to jedno z rozwiązań wchodzących w zakres kompleksowej oferty systemów zabezpieczeń marki Bosch. Jego głównym zadaniem jest sprawne i niezawodne zarządzanie systemami telewizji dozorowej. Program wyróżnia bardzo wysoka skalowalność, dzięki czemu sprawdzi się zarówno w systemach mniejszych, jak i składających się z kilkuset, czy nawet kilku tysięcy kamer – np. w systemach monitoringów miejskich, galeriach handlowych czy obiektach infrastruktury krytycznej.

Dzięki unikalnej architekturze BVMS charakteryzuje się „wbudowaną" niezawodnością – w systemie nie ma pojedynczego punktu potencjalnej awarii, a usterka serwera zarządzającego nadal umożliwia poprawną pracę, aż do czasu jej naprawienia. Funkcja ANR zaimplementowana w kamerach gwarantuje, że nawet w razie problemów z połączeniem sieciowym nagrania będą buforowane na karcie SD, a następnie uzupełnione na podstawowej przestrzeni dyskowej.

Architektura BVMS umożliwia również elastyczną konfigurację systemu i optymalny dobór macierzy dyskowych, w zależności od liczby kamer i wielkości ich strumienia – przy czym pojedyncza macierz dyskowa Bosch gwarantuje poprawną pracę przy strumieniu sumarycznym nawet do 1250 Mb/s.

Bosch Video Management System korzysta również z najnowszych technologii zapewniających wysoką wydajność pracy i obsługi. Wsparcie standardu H.265 oraz inteligentnego strumieniowania kamer Bosch pozwalają na znaczne zmniejszenie ruchu sieciowego i wymaganej przestrzeni dyskowej. Z kolei dekodowanie obrazu przez procesor graficzny GPU zmniejsza zużycie zasobów systemu i umożliwia jednoczesne wyświetlanie wielu obrazów z kamer wysokich rozdzielczości.

W zależności od wielkości systemu, w tym liczby kanałów i stacji roboczych, możliwy jest dobór odpowiedniej wersji licencjonowania serwera: **BVMS Lite** (do 64 kanałów), **BVMS Plus** (do 256 kanałów) lub **BVMS Professional** (do 2000 kanałów). Dla systemów największych lub rozproszonych dostępna jest również wersja **BVMS Enterprise**, która umożliwia zbudowanie jednolitego systemu, zawierającego do 50 podsystemów lub do 10 tys. kamer.

Firma Bosch oferuje również kompleksowe rozwiązanie *all-in-one*, w postaci urządzenia Divar IP 7000, które pełni funkcję zarówno przestrzeni zapisu, jak i serwera zarządzającego.

CBC: GANZ CORTROL

GANZ CORTROL jest uniwersalną platformą VMS obsługującą ponad 4000 modeli kamer IP. Atutem oprogramowania są funkcjonalności dające nowe możliwości wykorzystania systemów monitoringu wizyjnego jako proaktywnego narzędzia do wykrywania zdarzeń i powiadamiania operatora. Dlatego GANZ CORTROL sprawdza się m.in. w profesjonalnych centrach monitoringu wizyjnego.

System jest dostępny w trzech wersjach: PRIME, PREMIER oraz GLOBAL. Bezpłatna wersja **PRIME** to narzędzie dla systemów obsługujących do 16 kamer IP, w tym maks. 8 kamer obcych, innych niż GANZ. Wersja **PREMIER** jest w pełni funkcjonalnym oprogramowaniem przeznaczonym do małych i średnich systemów, zapewniającym nielimitowaną liczbę zdalnych użytkowników. Wersja **GLOBAL** jest kompleksową platformą VMS klasy Enterprise do zarządzania sieciowymi systemami VSS o strukturze rozproszonej. Oferuje różne narzędzia i funkcje, takie jak Video-Wall, replikacja danych, Failover (w tym również Edge Recording zaimplementowany w standardzie Onvif-G), centralne zarządzanie zasobami systemowymi, organizacje hierarchiczne, obsługa Active Directory oraz LDAP.

Przykładowy pojedynczy serwer rejestrujący (CPU: i5 7-gen, 8 GB RAM) bez uruchomionych dodatkowych funkcji analitycznych może obsłużyć 100 kanałów wideo dla kamer 4 Mpix/6 fps.

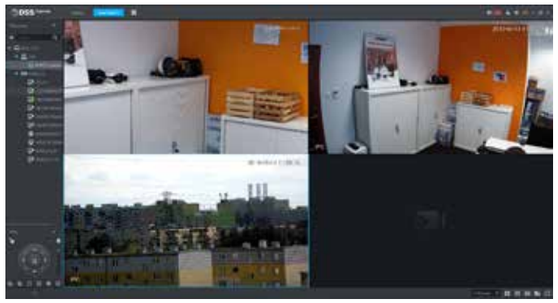
Oprogramowanie jest licencjonowane w zależności od liczby kanałów wideo, z dwuletnim okresem subskrypcji na aktualizację oprogramowania dostępnym domyślnie, z możliwością przedłużenia oraz odnowienia. Moduły dodatkowe typu VCA, FR (identyfikacja twarzy) oraz LPR są licencjonowane na zasadzie paczek kanałów.

GANZ CORTROL Console ma wbudowany kreator i edytor zaawansowanych makr wyzwalanych przez informacje spływające do serwera, takie jak wykrycie ruchu, brak dysku, zasłonięcie obrazu z kamery czy wzbudzenie czujki w systemie alarmowym SATEL. W efekcie można wywoływać jedną lub wiele funkcji (również warunkowych), przesyłać zapytania http, zapisywać log, wysyłać e-maile, wyświetlać obrazy z kamer czy wywoływać skrypt zapisany w pliku BAT.

Każdemu z alarmów i profili PTZ można nadać odpowiedni priorytet. Dzięki temu w przypadku wystąpienia kolizji zdarzeń serwer będzie zawsze wiedział, jaką akcję wykonać.

Wspierane systemy operacyjne: MS Windows Server, Windows 7 i 10 Pro.

Dahua Technology: DSS Pro



Systemy dozoru wizyjnego rozwijają się bardzo szybko, zyskując nowe funkcjonalności. Kamery i rejestratory dostępne dziś na rynku w niczym nie przypominają tych sprzed kilku lat. Rejestrator nie jest już tylko prostym urządzeniem rejestrującym obraz. Obsługa kilkudziesięciu kanałów wizyjnych, zaimplementowana zaawansowana analiza obrazu wsparta algorytmami sztucznej inteligencji (w tym rozpoznawanie twarzy i typu obiektu), algorytmy pozwalające na odczyt tablic rejestracyjnych, a nawet wbudowany switch PoE upraszczający infrastrukturę sieciową – wszystko to jest teraz dostępne w jednym rejestratorze. To pokazuje, że nawet duże i wymagające pod względem funkcjonalności systemy mogą być oparte na NVR-ach

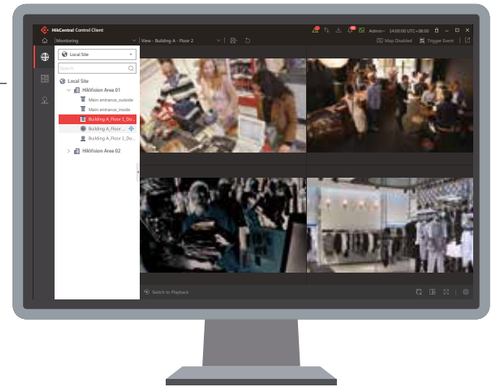
Ale jeśli to nie wystarczy? Jeśli chcemy zbudować większy system lub zarządzać wieloma lokacjami jednocześnie? Odpowiedzią na tego typu potrzeby jest DSS Pro – opracowane przez Dahua Technology oprogramowanie typu VMS. Z jednego miejsca jesteśmy w stanie zarządzać wszystkimi elementami systemu dozoru wizyjnego, m.in. kamerami, rejestratorami, macierzami dyskowymi. DSS Pro zapewnia integrację z rozwiązaniami innych producentów wspierającymi protokół ONVIF. Bardzo często VMS jest stosowany zamiast rejestratorów NVR – w takim przypadku to oprogramowanie DSS Pro jest odpowiedzialne również za rejestrację danych z systemu dozoru wizyjnego. Deklarowana liczba podłączonych kamer do jednego serwera (CPU: 2,4 GHz, 8 GB RAM) nie przekracza 2000. „Twardym" limitem jest przepustowość przypadająca na serwer – 700 Mb/s oraz liczba jednocześnie obsługiwanych serwerów zapisu –20.

W odróżnieniu od systemu opartego wyłącznie na rejestratorach NVR, oprogramowanie DSS Pro dzięki architekturze typu klient-serwer umożliwia dostęp do systemu wielu użytkownikom w tym samym czasie oraz wygodne zarządzanie uprawnieniami dla nich.

VMS pozwoliło też rozwiązać inne ograniczenie rejestratorów, umożliwiając elastyczne wyświetlanie obrazu oraz różnych informacji niezbędnych operatorowi w trakcie pracy. Zazwyczaj rejestrator pozwala na wyświetlanie obrazu na maks. dwóch monitorach. DSS Pro, dzięki dedykowanemu dekoderowi, jest w stanie nie tylko wyświetlać wiele kanałów jednocześnie, ale także obsługiwać wiele monitorów. To sprawia, że VMS jest coraz popularniejszym rozwiązaniem.

Wspierane systemy operacyjne: Centos 6.7 64-bit.

Hikvision: HikCentral



Firma Hikvision nieustannie tworzy i dostarcza kompleksowe rozwiązania dla branży monitoringu wizyjnego. Oprogramowanie HikCentral to profesjonalna platforma służąca do zarządzania obrazem i innymi funkcjami kamer CCTV, dostępna jako oprogramowanie oraz w wersji opartej na serwerze sprzętowym. HikCentral to zupełnie nowa jakość w dziedzinie produktów do systemów dozoru wizyjnego.

Platforma HikCentral jest scentralizowana, oparta na architekturze klient-serwer. Sprawdza się m.in. w takich aplikacjach, jak kompleksy biurowe, ułatwiając realizowanie codziennych zadań związanych z bezpieczeństwem. Jest wyposażona w funkcje: rozpoznawania twarzy, wsparcia dla kontroli dostępu, zarządzania alarmami i podstawową konfigurację alarmów czy zarządzania pojazdami. Dzięki automatycznemu tworzeniu obszarów logicznych na podstawie nazwy urządzeń i synchronizacji harmonogramu nagrywania rozpoczęcie korzystania z oprogramowania jest intuicyjne. Podgląd obrazów na żywo i odtwarzanie jest możliwe z wykorzystaniem funkcji transkodowania (zmiany rozdzielczości materiału przy słabym połączeniu sieciowym) oraz automatycznej lub ręcznej zmiany typu strumienia. HikCentral pozwala na niezależne odtwarzanie archiwum wybranego kanału, przy jednoczesnym podglądzie innego kanału w czasie rzeczywistym w tym samym interfejsie. Szybkie odnalezienie archiwalnych fragmentów wideo umożliwia analiza materiału za pomocą wyszukiwania VCA lub za pomocą wprowadzonych wcześniej znaczników.

HikCentral to jednolita platforma, która oprócz opisanych funkcji dozoru wizyjnego, oferuje integrację z systemami kontroli dostępu, ANPR, współpracę z POS oraz integrację z systemami innych producentów. Pod konkretne zamówienia firma Hikvision, korzystając z otwartych protokołów komunikacji, jest w stanie zaimplementować integrację z innymi systemami bezpieczeństwa (np. system sygnalizacji pożaru)– możliwe jest np. odpowiednie oznakowanie nagrań przy wystąpieniu alarmu pożarowego. Dostępny jest również pakiet narzędzi umożliwiający integrację oprogramowania HikCentral w platformach firm trzecich. Dzięki cyfrowej wymianie danych pomiędzy różnymi systemami budynkowymi można uzyskać efekt synergii i podnieść poziom bezpieczeństwa obiektu.

Axxon Intellect

Axxon Intellect to otwarta platforma PSIM wspomagająca zarządzanie bezpieczeństwem nawet w dużych systemach o skomplikowanej strukturze. Zbudowany na bazie oprogramowania Axxon Intellect integruje systemy telewizji dozorowej, sygnalizacji pożarowej, ochrony obwodowej, kontroli dostępu oraz DSO, przekształcając wiele różnych systemów bezpieczeństwa w jednolity system informacyjny. Axxon Intellect za pomocą zaawansowanych algorytmów poddaje analizie wpływające dane, umożliwiając operatorowi szybką i właściwą reakcję na zdarzenia.

W platformie Axxon Intellect zrezygnowano z klasycznej architektury klient-serwer na rzecz modelu rozproszonego, złożonego z trzech komponentów: serwera, klienta i bramy/routera. Serwery tworzą segment sieciowy o strukturze P2P *(peer-to-peer)*, a wszystkie dane i połączenia są skonfigurowane jako S2S *(server-to-server)* wszędzie, gdzie to możliwe. Stacje klienckie łączą się do jednego bądź wielu serwerów bezpośrednio lub poprzez bramy. Technologia rozproszona przyczynia się do większej niezawodności platformy. W razie uszkodzenia modułu programowego lub zerwania komunikacji Axxon Intellect automatycznie przełącza się do innego działającego serwera.

Axxon Intellect jest dostępne w dwóch wersjach: **Lite** oraz **Enterprise**. Program Lite jest w pełni funkcjonalną wersją programu Axxon Intellect Enterprise, jedynie ograniczoną do obsługi czterech serwerów (wersja Enterprise nie ma ograniczeń liczby podłączonych serwerów), bez limitu liczby podłączonych stacji roboczych lub kamer wideo w systemie. Zapewnia tworzenie zautomatyzowanych skryptów reakcji na zdarzenia, wspiera interaktywną mapę chronionych obiektów i zarządzanie dziennikiem zdarzeń.

Oprogramowanie Axxon Intellect licencjonuje się na podstawie liczby urządzeń podłączonych do systemu – serwerów, kamer i stacji klienckich (w tym urządzeń mobilnych). Opłaty za integracje zależą od rodzaju zintegrowanego rozwiązania i dotyczą najczęściej podpięcia centrali lub kontrolera SKD. Licencjonowaniu nie podlega natomiast liczba podłączonych czujek, map, scenariuszy, makr czy zwizualizowanych punktów.

Axxon Intellect jest rozwiązaniem PSIM, będąc jednocześnie systemem VMS wraz z obsługą zaawansowanych funkcji analizy zawartości obrazu.

Komponent serwerowy Axxon Intellect Enterprise działa obecnie na Windows NT, Linuxie oraz AIXie.

Ela-compil: GEMOS

GEMOS jest neutralną platformą PSIM pozwalającą zintegrować dowolne systemy zarówno z obszaru bezpieczeństwa, jak również komunikacji oraz automatyki budynkowej. Ułatwia to ogromna liczba interfejsów oraz mechanizm CMS *(Content Management System)* umożliwiający dostosowanie konfiguracji systemu do wymagań przyszłego użytkownika. Rozwiązanie jest stosowane w obiektach infrastruktury krytycznej, biurowcach, centrach komunikacyjnych (porty, dworce, lotniska), a także w obiektach wojskowych czy szpitalach. Wśród ponad 270 projektów znajdują się również elektrownie, kopalnie, stadiony, hotele i inne obiekty.

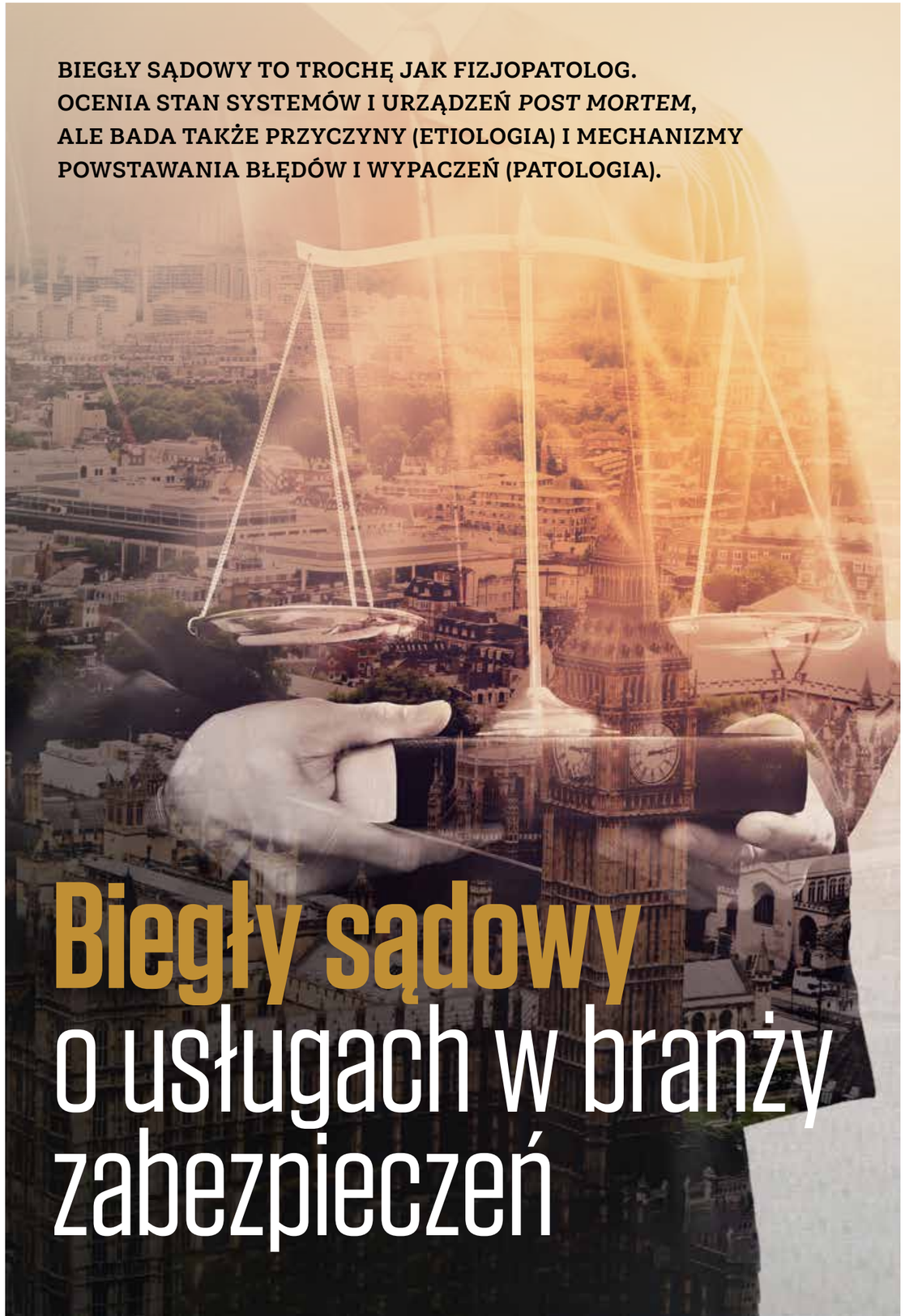
Gemos jest dostępny w czterech wersjach licencyjnych: **Smart** (1 stacja robocza, maks. 1 interfejs, maks. 900 punktów danych), **Light** (2 stacje robocze, maks. 2 interfejsy, maks. 2000 punktów danych), **Standard** (2 lub więcej stacji roboczych, maks. 10 interfejsów, maks. 10 000 punktów danych), **Professional** (2 lub więcej stacji roboczych, nielimitowana liczba interfejsów, punktów danych i procedur). Niezależnie od wersji każda wspiera opcję multimonitor. Dostępna jest również aplikacja mobilna na bazie systemu Android pozwalająca na współpracę z posterunkami mobilnymi (zgłaszanie incydentów, przyjmowanie zadań, kontrola przepustek, nadzór GPS itp.).

GEMOS jest instalowany na serwerze opartym na środowisku MS Windows Serwer albo Linux. Na stacji klienckiej wymagana jest tylko przeglądarka internetowa, dlatego można zastosować dowolny system operacyjny. Jako platforma PSIM jest zintegrowany z wieloma systemami VMS, m.in. Milestone, Genetec, Bosch BVMS, Avigilon ACC, Geutebrück, exacqVision, Mirasys, Macroscop, SeeTec, HikCentral, Dahua, Nuuo, Novus i Alnet.

W GEMOS stworzono blisko 300 interfejsów opartych na protokole komunikacyjnym systemu, z którym można się zintegrować. Integracja po protokole producenckim, sprawia, że interfejsy są powtarzalne i można je stosować na każdym obiekcie, gdzie zainstalowano dany system, niezależnie od skali. Najczęściej stosowane interfejsy dające również największe możliwości integracji, to systemy: telewizji dozorowej, kontroli dostępu, ochrony obwodowej, systemy wykrywania pożaru oraz centrale sterujące urządzeniami ppoż. Dosyć często integruje się także systemy łączności – interkomy, wideodomofony, a także centrale telefoniczne.

System integruje w praktyce urządzenia wszystkich najpopularniejszych marek spotykanych na naszym rynku, a także te nowocześniejsze – systemy kontrolujące i wykrywające drony i radary.

BIEGŁY SĄDOWY TO TROCHĘ JAK FIZJOPATOLOG. OCENIA STAN SYSTEMÓW I URZĄDZEŃ *POST MORTEM*, ALE BADA TAKŻE PRZYCZYNY (ETIOLOGIA) I MECHANIZMY POWSTAWANIA BŁĘDÓW I WYPACZEŃ (PATOLOGIA).



Biegły sądowy o usługach w branży zabezpieczeń

TEKST
Jerzy W. Sobstel

W Polsce sądy oczekują od biegłego jednoznacznego wskazania winnego, aby zająć się tylko wymierzeniem kary. Niekiedy, nie mogąc zorientować się w materii sporu, życzą sobie wręcz prowadzenia dochodzenia i rozpoznania sytuacji przez biegłego. Jednocześnie stosunek wymiaru sprawiedliwości do biegłych sądowych jest, najdelikatniej mówiąc, mało przyjazny. Nie zachęca do podejmowania się tej odpowiedzialnej, ale niekiedy niezbyt przyjemnej funkcji przez specjalistów z najwyższej półki.

Z jakimi sprawami mamy do czynienia?

Sądy, a także prokuratura i CBA przysyłają biegłemu akta różnych spraw, od najdrobniejszych po całkiem spore. Ograniczeniami są w praktyce wielkość i wartość systemów zabezpieczeń technicznych projektowanych i instalowanych w Polsce. Zacznijmy od spraw najmniejszych, chociaż czasami bardzo ważnych i znaczących dla ich uczestników. Są to spory sąsiedzkie, najczęściej o kamery montowane na klatkach schodowych i w garażach, czasami w otoczeniu budynków. I nie chodzi tu o legalność takiego postępowania, RODO czy też naruszanie prywatności, ale o fizyczne uszkadzanie sprzętu, opryskiwanie kamer lakierem lub farbą do włosów. Zgłoszenie takiego zdarzenia policji skutkuje postępowaniem sądowym. Przestaje być wesoło, gdy szczeniacki wybryk kończy się wyrokiem skazującym w sprawie karnej, a skazanym jest np. bankier lub dobrze zarabiający doradca finansowy.

Dużo pracy dostarczają biegłemu firmy prowadzące monitoring systemów sygnalizacji włamania i napadu z ochroną fizyczną. Szczególnie jedna z największych na rynku firm monitorujących ma tak wiele postępowań sądowych – jako pozwana oraz jako powódka – że biegły czasami ma jednocześnie kilka jej spraw na biurku i czuje się tak, jakby był jej pracownikiem etatowym. Gdybym nim jednak był, nie zgodziłbym się na treść umów, jakie firma ta przedstawia do podpisania swoim klientom. Zawierają one tylko dwie konkretne informacje: wysokość abonamentu i czas na podjęcie interwencji. I szereg wyłączeń odpowiedzialności usługodawcy za ewentualne straty powstałe wskutek zdarzenia. Nie wiadomo tylko, czy samo wysłanie patrolu jest już równoznaczne z podjęciem interwencji. Jeżeli operator stacji monitorowania ma 3 minuty na wysłanie patrolu, a ten 15 minut na dojazd do miejsca włamania, to czy interwencja została podjęta po 3, czy też po 18 minutach od wykrycia zdarzenia przez system alarmowy? Włamywacze coraz częściej planują swoją pracę i po 18 minutach nie ma już kogo ani czego szukać. Jeżeli patrol ochrony fizycznej jest jednoosobowy (a nie ma o tym słowa w umowie), to ochroniarz, dla własnego bezpieczeństwa, nie powinien nawet wysiadać z samochodu patrolowego. Zwykle ma on tylko adres obiektu bez jakiegokolwiek szkicu jego usytuowania, więc nawet nie wie, co miałby sprawdzać.

W umowach na monitoring SSWiN, przynajmniej małych i średnich obiektów, próżno szukać parametrów technicznych użytego sprzętu, jakie są określone w normach dotyczących systemów i urządzeń transmisji alarmów [1][2][3]. Usługodawcy nie informują klientów o czasie i metodzie transmisji, monitorowaniu sprawności systemu, o tym, czy transmisja jest jedno-, czy też dwudrogowa, jakie urządzenie transmisji sprzedają lub udostępniają klientowi. Nie ma mowy o certyfikatach, deklaracjach zgodności, CE itd. Jeden z dużych krajowych producentów urządzeń transmisji alarmów stwierdził wręcz, że wszystkie te informacje są tajemnicą jego firmy i żaden instalator dotychczas od niego ich nie żądał. Tym bardziej trudno się spodziewać, aby firmy monitorujące stosowały się do wymagań dotyczących stacji monitorowania zapisanych w normach serii PN-EN 50518. Przy okazji warto przypomnieć, że nowa, zintegrowana i całkowicie zmieniona wersja normy EN 50518: 2019 została już poddana głosowaniu i niebawem zostanie opublikowana. Może wreszcie któraś z dużych firm zdobędzie się na certyfikację swojej stacji?

Gdy dochodzi do włamania i kradzieży w dużym sklepie lub hurtowni, do boju ruszają radcowie prawni obu stron. Stronami sporu zwykle nie są (jak można by się było spodziewać) poszkodowany i firma zabezpieczająca okradziony obiekt, ale firmy ubezpieczeniowe, ponieważ obie strony są ubezpieczone. I wtedy okazuje się, że ubezpieczyciel hurtowni, zawierając umowę, nie sprawdził, jak obiekt jest zabezpieczony albo czy w ogóle jest zabezpieczony. Po drugiej stronie ubezpieczyciel, zawierając ubezpieczenie OC, nie zainteresował się tym, jak działa dostawca systemów zabezpieczeń, czy ma sprzęt i wykwalifikowanych pracowników, czy stosuje się do norm i przepisów. Oczywiście o normie PN-EN 16763 [4] nikt nigdy nie słyszał, a zawiera ona gotową listę kontrolną do sprawdzenia kwalifikacji firmy.

W następujących po sobie, a nawet prowadzonych równocześnie sprawach opiniowanych przez biegłego firma ubezpieczająca obiekt oraz firma ubezpieczająca dostawcę usług, a także ich reasekuratorzy występują naprzemiennie jako powód i pozwany. Wtedy, bez względu na wynik postępowania sądowego, kasa zawsze pozostaje w rodzinie (ubezpieczeniowej), a my za to zapłacimy składkami

Nowa, zintegrowana i całkowicie zmieniona wersja normy EN50518:2019 jest już po głosowaniu i niebawem zostanie opublikowana.

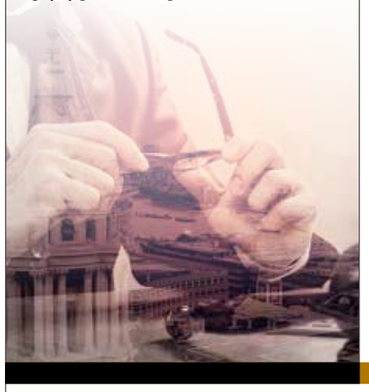
za ubezpieczenie. Trochę się tylko prawnicy i biegli sądowi na tym utuczą, a sądy mają przy każdej takiej sprawie zajęcie co najmniej na trzy lata.
Nie wpływa to niestety ani na poziom zabezpieczeń technicznych obiektów, ani na profesjonalizm usługodawców. Ci ostatni jakby zapomnieli o istnieniu norm europejskich i polskich, zwłaszcza o specyfikacjach technicznych dot. projektowania, instalacji i serwisowania systemów zabezpieczeń technicznych. W opinii biegłego znajomość norm jest obecnie znacznie mniejsza niż dziesięć lat temu, nie mówiąc już o tych dawnych czasach, gdy stosowanie Polskich Norm było obowiązkowe. Obecnie korzystanie z PN, przenoszących normy europejskie lub międzynarodowe, jest wprawdzie dobrowolne, ale ich stosowanie i przywoływanie w dokumentacji świadczy o poziomie technicznym i rzetelności usługodawcy. Jeszcze żadna sędzina, a to one zwykle rozstrzygają w sprawach gospodarczych, nie oparła się argumentacji biegłego dotyczącej oceny rzetelności firmy wywiedzionej ze stosowania lub ignorowania Polskich Norm przez tę firmę. Czasami jest to argument przesądzający o wyroku.

Wyjątkiem są tutaj normy zharmonizowane dotyczące ochrony przeciwpożarowej, których stosowanie jest de facto obligatoryjne. W dodatku wszyscy już chyba wiedzą, że co najmniej od czasu tzw. Elliott case [5] zgodnie z wyrokiem Europejskiego Trybunału Sprawiedliwości europejskie normy zharmonizowane są częścią prawa Unii Europejskiej, a tym samym i prawa krajowego.

Poważnym problemem jest niski poziom wiedzy projektantów zabezpieczeń obiektów małej i średniej wielkości. Skutkuje to nie tylko zaniżeniem poziomu bezpieczeństwa obiektów, ale także ograniczeniem wartości kontraktów, a więc działaniem na szkodę zarówno klienta, usługodawcy, jak i całego środowiska zabezpieczeń technicznych. Projekty są wykonywane schematycznie albo ich w ogóle nie ma, nie przeprowadza się analizy podatności na włamanie. Wszystko to stwarza pole do popisu dla włamywaczy, którzy zwykle mają dużo czasu na „rozpracowanie" obiektu. Są wille, w których wartość pojazdów stojących w garażu przekracza milion złotych, nie wspominając o tym, co wisi na ścianach, a są zabezpieczane jak zwykła budka z piwem. Być może ich właściciele bardziej wierzą w wysokie ubezpieczenie swoich artefaktów niż w porządne ich zabezpieczenie i nie chcą wydawać na system ochrony więcej niż sąsiedzi. Zawsze jednak można ich przekonać, że największą wartością w ich rezydencji są oni sami i że to właśnie ich ma chronić system zabezpieczeń.

Gdy dochodzi do sporu pomiędzy inwestorem a wykonawcą systemu zabezpieczeń technicznych, zazwyczaj jego przyczyny tkwią w specyfikacji technicznej wymagań, na podstawie której doszło do podpisania kontraktu. Zdarza się tak w przypadku zamówień publicznych, w którejś z jego form przewidzianych prawem, przetargów ogłaszanych przez prywatnych inwestorów czy też systemów tworzonych na bezpośrednie zamówienie właściciela obiektu. Przytrafia się to zarówno nowym inwestorom, jak i dużym podmiotom mającym rozbudowane działy bezpieczeństwa, których sama nazwa budzi respekt, a jednak...

Opracowanie dobrej specyfikacji technicznej na nowy system zabezpieczeń złożonego obiektu lub modernizację starego wymaga rozległej wiedzy o aktualnym stanie techniki zabezpieczeń i jej trendach, znajomości zabezpieczanego obiektu, jego podatności oraz możliwych skutkach naruszenia bezpieczeństwa, np. dla ciągłości działania firmy. Wymaga spojrzenia na problem chłodnym okiem z lotu ptaka. Taką perspektywę mogłaby mieć np. zewnętrzna firma doradcza, szczególnie gdyby ponosiła odpowiedzialność materialną za ewentualne błędy w dokumentacji oraz była zobligowana do nadzorowania całego procesu budowy i wdrażania systemu do eksploatacji.
Często jednak specyfikacje wymagań technicznych na urządzenia lub systemy zabezpieczeń są tworzone przez pracowników inwestora, którzy podobne systemy już u siebie mają albo je widzieli na jakichś targach lub w katalogach. Brakuje im szerszej wiedzy i perspektywy, niektóre wymagania są przez nich domyślnie traktowane jako oczywiste, inne powstają ze złożenia opisów systemów znalezionych w katalogach, co prowadzi do niespójności stawianych wymagań. Występują też problemy wynikające z nieznajomości przewidywanych zmian w legislacji lub normalizacji. Specyfikacje są często odmiennie rozumiane przez zamawiającego i usługodawcę. Problem ujawnia się już po podpisaniu kontraktu lub, co gorsza, przy odbiorze systemu.
W przypadku nowych obiektów budowanych w formule „zaprojektuj i zbuduj" systemy zabezpieczeń są widziane przez inwestora gdzieś na dalekim planie (także finansowym), a wymagania techniczne piszą osoby raczej przypadkowe. Zdarza się też, że robi to firma zewnętrzna, ale w przypadku ewidentnych nawet błędów (z czym spotkałem się ostatnio) nie pojawia się ona w postępowaniu sądowym pomiędzy inwestorem a wykonawcą, nawet jako świadek – ani sędzia, ani rzecznicy stron nie mieli do niej żadnych pytań o przyczyny powstania tych błędów.



Kolejnym problemem jest brak koordynacji przy projektowaniu i budowie obiektów. Dotyczy to zarówno współpracy systemów zabezpieczeń z elementami konstrukcji lub z wyposażeniem obiektu, jak i współdziałania systemów elektronicznych ze sobą, np. BMS z systemami zabezpieczeń. Konsekwencje finansowe ponosi zwykle inwestor, ale firmy usługowe tracą czas na poprawki, muszą dłużej czekać na wynagrodzenie lub dopominać się przed sądem zapłaty za wykonaną pracę.

Korzystanie z PN, przenoszących normy europejskie lub międzynarodowe, jest wprawdzie dobrowolne, ale ich stosowanie i przywoływanie w dokumentacji świadczy o poziomie technicznym i rzetelności usługodawcy.

Wizja szybkiego zarobku nie powinna przesłaniać standardowych zasad bezpieczeństwa. Warto poświęcić czas i skorzystać z metody weryfikacji, by zredukować do minimum ryzyko niepowodzenia transakcji.

Specyfikacja techniczna PN-CLC/TS 50131-7 [6] zaleca stosowanie okresu próbnego już po podjęciu praktycznej eksploatacji systemu, a przed ostatecznym rozliczeniem kontraktu. Technikę tę doskonale znamy z życia prywatnego („cyrografy" ślubne niemal zawsze są podpisywane dopiero po pomyślnie zakończonym takim właśnie okresie próbnym). Inwestorzy i usługodawcy, działając w pośpiechu, często unikają zapisów o okresie próbnym. Przeprowadza się jednodniowe szkolenie użytkownika, podpisuje protokół odbioru systemu i... już można iść do kasy. Ale wtedy zaczynają się problemy. Niedouczona obsługa systemu popełnia wszystkie możliwe i nieoczekiwane błędy skutkujące zawieszaniem się lub uszkodzeniami systemu, wysokimi kosztami napraw gwarancyjnych, a nawet postępowaniem sądowym.
Zdarza się, że inwestor (np. z listy wojewody), kupując system za kilka milionów zł, zapomina o etatach dla jego obsługi. Wysyła na szkolenie przypadkowych pracowników, którzy następnego dnia wracają do swoich zajęć. Skutki pojawiają wcześniej lub później i rykoszetem uderzają także w dostawcę systemu. Nie doszłoby do tego, gdyby nabywca był zmuszony przeprowadzić eksploatację próbną przez czas określony w kontrakcie.

W przypadku największych firm, tych z listy wojewody oraz od infrastruktury krytycznej, postępowania prowadzone przez prokuraturę i CBA mają charakter niemal rytualny. Jeżeli były poważniejsze inwestycje w systemy zabezpieczeń technicznych, to po zmianach zarządu z dużym prawdopodobieństwem można oczekiwać postępowania, które będzie wymagało udziału biegłych, czasem nawet kilku. Wszak nowy zarząd musi się odciąć od poczynań starego. Biegli z radością witają zmiany na scenie politycznej, bo za nimi idą zmiany zarządów firm i nowe, duże zlecenia.
W dużych firmach źródło problemu z ich systemami zabezpieczeń technicznych tkwi w sporach kompetencyjnych, np. pomiędzy działami IT a działami bezpieczeństwa. Szefowie firm są rozliczani z zysku, a zabezpieczenia „to przecież tylko koszt" i ich rozbudowa zysków nie przyniesie.

Kim jest biegły sądowy? Co może? Co powinien?

Tak dokładnie to nie wiadomo. Zgodnie z art. 157 § 1 ustawy – Prawo o ustroju sądów powszechnych [8] prezes sądu okręgowego ustanawia biegłych sądowych i prowadzi ich listę. Tyle jest list biegłych, ile sądów okręgowych. Tryb powoływania i odwoływania biegłych jest określony w rozporządzeniu [9] wydanym na podstawie tej ustawy. Od lat mówi się o potrzebie przyjęcia ustawy o biegłych sądowych. Ministerstwo Sprawiedliwości zapowiadało przygotowanie takiej ustawy już w 2016 r. W ub. roku Rzecznik Praw Obywatelskich po raz kolejny zwrócił się do Ministra Sprawiedliwości o przyspieszenie (podjęcie?) prac nad tą ustawą [7]. W piśmie tym czytamy:
Ustawa ta ma zmierzać do uregulowania zagadnień prawnych dotyczących biegłych w jednym akcie normatywnym, uwzględniając kwestie powoływania i weryfikacji kwalifikacji biegłych sądowych w celu zapewnienia obywatelom, których sprawy są rozstrzygane przez sądy powszechne, często w oparciu o opinie biegłych, dostępu do ekspertów o najwyższych kwalifikacjach merytorycznych i etycznych.
Jak wskazuje RPO, sędziowie zbyt często opierają rozstrzygnięcia wyłącznie na opinii biegłych sądowych, bez ich samodzielnej i krytycznej analizy.

W sprawach gospodarczych, z którymi głównie mam do czynienia, sędziowie rzeczywiście opierają się na opinii biegłego, gdyż same są często jak dzieci zagubione we mgle, bez orientacji w przedmiocie sporu i bez zdolności do podjęcia zdroworozsądkowych decyzji, np. o przerwaniu bezsensownego sporu.

Istotne znaczenie ma także zasada kontradyktoryjności procesu. Zgodnie z nią spór toczy się między stronami i na nich spoczywa obowiązek udowodnienia swoich twierdzeń. Sąd jest jedynie obserwatorem i arbitrem, który na koniec procesu wydaje wyrok – skazujący i obciążający kosztami postępowania jedną ze stron. Dlatego też sądy wymagają od biegłych jednoznacznych opinii. Tymczasem w sprawach gospodarczych rzadko mamy do czynienia z sytuacją 27:1, gdy jedna ze stron ma całkowitą rację. Częściej jest to stan 18:10, gdy korzystniejsze byłoby rozwiązanie sporu poprzez „łagodną perswazję sądu" niż skazanie jednej ze stron. Nie pozwala jednak na to zasada kontradyktoryjności postępowania, a w sprawach, które trafiają do sądu, strony najczęściej nie zgadzają się na polubowne rozwiązanie sporu lub postępowanie arbitrażowe.
Rzecznicy stron (zwykle radcowie prawni) często nie pomagają sędziemu w podjęciu decyzji, bo przy całej swojej elokwencji, znajomości prawa i wcześniejszych wyroków sądowych nie potrafią wyłuskać istoty sporu ani nie są zainteresowani jego szybkim zakończeniem. W tej sytuacji opinia biegłego jest dla sędziego ostatnią deską ratunku. Czasami oczekuje on od biegłego nie tylko wydania opinii na podstawie przedstawionych mu akt sprawy, ale także przeprowadzenia działań o charakterze dochodzeniowo-śledczym.

Żeby ten stan zmienić, należałoby raczej pomyśleć o zmianach w procedurze postępowania cywilnego oraz lepszym kształceniu sędziów w zakresie prawa i praktyki gospodarczej, niż stawiać zarzuty biegłym i ograniczać ich prerogatywy. Można mieć wiele zastrzeżeń także do biegłych, szcze-

gólnie do ich kwalifikacji zawodowych. Zdarza mi się pisać opinię w uzupełnieniu już wydanej opinii biegłego lub po odrzuceniu takiej opinii przez sąd. Piszą je czasami osoby przypadkowe, które nie powinny być biegłymi we wskazanej przez siebie dziedzinie. Uważam jednak, że żadne szkolenia kandydatów na biegłych ani procedury weryfikacji ich kwalifikacji zawodowych i certyfikacji nie pomogą, dopóki wynagrodzenie biegłych będzie tak niskie jak obecnie, a stosunek sądów do biegłych – tak nieprzyjazny jak dzisiaj.

Stawka podstawowa wynagrodzenia biegłego wynosi dziś od 22,90 zł do 32,39 zł za godzinę i jest nieco wyższa w przypadku doktorów i profesorów [10][11]. Do czasu pracy biegłego nie wlicza się czasu traconego na dojazd do sądu lub na wizję lokalną, a bywa, że trzeba ją przeprowadzić na drugim końcu Polski. Co ciekawe, sądy powołują się przy tym na dekrety z czasów stalinowskich (dawno anulowane), ignorując rozstrzygnięcia Europejskiego Trybunału Sprawiedliwości w tym zakresie. Sędziowie „wiedzą też lepiej", ile czasu mogło zająć biegłemu przygotowanie opinii. W jednej z opiniowanych ostatnio spraw akta liczyły 960 kart, w tym części opisowe projektów wstępnych, wykonawczych i powykonawczych zaawansowanych systemów zabezpieczeń technicznych, rysunki techniczne na płytach CD, specyfikacje przetargowe, kosztorysy i umowy. Sędzia orzekła, że na zapoznanie się z całym zgromadzonym materiałem, zrobienie notatek itd. potrzeba nie więcej niż 8 godzin. Biegły powinien, wg niej, przeanalizować 120 stron trudnego tekstu w godzinę, nie licząc rysunków.

Złożenie zażalenia na taką decyzję sędziego skutkuje przekazaniem sprawy do wyższej instancji i opóźnieniem wypłaty wynagrodzenia co najmniej o dalsze sześć miesięcy w stosunku do „normalnego" czasu oczekiwania. „Normalny" czas oczekiwania na wypłatę wynagrodzenia za wykonaną pracę i na zwrot poniesionych wydatków (np. na hotel i paliwo) wynosi, w przypadku spraw cywilnych, średnio dziewięć miesięcy. Podatek trzeba jednak zapłacić po wystawieniu fak-

> Od lat mówi się o potrzebie przyjęcia ustawy o biegłych sądowych. MS zapowiadało jej przygotowanie już w 2016 r.

tury. Wysokość kilometrówki wyznacza każdy z prezesów sądów okręgowych z osobna. W Warszawie wynosi ona nie standardowe 0,8358 zł/km, ale 0,60 zł/km. Może biegli i adwokaci w Warszawie korzystają wyłącznie z tańszych w eksploatacji samochodów (albo hulajnóg) elektrycznych?

Sąd „postanawia" powołać biegłego i „wzywa" go do złożenia opinii w określonym terminie. Zwykle są to dwa miesiące, ale zdarza się, że tylko dwa tygodnie. Wraz z „postanowieniem" biegły otrzymuje też „pouczenie", które ma go zmobilizować do pracy. Zgodnie z §5 rozporządzenia [9] biegły nie może odmówić wykonania należących do jego obowiązków czynności w okręgu sądu okręgowego, przy którym został ustanowiony, zleconych przez sąd lub organ prowadzący postępowanie przygotowawcze w sprawach karnych. Usprawiedliwienie niestawiennictwa z powodu choroby wymaga przedstawienia zaświadczenia wystawionego przez lekarza sądowego (art. 177 k.p.k). Informację o tym, gdzie takowego szukać, można podobno znaleźć na tablicy w siedzibie sądu. Za nieusprawiedliwione niestawiennictwo lub za opóźnienie w złożeniu opinii sąd skaże biegłego na grzywnę w kwocie do 10 tys. zł (art. 274 k.p.c.).

Na zakończenie „wisienka na torcie" dla biegłego sądowego, czyli bezpośrednia obrona jego opinii w sali sądowej. Te potyczki słowne z elokwentnymi prawnikami zażarcie broniącymi swoich klientów czasami bywają zabawne, ale nigdy nie są przyjemne. Często zaczynają się od ataku personalnego na biegłego oraz próby podważenia jego kwalifikacji i kompetencji. Niedawno jeden z prawników, dla którego zleceniodawcy opinia biegłego była niekorzystna, pojawił się w sali sądowej z listą dwudziestu czterech pytań „do" i „o" biegłego. Listą przygotowaną przez branżowca, a więc osobę zorientowaną w materii sporu. Na szczęście po uzyskaniu wyczerpującej odpowiedzi na pierwsze pytanie radca prawny zrezygnował z zadawania kolejnych.
Nikt nikomu nie każe być biegłym sądowym, jednak nie atakujcie biegłych zbyt ostro, bo zgodnie z art 157 §3 [8]: ***W związku z wykonywaniem czynności wynikających z postanowienia o zasięgnięciu opinii biegły korzysta z ochrony prawnej przewidzianej dla funkcjonariuszy publicznych.*** □

BIO

Jerzy W. Sobstel

Prezes Stowarzyszenia Ekspertów Normalizacji, Walidacji i Certyfikacji NOWACERT. Od 2004 r. działa w Europejskich Komitetach Normalizacyjnych CEN/TC72, CEN/TC439, CEN/CLC/TC4, CLC/TC79. Przewodniczący Komitetu PKN/KT323 Usługi w ochronie osób i mienia. Właściciel firmy doradczej SOSTEL Jerzy Sobstel.

LITERATURA

1. PN-EN 50136-1:2012 - wersja polska. Systemy alarmowe - Systemy i urządzenia transmisji alarmu - Część 1: Wymagania ogólne dotyczące systemów transmisji alarmu. **2.** PN-EN 50136-2:2014-05 - wersja angielska. Systemy alarmowe - Systemy i urządzenia transmisji alarmu - Część 2: Wymagania dotyczące nadajnika-odbiornika miejsca chronionego (SPT). **3.** PN-EN 50136-3:2014-05 - wersja angielska. Systemy alarmowe - Systemy i urządzenia transmisji alarmu - Część 3: Wymagania dotyczące nadajnika-odbiornika centrum odbiorczego (RCT). **4.** N-EN 16763:2017-04 - wersja angielska Usługi w zakresie systemów ochrony przeciwpożarowej oraz systemów zabezpieczeń technicznych. **5.** EUCJ Elliott case (C-613/14). **6.** PKN-CLC/TS 50131-7:2011 Systemy alarmowe - Systemy sygnalizacji włamania i napadu - Część 7: Wytyczne stosowania. **7.** https://www.rpo.gov.pl/sites/default/files/ **8.** Prawo o ustroju sądów powszechnych (Dz.U. 2001 nr 98 poz. 1070). **9.** Rozporządzenie Ministra Sprawiedliwości z 24 stycznia 2005 r. w sprawie biegłych sądowych (Dz.U. nr 15, poz. 133). **10.** Rozporządzenie Ministra Sprawiedliwości z dnia 24 kwietnia 2013 r. w sprawie określenia stawek wynagrodzenia biegłych, taryf zryczałtowanych oraz sposobu dokumentowania wydatków niezbędnych dla wydania opinii w postępowaniu cywilnym (Dz.U. 2013 r., poz. 518). **11.** Rozporządzenie Ministra Sprawiedliwości z dnia 24 kwietnia 2013 r. w sprawie określenia stawek wynagrodzenia biegłych, taryf zryczałtowanych oraz sposobu dokumentowania wydatków niezbędnych dla wydania opinii w postępowaniu karnym (Dz.U.2017.0.2049).

Instrukcja bezpieczeństwa pożarowego

Kolejny wymagany prawem, niepotrzebny dokument?

T E K S T
Iza Trzeciak

Instrukcja bezpieczeństwa pożarowego zgodnie z rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 7 czerwca 2010 r. [1] ma na celu ustalenie wymagań ochrony przeciwpożarowej w zakresie organizacyjnym, technicznym i porządkowym, jakie należy uwzględnić podczas eksploatacji konkretnego budynku. Zwolnione z tego obowiązku są budynki i strefy pożarowe, w których nie występuje strefa zagrożenia wybuchem, a ponadto:

1) **kubatura brutto budynku lub jego części stanowiącej odrębną strefę pożarową nie przekracza 1000 m³,**
2) **kubatura brutto budynku inwentarskiego nie przekracza 1500 m³,**
3) **powierzchnia strefy pożarowej obiektu innego niż budynek nie przekracza 1000 m².**

W praktyce tylko niewielka część wymienionych budynków i stref pożarowych może skorzystać ze zwolnienia z obowiązku posiadania instrukcji bezpieczeństwa pożarowego. Mogą to być np. strefy pożarowe z lokalami handlowo-usługowymi zlokalizowanymi na parterach budynków mieszkalnych czy niewielkie budynki magazynowe. Warto zauważyć, że opracowania i wdrożenia IBP wymaga się od większości np. kościołów czy szkół, co mogą egzekwować (i coraz częściej to czynią) funkcjonariusze wydziałów kontrolno-rozpoznawczych Państwowej Straży Pożarnej, przeprowadzając w tych obiektach kontrole przestrzegania przepisów przeciwpożarowych.

Co powinna zawierać IBP?

Wspomniane rozporządzenie [1], które nakłada obowiązek opracowania IBP, określa też wyczerpująco zawartość tego dokumentu. Są to następujące informacje:
1. Warunki ochrony przeciwpożarowej wynikające z przeznaczenia, sposobu użytkowania, prowadzonego procesu technologicznego, magazynowania (składowania) i warunków technicznych obiektu, w tym zagrożenia wybuchem.

Warunki ochrony przeciwpożarowej (inaczej operat – WOP) to jeden z najistotniejszych elementów instrukcji opisujący charakterystykę danego obiektu, przyjęte rozwiązania budowlane i instalacyjne. WOP powinien zawierać kilkanaście punktów, wymienionych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 2 grudnia 2015 r. [2] w sprawie uzgadniania projektu budowlanego pod względem ochrony przeciwpożarowej.

Rozporządzenie z 7 czerwca 2010 r. nakłada obowiązek opracowania IBP, określa też wyczerpująco zawartość tego dokumentu.

NA WARUNKI OCHRONY PRZECIWPOŻAROWEJ SKŁADAJĄ SIĘ:

1.1. Informacje o powierzchni, wysokości i liczbie kondygnacji.

1.2. Charakterystyka zagrożenia pożarowego, w tym parametry pożarowe materiałów niebezpiecznych pożarowo, zagrożenia wynikające z procesów technologicznych oraz w zależności od potrzeb charakterystykę pożarów przyjętych do celów projektowych.

1.3. Informacje o kategorii zagrożenia ludzi oraz przewidywanej liczbie osób na każdej kondygnacji i w pomieszczeniach, których drzwi ewakuacyjne powinny otwierać się na zewnątrz pomieszczeń.

1.4. Informacje o przewidywanej gęstości obciążenia ogniowego.

1.5. Ocena zagrożenia wybuchem pomieszczeń oraz przestrzeni zewnętrznych.

1.6. Informacje o klasie odporności pożarowej oraz klasie odporności ogniowej i stopniu rozprzestrzeniania ognia elementów budowlanych.

1.7. Informacje o podziale na strefy pożarowe oraz strefy dymowe.

1.8. Informacje o usytuowaniu ze względu na bezpieczeństwo pożarowe, w tym o odległości od obiektów sąsiadujących.

1.9. Informacje o warunkach i strategii ewakuacji ludzi lub ich uratowania w inny sposób.

1.10. Informacje o sposobie zabezpieczenia przeciwpożarowego instalacji użytkowych, a w szczególności wentylacyjnej, ogrzewczej, gazowej, elektrycznej, teletechnicznej i piorunochronnej.

1.11. Informacje o doborze urządzeń przeciwpożarowych i innych urządzeń służących bezpieczeństwu pożarowemu, dostosowanym do wymagań wynikających z przepisów dotyczących ochrony przeciwpożarowej i przyjętych scenariuszy pożarowych, z podstawową charakterystyką tych urządzeń.

1.12. Informacje o wyposażeniu w gaśnice.

1.13. Informacje o przygotowaniu obiektu budowlanego i terenu do prowadzenia działań ratowniczo-gaśniczych, a w szczególności informacje o drogach pożarowych, zaopatrzeniu w wodę do zewnętrznego gaszenia pożaru oraz o sprzęcie służącym do tych działań.

2. Określenie wyposażenia w wymagane urządzenia przeciwpożarowe i gaśnice oraz sposoby poddawania ich przeglądom technicznym i czynnościom konserwacyjnym.

3. Sposoby postępowania na wypadek pożaru i innego zagrożenia.

4. Sposoby zabezpieczenia prac niebezpiecznych pod względem pożarowym, jeżeli takie prace są przewidywane.

5. Warunki i organizację ewakuacji ludzi oraz praktyczne sposoby ich sprawdzania.

6. Sposoby zapoznania użytkowników obiektu, w tym zatrudnionych pracowników, z przepisami przeciwpożarowymi oraz treścią przedmiotowej instrukcji.

7. Zadania i obowiązki w zakresie ochrony przeciwpożarowej dla osób będących ich stałymi użytkownikami.

8. Plany obiektów, obejmujące także ich usytuowanie, oraz terenu przyległego, z uwzględnieniem graficznych danych dotyczących w szczególności:

a) powierzchni, wysokości i liczby kondygnacji budynku,

b) odległości od obiektów sąsiadujących,

c) parametrów pożarowych występujących substancji palnych,

d) występującej gęstości obciążenia ogniowego w strefie pożarowej lub w strefach pożarowych,

e) kategorii zagrożenia ludzi, przewidywanej liczby osób na każdej kondygnacji i w poszczególnych pomieszczeniach,

f) lokalizacji pomieszczeń i przestrzeni zewnętrznych zaklasyfikowanych jako strefy zagrożenia wybuchem,

g) podziału obiektu na strefy pożarowe,

h) warunków ewakuacji ze wskazaniem kierunków i wyjść ewakuacyjnych,

i) miejsc usytuowania urządzeń przeciwpożarowych i gaśnic, kurków głównych instalacji gazowej, materiałów niebezpiecznych pożarowo oraz miejsc usytuowania elementów sterujących urządzeniami przeciwpożarowymi,

j) wskazania dojść do dźwigów dla ekip ratowniczych,

k) hydrantów zewnętrznych oraz innych źródeł wody do celów przeciwpożarowych,

l) dróg pożarowych i innych dróg dojazdowych, z zaznaczeniem wjazdów na teren ogrodzony.

9. Wskazanie osób/podmiotów opracowujących instrukcję.

Istotnym elementem dla jednostek PSP i użytkownika są plany obiektu, które powinny obejmować rzuty wszystkich kondygnacji i plan terenu.

W przypadku opracowywania instrukcji bezpieczeństwa pożarowego dla budynku nowego określenie warunków ochrony przeciwpożarowej (punkt 1, jaki musi zawierać IBP) jest stosunkowo proste – wszak powyższe punkty muszą znajdować się w projekcie budowlanym, a budynek powinien zostać wykonany zgodnie z nim. Sprawy nieco się komplikują podczas opracowywania instrukcji dla budynku istniejącego, którego dokumentacja budowlana nie przetrwała próby czasu, i trzeba opracować niezbędne informacje jedynie na podstawie wizji lokalnej, wspierając się własną wiedzą i doświadczeniem. Częstym problemem staje się wówczas dylemat – czy określić warunki ochrony ppoż., jakie dany budynek powinien spełniać obecnie, czy opisać stan faktyczny.

Pytanie nie jest bezpodstawne, bo najczęściej w przypadku budynków kilkudziesięcioletnich te dwa opisy nie są tożsame. Jak podejść do tego problemu? Rozważyć cel opracowywania instrukcji! Rozporządzenie [1] określa, że warunki ochrony ppoż. zawarte w IBP dotyczące wskazanych obiektów są przekazywane do właściwego miejscowo komendanta powiatowego (miejskiego) Państwowej Straży Pożarnej w celu ich wykorzystania na potrzeby planowania, organizacji i prowadzenia działań ratowniczych. Ponadto instrukcja bezpieczeństwa pożarowego powinna się znajdować w miejscach dostępnych dla ekip ratowniczych, a sposób jej przechowywania powinien umożliwiać natychmiastowe wykorzystanie na potrzeby prowadzenia działań ratowniczych. Zatem IBP jest opracowywana dla jednostek PSP, dla których ma stanowić zbiór istotnych informacji o budynku i jego otoczeniu w przypadku prowadzenia w nim działań ratowniczo-gaśniczych. Ponadto jest ona dla użytkownika skryptem dotyczącym ochrony przeciwpożarowej użytkowanego budynku. Znajdują się tam podstawowe informacje o obowiązkach użytkownika obiektu, częstotliwościach dokonywania czynności serwisowych urządzeń ppoż., obowiązku organizacji próbnych ewakuacji z budynku, procedurach na wypadek wystąpienia pożaru w budynku.

Istotnym elementem, zarówno dla jednostek PSP, jak i dla użytkownika, są plany obiektu, które powinny obejmować swoim zakresem rzuty wszystkich kondygnacji oraz plan zagospodarowania terenu, z zaznaczeniem informacji istotnych pod kątem ochrony przeciwpożarowej.
Instrukcja bezpieczeństwa pożarowego musi być poddawana okresowej aktualizacji – co najmniej raz na dwa lata, a także po zmianach sposobu użytkowania obiektu lub procesu technologicznego, które wpływają na zmianę warunków ochrony przeciwpożarowej. Remonty i przebudowy zmieniające układ pomieszczeń, mające wpływ na zmianę kierunków ewakuacji, również warto uwzględnić w instrukcji. Aktualne dane o budynku, w szczególności rzuty kondygnacji i plan zagospodarowania terenu, mogą okazać się bardzo przydatne dla strażaków prowadzących działania ratowniczo-gaśnicze. Oby nie były konieczne. □

BIO

Iza Trzeciak

absolwentka Wydziału Inżynierii Bezpieczeństwa Pożarowego w Szkole Głównej Służby Pożarniczej. Założycielka bloga o ochronie przeciwpożarowej blog-ppoz.pl oraz sklepu sklep.blog-ppoz.pl, oferującego min. produkty służące do zabezpieczenia domu przed pożarem. Zawodowo zajmuje się ochroną przeciwpożarową budynków.

LITERATURA

1. 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).

2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 2 grudnia 2015 r. w sprawie uzgadniania projektu budowlanego pod względem ochrony przeciwpożarowej (Dz.U. 2015 poz. 2117).

Zmiany w systemie certyfikacji firm partnerskich

Schrack Seconet Polska

SCHRACK SECONET, JAKO PRODUCENT WYSOKIEJ KLASY SYSTEMÓW BEZPIECZEŃSTWA, OD SAMEGO POCZĄTKU SWOJEJ DZIAŁALNOŚCI W POLSCE SKONCENTROWAŁ SIĘ NA BUDOWIE SIECI AUTORYZOWANYCH PARTNERÓW. POCZĄTKOWO WSZYSTKIE FIRMY WSPÓŁPRACUJĄCE Z PRODUCENTEM (PO PRZEJŚCIU DOŚĆ SKOMPLIKOWANEGO PROCESU AUTORYZACJI) UZYSKIWAŁY CERTYFIKAT AUTORYZACJI, UWIARYGADNIAJĄCY NA RYNKU ZAKRES ICH KOMPETENCJI.

Blisko 10 lat temu producent zdecydował o wprowadzeniu nowej struktury partnerskiej: zakres kompetencji – wynikający z doświadczenia rynkowego – definiował trzy grupy współpracy firm wykonawczych z producentem. Z początkiem 2019 r. wprowadzono kilka zmian w nomenklaturze (m.in. nazewnictwo firm rozpoczynających współpracę) oraz nowe wzory certyfikatów.
Po zakończonym rekordowym wynikiem działalności 2018 roku, mając na uwadze konieczność jeszcze większej koncentracji na najwyższej jakości produktach i usługach, Schrack Seconet Polska przeprowadziła kolejną, istotną modyfikację zasad certyfikacji Partnerów w Polsce.

Rynek zaawansowanych technologicznie systemów bezpieczeństwa (pożarowego) jest coraz większy, tym samym zwiększa się liczba podmiotów działających na tym rynku. Powstają nowe firmy, a młodzi specjaliści coraz chętniej angażują się we współpracę z uznanymi na rynku producentami. Potrzeba zwiększania sprzedaży produktów musi jednak iść w parze z wysoką jakością usług. By tak było, partnerzy producenta świadczący usługi projektowe, instalacyjne, programistyczne oraz serwisu i konserwacji muszą (bezwzględnie) posiadać stosowną wiedzę w zakresie specjalistycznych rozwiązań, uczestniczyć w regularnych szkoleniach, a także posiadać narzędzia umożliwiające poprawne wdrożenia i utrzymanie ciągłości działania oferowanych klientom systemów.

Podstawowa struktura firm partnerskich Schrack Seconet Polska – przedsiębiorstw współpracujących z producentem – od początku 2019 r. wyróżnia trzy grupy kompetencyjne:
- Autoryzowanych Partnerów Wiodących (APW)
- Autoryzowanych Partnerów (AP)
- Partnerów Pre-Autoryzowanych (PPA)

Głównym statusem nadal pozostaje Autoryzowany Partner – firma rzetelna, o dobrej kondycji finansowej, wyposażona w najnowszy pakiet oprogramowania i oryginalny sprzęt serwisowy. Obowiązkiem Autoryzowanych Partnerów jest także posiadanie magazynu części zamiennych oraz profesjonalnych zasobów kadrowych, dzięki czemu mogą oni bez zbędnej zwłoki świadczyć usługi na najwyższym możliwym poziomie satysfakcji klientów. Autoryzowany Partner może pełnić także funkcję dystrybutora produktów Schrack Seconet dla innych firm, niezwiązanych osobnymi umowami z producentem. Podobnie jak w latach poprzednich spośród grona Autoryzowanych Partnerów Schrack Seconet zostały wyróżnione firmy spełniające najbardziej restrykcyjne warunki autoryzacji. Posiadają one status Autoryzowanych Partnerów Wiodących. Firmy te cechują m.in. najwyższa jakość współpracy, bardzo dobra kondycja finansowa, pozytywne wyniki regularnych audytów producenta, wysoko wykwalifikowana kadra specjalistów, najbogatsza w gronie Partnerów Autoryzowanych lista referencyjna zrealizowanych projektów oraz wysoka etyka współpracy.

Tylko Autoryzowani Partnerzy oraz Autoryzowani Partnerzy Wiodący otrzymują certyfikat autoryzacji Schrack Seconet Polska, który odnawiany jest co 2 lata.

Nowością w roku 2019 było stworzenie statusu Partnera Pre-Autoryzowanego, dla firm, które rozpoczynają swoją przygodę z producentem (rozpoczynają proces autoryzacji), albo współpracują ze Schrack Seconet okazjonalnie i nie są zainteresowane utrzymywaniem wysokich rygorów współpracy z producentem w sposób ciągły, a jedynie w trakcie realizacji konkretnych (własnych) projektów. Firmy te nie mają uprawnień producenta do prowadzenia prac programistycznych lub serwisu gwarancyjnego instalacji wykonanych przez innych APW oraz AP, ale mogą (po odbyciu odpowiednich szkoleń) prowadzić samodzielnie cały proces projektowy, wykonawczy i serwisowy instalacji własnych. Firmy te, współpracując z producentem oraz pozostałymi Autoryzowanymi Partnerami, zdobywają doświadczenie w prowadzeniu projektów, instalacji i programowania systemów opartych na produktach Schrack Seconet. Metoda drobnych kroków w tak trudnej branży sprawdza się doskonale, a użytkownicy mogą być pewni, że mają do czynienia z firmami poważnymi, rzetelnymi, wspieranymi przez producenta w konkretnych projektach.
Partnerzy Pre-Autoryzowani są również wyposażeni w najnowszy pakiet oprogramowania oraz posiadają przeszkolony zespół specjalistów – jednak nie muszą spełniać szeregu ważnych dla AP/APW kryteriów autoryzacji czy posiadać magazynu części i materiałów. Korzystają przy tym z pomocy i wsparcia firm z grona AP/APW, co pozwala im realizować swoje projekty w sposób oczekiwany przez użytkowników.

Z uwagi na mniejsze niż w przypadku firm z grona AP/APW doświadczenie w posługiwaniu się produktami Schrack Seconet, firmy z grona PPA nie posiadają certyfikatu autoryzacji, w związku z czym nie angażują się w rozbudowę, zmiany konfiguracji lub serwis gwarancyjny istniejących obiektów i systemów (np. sieciowych) wdrożonych przez innych Partnerów Schrack Seconet. **Zakres ich kompetencji określa Potwierdzenie Pre-Autoryzacji. PPA wspierani są przez producenta w zakresie realizacji nowych inwestycji.** W takich przypadkach, producent (na prośbę PPA) ściśle współpracuje z Partnerem w takim zakresie, jaki jest niezbędny do prawidłowej realizacji projektu i wdrożenia systemu, a także utrzymania i serwisu instalacji w kolejnych latach.

Zmiany we wzorach Certyfikatów

Certyfikaty potwierdzające autoryzację są wydawane wyłącznie dla przedsiębiorstw Autoryzowanych Partnerów (AP) oraz Autoryzowanych Partnerów Wiodących (APW).
Od roku 2019 producent nie wydaje już oddzielnych certyfikatów imiennych dla specjalistów.

Dotychczasowe certyfikaty dla przedsiębiorstw oraz imienne, potwierdzające uprawnienia na poszczególne systemy (sygnalizacji pożarowej, przyzywowe, dźwiękowe systemy ostrzegawcze), zostają zastąpione JEDNYM, DWUSTRONICOWYM certyfikatem wystawionym na konkretną firmę.

Pierwsza strona dokumentu zawiera szczegółowe dane dotyczące przedsiębiorstwa (pełna nazwa, siedziba), numer, datę ważności dokumentu oraz hologram potwierdzający autentyczność dokumentu. Druga strona certyfikatu (załącznik) to szczegółowa tabela rozpoczynająca się od informacji potwierdzających m.in. nazwę przedsiębiorstwa, numer dokumentu oraz datę jego ważności.

Informacje zawarte w załączniku do certyfikatu opisują zakres autoryzacji dla firmy i zakres kompetencji jej poszczególnych specjalistów, w tym:
- rodzaj systemu (SSP, HC, DSO) oraz dokładny jego typ,
- imiona i nazwiska specjalistów przeszkolonych w konkretnym obszarze.

Zamiast certyfikatu imiennego, przeszkolonym pracownikom nadano identyfikator kompetencji będący INDYWIDUALNYM numerem dla każdego specjalisty. Druga strona dokumentu również zostaje potwierdzona hologramem w miejscu, w którym zostały wymienione zdobyte uprawnienia. Specjaliści wymienieni w tabelach certyfikatów to osoby, które odbyły szkolenia w zakresie projektowania, programowania oraz serwisu i konserwacji systemów bezpieczeństwa wyszczególnionych w dokumencie potwierdzającym ich kompetencje. Osoby te są przez producenta wspierane wyłącznie w okresie zatrudnienia w firmie, dla której wydano certyfikat lub potwierdzenie Pre-Autoryzacji.

Dokumenty potwierdzające współpracę z firmami w grupie: Partnerzy Pre-Autoryzowani

Potwierdzenie Pre-Autoryzacji to także dwustronicowy dokument. Podstawową różnicą (oprócz nazwy) jest jego szata graficzna – niepełne obramowanie na obu stronach dokumentu. Podobnie jak w przypadku certyfikatów oryginalny dokument potwierdzający Pre-Autoryzację zawiera:
- dane przedsiębiorstwa, numer, datę ważności oraz hologram oryginału (pierwsza strona),
- zakres Pre-Autoryzacji dla firmy i jej poszczególnych specjalistów (rodzaj systemu i dokładny jego typ, imiona i nazwiska pracowników przeszkolonych w konkretnym obszarze, identyfikator kompetencji będący INDYWIDUALNYM numerem dla każdego przeszkolonego specjalisty). Druga strona dokumentu również zostaje potwierdzona hologramem w miejscu, w którym zostały wymienione zdobyte uprawnienia.

Certyfikaty i zaświadczenia dla firm partnerskich są wydawane czasowo. Ich daty ważności wskazane są na poszczególnych dokumentach. Wszystkie oryginalne certyfikaty APW/AP i potwierdzenia dla PPA posiadają hologramy potwierdzające autentyczność.

Zaświadczenie ze szkolenia projektowego

Zaświadczenia według nowego wzorca (od roku 2019) to dokumenty potwierdzające odbycie podstawowego szkolenia wprowadzającego (produktowo-projektowego). Udział w szkoleniu, a tym samym zaświadczenie nie upoważniają do prowadzenia prac związanych z programowaniem, instalacją oraz serwisem systemów sygnalizacji pożarowej, dźwiękowych systemów ostrzegawczych i systemów przyzywowych Schrack Seconet.

Uzyskanie kompetencji w zakresie każdego systemu oferowanego przez Schrack Seconet wymaga przejścia dedykowanego etapu szkoleń i zdobycia wiedzy w odpowiednim zakresie oraz (często) posiadania odpowiedniego zestawu sprzętu serwisowego lub oprogramowania.

CERTYFIKATY AUTORYZACJI WYDAWANE PRZEZ SCHRACK SECONET MUSZĄ WSKAZYWAĆ WYRAŹNIE ZAKRES PRODUKTOWY, JAKIEGO DOTYCZĄ:
- certyfikaty najnowsze z obszaru SSP / DSO: Integral IP MX, CX, BX, AIRSCREEN ASD 53x, d-LIST, SecoLOG IP, Integral WAN, APS®-APROSYS
- certyfikaty najnowsze z obszaru HC/NC: VISOCALL IP, VISOCALL BASIC, VISOCALL PLUS, VISO-OPT
- certyfikaty w zakresie systemów poprzednich generacji*: BMZ Maxima, BMZ S2L, BMZ Compact, BMZ Integral, Integral Evolution, SecoNET, SecoLOG v. 1.

Zmiany w systemie certyfikacji przedstawia infografika na s. 84.

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

* Utrzymywane są tak długo, jak długo pracownicy przeszkoleni w ich zakresie pozostają zatrudnieni w danej firmie AP/APW.

Zmiany w systemie certyfikacji Partnerów Schrack Seconet w Polsce

Dotychczasowe certyfikaty dla APW/AP* wystawiane dla przedsiębiorstwa oraz imiennie na każdego, przeszkolonego specjalistę (na każdy system osobno) zostają dziś zastąpione JEDNYM, dwustronicowym dokumentem z kompletem informacji.

Certyfikat z ramką w kolorze czerwonym dotyczy systemów sygnalizacji pożarowej oraz DSO z aktualnej oferty producenta: Integral IP MX, CX, BX, czujki zasysającej dymu: AIR SCREEN ASD 53x, czujki liniowej ciepła d-LIST, systemu wizualizacji zdarzeń pożarowych SecoLOG IP V2, sieci rozproszonych Integral WAN powyżej 16 central oraz dźwiękowego systemu ostrzegawczego APS®-APROSYS.

Certyfikat z ramką w kolorze niebieskim dotyczy systemów przyzywowych i komunikacji z aktualnej oferty Schrack Seconet: VISOCALL IP, VISOCALL IP BASIC, VISOCALL PLUS oraz VISO-OPT.

Każdy oryginalny dokument Schrack Seconet posiada okrągły hologram na pierwszej stronie oraz mniejsze, prostokątne hologramy jako potwierdzenie kompetencji na konkretne systemy.

*Autoryzowanego Partnera Wiodącego / Autoryzowanego Partnera

Certyfikat z ramką w kolorze grafitowym dotyczy systemów sygnalizacji pożarowej starszej generacji: BMZ Integral, BMZ Integral C, systemu rozporoszonego SecoNET, BMZ Maxima, BMZ Compact, BMZ S2L oraz systemu wizualizacji zdarzeń SecoLOG IP V1.

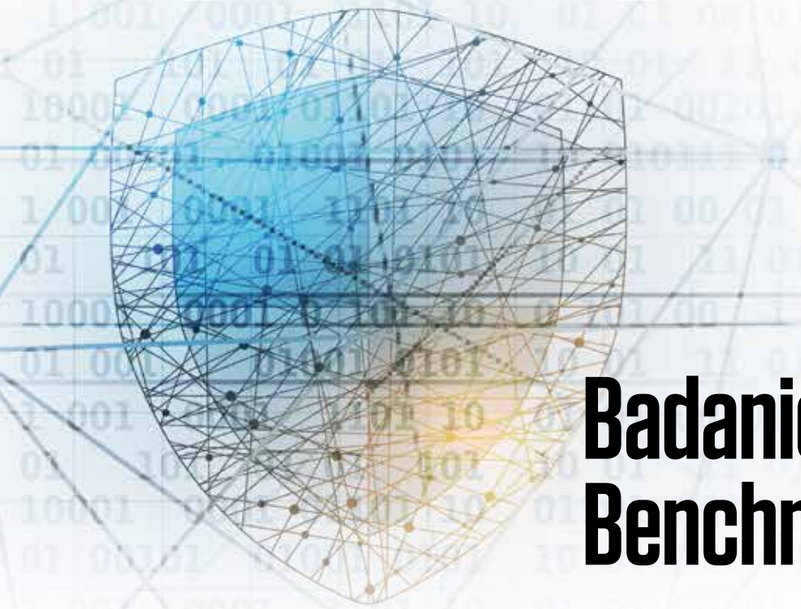
Dotychczasowe zaświadczenia dla PH wystawiane dla przedsiębiorstwa oraz imiennie na każdego przeszkolonego specjalistę (na każdy system osobno) zostają dziś zastąpione JEDNYM, dwustronicowym dokumentem, potwierdzającym zakres i obszary współpracy z **PPA (Partnerami Pre-Autoryzowanymi** – NOWY STATUS PARTNERSKI).

Potwierdzenie preautoryzacji wyróżnia niepełna ramka. Dokument również posiada dwie strony z kompletem informacji o firmie oraz specjalistach przeszkolonych na poszczególne systemy.

Zmiany graficzne dotyczą także dotychczasowego zaświadczenia o odbyciu szkolenia projektowego. Niezmiennie dokument ten nie upoważnia do prowadzenia prac związanych z programowaniem, instalacją oraz serwisem systemów Schrack Seconet.

Schrack Seconet Polska

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



Badanie CISO Benchmark Study

2019: Biznes zwiększa wydatki na analizę ryzyka, technologie i szkolenia z zakresu cyberbezpieczeństwa

Cisco zaprezentowało piątą edycję rocznego raportu CISO Benchmark Study 2019. W badaniu wzięło udział ponad 3000 specjalistów do spraw cyberbezpieczeństwa z 18 krajów świata. Respondenci jako priorytety wskazali konsolidację dostawców rozwiązań cybersec, potrzebę współpracy pomiędzy zespołami zajmującymi się sieciami i cyberbezpieczeństwem, a także konieczność zwiększania świadomości pracowników poprzez ćwiczenia praktyczne.

Wielu specjalistów na stanowiskach *chief information security oficer* (CISO) jest coraz bardziej przekonanych, że migracja do chmury przyczyni się do wzrostu bezpieczeństwa. Na współczesne złożone środowiska cyberbezpieczeństwa często składają się rozwiązania pochodzące od 10 lub większej liczby dostawców, co może wpływać na ich przejrzystość. 65% respondentow przyznaje, że ma trudności z określeniem zakresu naruszeń bezpieczeństwa, ograniczaniem ich wpływu i zapobieganiem im w przyszłości. Nieznane zagrożenia funkcjonujące poza organizacją, które odpowiadają za ataki, wykorzystując błędy użytkowników, dane, urządzenia i aplikacje, również budzą niepokój CISO.

Aby stawić czoła tym wyzwaniom i lepiej chronić swoje organizacje:

- → 44% **respondentów** zwiększyło wydatki na technologie z zakresu bezpieczeństwa,
- → 39% **respondentów** prowadzi szkolenia z zakresu cyberbezpieczeństwa wśród pracowników,
- → 39% **respondentów** koncentruje się na wdrażaniu technik mających na celu redukcję ryzyka wystąpienia cyberataku.

Respondenci zwrócili również uwagę na wciąż bardzo wysokie skutki finansowe cyberataków. Według połowy uczestników badania najpoważniejszy cyberatak wymierzony w ich organizację kosztował nie więcej niż 0,5 mln USD. 45% respondentów zadeklarowało stratę przekraczającą 500 tys. USD, a dla 8% oznaczało to koszt nawet przekraczający 5 mln USD.
W tegorocznej edycji badani, więcej specjalistów na stanowiskach CISO niż kiedykolwiek wcześniej przyznaje, że działa proaktywnie, aby zredukować ryzyko wystąpienia cyberataku. Respondenci deklarują inwestycje w technologie krytyczne dla działania organizacji oraz rozwiązania z zakresu cyberbezpieczeństwa. Wciąż jednak jest wiele do zrobienia – mówi Łukasz Bromirski, dyrektor ds. technologii w Cisco Polska. – *Nie da się zabezpieczyć przed tym, czego nie widać, a specjaliści do spraw cyberbezpieczeństwa wciąż napotykają problemy związane z wglądem w zasoby IT i identyfikowaniem zagrożeń.*

Kluczowe wnioski z raportu wskazują wiele pozytywnych zmian dokonanych w ostatnim roku przez specjalistów ds. bezpieczeństwa

- → **Trend polegający na odchodzeniu od rozwiązań punktowych na rzecz konsolidacji rozwiązań trwa** – w 2017 r. 54% respondentów przyznało, że korzysta z usług 10 lub mniejszej liczby dostawców. W najnowszej edycji badania takiej odpowiedzi udzieliło 63% badanych.
  - W wielu przypadkach, rozwiązania pochodzące od wielu dostawców nie są zintegrowane, co powoduje problemy związane z selekcją i nadawaniem priorytetów alertom i informacjom o incydentach. Badanie wykazało, że nawet ci specjaliści na stanowiskach CISO, którzy zadeklarowali, że korzystają z mniejszej liczby rozwiązań punktowych, mogliby lepiej zarządzać powiadomieniami, gdyby korzystali ze spójnej architektury.

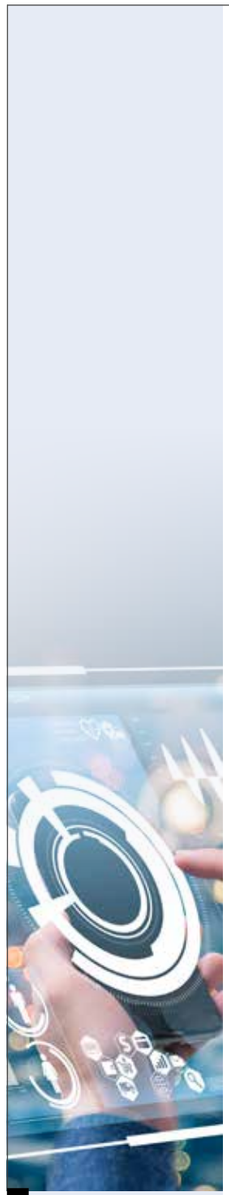
- → **Zespoły, które najbliżej współpracują ze sobą,** odnotowują najmniejsze straty. Eliminacja silosów ma pozytywne skutki finansowe:
  - **95% specjalistów** ds. cyberbezpieczeństwa zadeklarowało, że ich zespoły odpowiadające za sieć i bezpieczeństwo współpracują blisko lub bardzo blisko;
  - **59% respondentów**, którzy wskazali, że ich zespoły odpowiadające za sieć i bezpieczeństwo współpracują blisko lub bardzo blisko, przyznało również, że straty finansowe spowodowane najpoważniejszym atakiem wyniosły mniej niż 100 tys. USD.

- → **Specjaliści ds. cyberbezpieczeństwa** coraz bardziej ufają rozwiązaniom cyberbezpieczeństwa dostarczanym z chmury.
  - **93% specjalistów** na stanowiskach CISO wskazało, że migracja do chmury przyczyniła się do zwiększenia efektywności ich zespołów;
  - **zmalała ocena stopnia trudności** zabezpieczenia infrastruktury chmurowej – w 2019 r. za duże wyzwanie uważało to 52% ankietowanych w porównaniu z 55% w roku 2017.

- → **Cyberzmęczenie** – rozumiane jako porzucenie starań, aby pozostać o krok przed cyberprzestępcami, spadło z 46% w 2018 r. do 30% w 2019 r.

Wojna pomiędzy specjalistami do spraw cyberbezpieczeństwa a cyberprzestępcami jest daleka od zakończenia. Specjaliści Cisco wskazują obszary wymagające poprawy

- → **Pracownicy i użytkownicy** wciąż stanowią najsłabszy punkt systemu zabezpieczeń.
  - Kluczowe jest prowadzenie szkoleń z zakresu cyberbezpieczeństwa mających na celu zwiększenie świadomości już od pierwszego dnia pracy nowych członków zespołu.
  - Tylko 51% respondentów twierdzi, że świetnie sobie radzi z zarządzaniem bezpieczeństwem pracowników w ramach kompleksowych procesów wprowadzenia ich do zespołu, zmiany zespołu czy odejścia z firmy.



- → Poczta e-mail wciąż jest głównym wektorem cyberataków.
  - Phishing i ryzykowne zachowania użytkowników (np. klikanie w podejrzane linki czy odwiedzanie zainfekowanych stron) wciąż stanowią poważny problem dla CISO. Ocena ryzyka wystąpienia tego rodzaju zdarzeń utrzymywała się na podobnym poziomie w ciągu ostatnich trzech lat, wahając się od 56% do 57%.

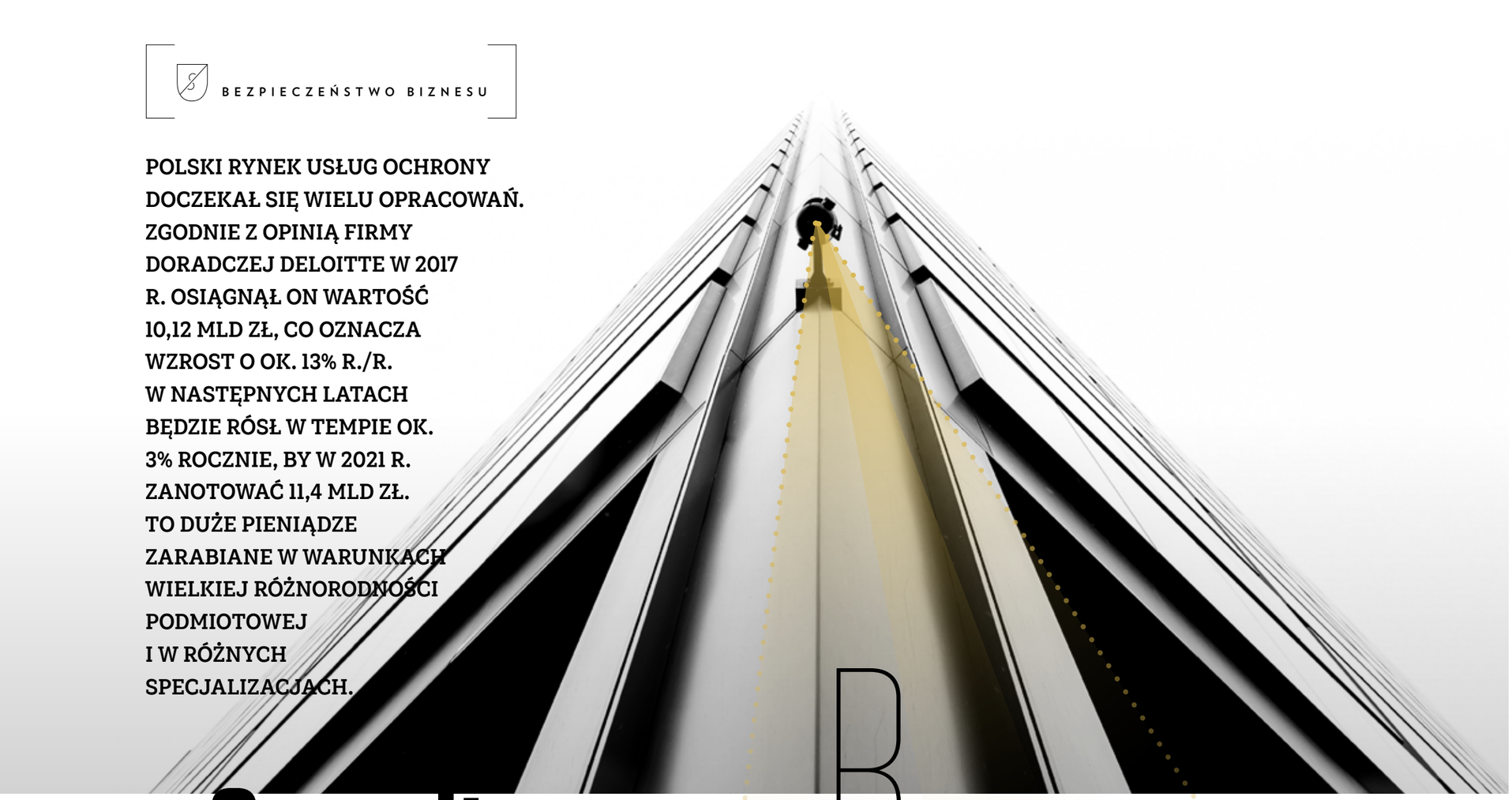
- → **Selekcja alertów bezpieczeństwa i niwelowanie skutków ataku pozostaje wyzwaniem.** Spadek analizowanych i naprawianych alertów z 50,5% w 2018 r. do 42,7% w tym roku budzi niepokój, tym bardziej że dla wielu CISO jest to główny wskaźnik efektywności działań z zakresu cybersecurity.
  - Sposoby oceny poziomu skuteczności cyberbezpieczeństwa wciąż się zmieniają. Liczba respondentów, dla których wskaźnikiem efektywności jest czas wykrycia, spadła średnio z 61% w 2018 r. do 51% w roku 2019. Czas wprowadzenia łatek również ma mniejsze znaczenie, spadek z 57% w 2018 r. do 40% w 2019 r. CISO przywiązują większą wagę do czasu potrzebnego na zniwelowanie skutków cyberataku: 48% odpowiedzi w 2019 r., w porównaniu z 30% w roku 2018.

Rekomendacje dla CISO

- → **Opieranie budżetów cyberbezpieczeństwa** na mierzalnych wynikach działań i praktycznych strategiach oraz ocenie ryzyka. Te elementy powinny wpływać na decyzje zakupowe działów IT, kształtowanie strategii oraz podejmowanie decyzji.
- → **Istnieją sprawdzone procesy,** które organizacje mogą wdrożyć, aby zniwelować ryzyko i zakres cyberataków. Przygotuj swoją organizację poprzez praktyczne ćwiczenia, wprowadź rygorystyczne metody śledcze oraz poznaj optymalne sposoby przywrócenia stabilnego działania po wystąpieniu cyberataku.
- → **Jedynym sposobem, aby zrozumieć rzeczywiste potrzeby** związane z cyberbezpieczeństwem, jest współpraca pomiędzy poszczególnymi działami: IT, sieciowym, bezpieczeństwa oraz ryzyka/zgodności.
- → **Koordynacja reakcji na incydenty** z wykorzystaniem różnych narzędzi, aby płynnie przejść od wykrycia do działania, przy jednoczesnym ograniczeniu działań manualnych.
- → **Połączenie wykrywania zagrożeń** z zabezpieczeniami dostępu, aby stawić czoła zagrożeniom wewnętrznym i móc prowadzić politykę *zero trust.*
- → **Wprowadzenie szkoleń dotyczących** *phishingu,* wieloetapowa autoryzacja, zaawansowane filtry antyspamowe oraz uwierzytelnianiu DMARC, aby zabezpieczyć się przed atakami typu BEC (*Business Email Compromise*). □

Cisco Systems Poland Sp. z o.o.

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



POLSKI RYNEK USŁUG OCHRONY DOCZEKAŁ SIĘ WIELU OPRACOWAŃ. ZGODNIE Z OPINIĄ FIRMY DORADCZEJ DELOITTE W 2017 R. OSIĄGNĄŁ ON WARTOŚĆ 10,12 MLD ZŁ, CO OZNACZA WZROST O OK. 13% R./R. W NASTĘPNYCH LATACH BĘDZIE RÓSŁ W TEMPIE OK. 3% ROCZNIE, BY W 2021 R. ZANOTOWAĆ 11,4 MLD ZŁ. TO DUŻE PIENIĄDZE ZARABIANE W WARUNKACH WIELKIEJ RÓŻNORODNOŚCI PODMIOTOWEJ I W RÓŻNYCH SPECJALIZACJACH.

Security startup dekady,

czyli nowe oblicze bezpieczeństwa Infrastruktury Krytycznej Kraju

TEKST
Jacek Tyburek

Rynek ochrony dzielimy na dwa segmenty – security, obejmujący ochronę fizyczną i monitoring, oraz usługi cash-handlingowe, czyli *obsługę gotówki (przewozy, liczenie, zasilanie bankomatów itp.). Zdecydowanie większy jest segment security. Jego udział w latach 2016-2017 wyniósł ok. 93%* – powiedział Jacek Pogonowski, prezes Konsalnetu podczas XX Debaty Eksperckiej ISBnews i Centrum im. A. Smitha „Branża ochrony w Polsce i na świecie – perspektywy, szanse, zagrożenia", która odbyła się w październiku 2017 r. Wtedy to zaprezentowano ww. raport Deloitte.

Opinia ta nie wyczerpuje pełnego obrazu. Rynek usług ochrony osób i mienia to przede wszystkim rynek obiektów przemysłowych, handlowych, logistycznych, infrastrukturalnych, jednostek wojskowych i innych. Zróżnicowania dopełnia nowy trend, który w ostatnich 10 latach się nasila. Wielkie polskie przedsiębiorstwa stanowiące obszar tzw. przedsiębiorstw strategicznie ważnych dla gospodarki narodowej zaczęły zakładać własne organizacje i zasoby organizacyjne z obszaru bezpieczeństwa i ochrony. W ramach tak definiowanego pojęcia rynku występuje również ochrona obiektów strategicznych z punktu widzenia interesów państwa polskiego. Zjawisko to nie doczekało się jeszcze poważniejszych opracowań analizujących struktury działających firm oraz ich potencjału i możliwości strategicznego rozwoju i konsolidacji.

Firmy ochrony funkcjonujące z sukcesem od wielu lat wywodzą się jeszcze z tradycji Straży Przemysłowych, jak w przypadku Orlen Ochrona czy Straży Pocztowej, która dzisiaj funkcjonuje jako Poczta Polska Pion Ochrony. Obecnie na rynku usług ochrony działa 10 firm zajmujących się bezpieczeństwem, które stanowią (w różnym stopniu) własność Skarbu Państwa. Zdecydowana większość z nich wchodzi w skład grup kapitałowych państwowych koncernów w różnych segmentach, ale są też spółki, które przebranżowiły się z pierwotnej działalności do realizacji misji zapewniania bezpieczeństwa.

Aby wymienić (alfabetycznie) te spółki oraz obszar ich aktywności biznesowych i deklarowanych publicznie, należy zacząć od spółki ACS. Przejęła ona obowiązki wcześniej realizowane przez komercyjne firmy ochrony na terenie portu lotniczego Okęcie. ACS zajmuje się wyłącznie kontrolą pasażerów i bagażu pod nadzorem Straży Granicznej; zapewnia 4-osobową obsadę jednej bramki kontroli bezpieczeństwa. Z kolei patrole, kontrole w strefie ogólnodostępnej oraz obsada bram cargo jest zadaniem Straży Ochrony Lotniska.

Elbest Security to spółka w grupie PGE, której największe obecnie kontrakty stanowią obiekty paliwowo-energetyczne należące do PGE GiEK SA, oraz biurowiec PGE Polska Grupa Energetyczna SA w Warszawie i PGE GiEK S.A. w Bełchatowie. Elbest Security zabezpiecza mecze ekstraklasy piłki nożnej PGE GKS Bełchatów, PlusLigi piłki siatkowej PGE SKRA Bełchatów.

Kolejnym podmiotem wyrastającym z sektora energetycznego jest Energa Ochrona, która konsekwentnie przejmuje ochronę obiektów wchodzących w skład Grupy Energa. Północ kraju jest szczególnie mocno reprezentowana w tej kategorii. Grupa Lotos również powołała własną firmę specjalizującą się w ochronie. Jest nią Lotos Ochrona, która swoje podstawowe zadanie definiuje jako kompleksowe świadczenie usług ochrony osób i mienia na rzecz Grupy Kapitałowej LOTOS SA w zakresie przestrzegania wymogów bezpieczeństwa na terenie chronionym.
Interesującym podmiotem jest Naftor sp. z o.o. Istnieje od 2004 r., kiedy to wydzielono ją ze struktury Naftobazy sp. z o.o. (następnie funkcjonującej jako Operator Logistyczny Paliw Płynnych sp. z o.o.), która była największym w Polsce przedsiębiorstwem specjalizującym się w magazynowaniu i obrocie paliw płynnych.
Celem powołania Naftor sp. z o.o. było zapewnienie profesjonalnej ochrony baz paliw należących do Naftobazy– obiektów strategicznych o kluczowym znaczeniu dla bezpieczeństwa energetycznego państwa. Przez 10 lat funkcjonowania w strukturach Grupy Kapitałowej PERN spółka zdobyła niezbędne doświadczenie w zakresie ochrony fizycznej i technicznej wielkopowierzchniowych obiektów o wysokim stopniu zagrożenia pożarowego i ekologicznego. Naftor rozszerza swoje działania na rzecz Zakładów Azotowych oraz konsekwentnie buduje portfel usług i specjalizacji w różnych obszarach bezpieczeństwa.

W artykule zebrano podstawowe informacje na temat nabierającego znaczenia trendu tworzenia państwowych spółek ochrony.

Na przeciwnym biegunie operacyjnym jest stosunkowo młoda firma JSW Ochrona, która jako spółka koncentruje się obecnie na zabezpieczeniu interesów Grupy Kapitałowej Jastrzębskiej Spółki Węglowej.
Najbardziej ugruntowane na rynku państwowych spółek ochrony są Orlen Ochrona oraz Pion Ochrony Poczty Polskiej. Obie organizacje działają w różnych obszarach, obie przeszły długą drogę od zmilitaryzowanych formacji zorganizowanych wg zasad straży przemysłowych do nowoczesnych firm świadczących usługi na rzecz własnych grup kapitałowych, a coraz częściej wychodzących poza tradycyjne obszary. Obie firmy ze względu na skalę działania oraz zakres geograficzny mają rozwinięte funkcje zarówno operacyjne, wyspecjalizowane w zakresie głównego obszaru odpowiedzialności, jak i coraz lepiej rozwinięte kompetencje zaawansowanego zarządzania ryzykiem.

Na tym tle interesującym przykładem jest Polski Holding Obronny (**PHO**) wyrosły z dawnego Bumaru i będący w 36% udziałowcem Polskiej Grupy Zbrojeniowej (PGZ). Dedykowane państwowemu przemysłowi obronnemu usługi związane z ochroną i bezpieczeństwem zostały uruchomione jako cel strategiczny firmy w 2016r. Aktualnie PHO zapewnia ochronę znacznej części spółek PGZ. Twórca struktury bezpieczeństwa Polskiego Holdingu Obronnego, pomysłodawca i inicjator powstania grupy zrzeszającej najważniejsze państwowe spółki ochrony, Krzysztof Pohorecki tak opisuje powody powstania tego segmentu ochrony strategicznych obszarów państwa: ***W obecnym kształcie branża bezpieczeństwa w Polsce nie daje państwu rękojmi kontroli nad jej funkcjonowaniem. Sytuacja narastającego napięcia międzynarodowego i realne zagrożenia hybrydowe zmuszają najważniejsze organizacje i firmy państwowe do wzięcia odpowiedzialności za własne bezpieczeństwo i zapewnienia sobie pełnej kontroli nad tym krytycznym obszarem działania***. PHO na swojej stronie internetowej informuje o wielu aspektach prowadzonej działalności. Na szczególną uwagę zasługuje projekt „Partnerstwo dla promocji polskiej innowacji i bezpieczeństwa". Ostatnią spółką (w kolejności alfabetycznej) jest Wsparcie Tauron. Firma w Grupie Tauron, podobnie jak inne firmy ochrony w branży energetycznej, koncentruje się obecnie na najwyższej jakości zabezpieczaniu majątku i misji dostawcy energii elektrycznej.

Czytając opracowania Rządowego Centrum Bezpieczeństwa (**RCB**) **na temat ochrony infrastruktury krytycznej** (**IK**), znajdujemy uzasadnienie do przykładania szczególnej wagi do ochrony infrastruktury krytycznej, która pełni kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli. W wyniku zdarzeń spowodowanych siłami natury lub będących konsekwencją działań człowieka IK może być zniszczona, uszkodzona, a jej działanie może ulec zakłóceniu, przez co może być zagrożone życie i mienie obywateli. Równocześnie tego typu wydarzenia negatywnie wpływają na rozwój gospodarczy państwa. Stąd też ochrona infrastruktury krytycznej jest jednym z priorytetów stojących przed administracją państwową. Istota zadań związanych z IK sprowadza się nie tylko do zapewnienia jej ochrony przed zagrożeniami, ale także do tego, aby ewentualne uszkodzenia i zakłócenia w jej funkcjonowaniu były możliwie krótkotrwałe, łatwe do usunięcia i nie wywoływały dodatkowych strat dla obywateli i gospodarki. Ochrona infrastruktury krytycznej obejmuje wszelkie działania zmierzające do zapewnienia jej funkcjonalności, ciągłości działania i integralności mające na celu zapobieganie zagrożeniom, ryzykom lub słabym punktom, ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków i innych zdarzeń zakłócających jej prawidłowe funkcjonowanie.
RCB stworzyło w 2015 r. (z późniejszymi zmianami w 2018 r.) zręby programowe opracowane na zasadzie standardów w postaci Narodowego Programu Infrastruktury Krytycznej. Drugi dokument to „Standardy służące zapewnieniu sprawnego funkcjonowania IK – dobre praktyki i rekomendacje" z tego samego okresu co program narodowy.

OBSZARY INFRASTRUKTURY KRYTYCZNEJ KRAJU WG DEFINICJI RCB	SECURITY SSP DZIAŁAJĄCE W WYMIENIONYCH OBSZARACH
Zaopatrzenie w energię, surowce energetyczne i paliwa	Orlen Ochrona, Lotos Ochrona, Energa Ochrona, JSW Ochrona, Wsparcie Tauron, Naftor
Łączność	Naftor, PHO, Poczta Polska
Sieci teleinformatyczne	PHO
Finansowe	Poczta Polska, Orlen Ochrona, PHO
Zaopatrzenie w żywność	X
Zaopatrzenie w wodę	X
Ochrona zdrowia,	X
Transportowe	Poczta Polska, ACS
Ratownicze	Orlen Ochrona, JSW Ochrona
Zapewniające ciągłość działania administracji publicznej	PHO, Poczta Polska,
Produkcji, składowania, przechowywania oraz stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych	Orlen Ochrona, Lotos Ochrona, Energa Ochrona, JSW Ochrona, Wsparcie Tauron, Naftor

Wymienione wyżej spółki powstawały częściowo przed 2010 r. Połowa z nich została utworzona po 2015 r. Trudno więc dopatrywać się w tym względzie skoordynowanych działań państwa. Nie stawia się tezy (nawet gdyby ktoś próbował to robić, byłoby to z gruntu nieprawdziwe), że państwo świadomie buduje system bezpieczeństwa infrastruktury krytycznej oparty na państwowych podmiotach gospodarczych. Niemniej jednak proces ten wzajemnie się zazębia i nie można się oprzeć wrażeniu, że wraz z rozwojem tych spółek zaczyna on nabierać „substancji" pozwalającej wejść na kolejny etap prac.

W opracowaniach RCB na temat ochrony infrastruktury krytycznej znajdujemy uzasadnienie do przykładania szczególnej wagi do ochrony IK, która pełni kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli.

W tabeli zostały zestawione kategorie wyszczególnione przez RCB jako obszary infrastruktury krytycznej w odniesieniu do zadań deklarowanych przez spółki w oficjalnych publikacjach na swój temat. Widać wyraźnie skupienie uwagi na obszarach, które można by nazwać „twardą infrastrukturą krytyczną", czyli energetyka, paliwa, przy zupełnym pominięciu specjalizacji w zabezpieczeniu infrastruktury związanej z dostawą wody, żywności czy ochroną zdrowia. Te „miękkie" obszary są obsługiwane przez komercyjne firmy ochrony i nie widać na horyzoncie państwowych spółek, które miałyby apetyt na sprawowanie kontroli nad bezpieczeństwem tych sektorów.

Obszar szczególnych interesów strategicznych państwa i model ich ochrony dookreślają również przepisy dotyczące obiektów tzw. obowiązkowej ochrony oraz zapisów ustawy o działaniach antyterrorystycznych. Nie sposób tutaj nie wymienić całego zakresu ochrony, który od czasu do czasu rozpala wyobraźnię zarządów firm ochrony czy bezpieczeństwa jednostek wojskowych i instytucji MON. Jednostki wojskowe to klient specyficzny, ale z poważnym budżetem na poziomie 700 mln zł rocznie. W bezpośrednim zarządzie MON znajdują się również spółki tworzące Polską Grupę Zbrojeniową. Oba te obszary w sposób naturalny są przedmiotem szczególnego zainteresowania Polskiego Holdingu Obronnego, ale również innych spółek z wymienionej listy. Bardzo dużym graczem w sektorze spółek Skarbu Państwa lub posiadających udział Skarbu Państwa jest Agencja Rozwoju Przemysłu. Ten państwowy konglomerat również prowadzi świadomą politykę bezpieczeństwa, która ze względu na wielki obszar podmiotów jest działaniem strategicznym.
Mamy więc do czynienia z kształtowaniem się niezwykle interesującego obrazu rynku usług związanych z bezpieczeństwem. Przy okazji należy zauważyć, że nie ma dobrego punktu odniesienia w innych państwach Unii Europejskiej. Trudno znaleźć dominujący model ochrony podmiotów gospodarczych, zarówno prywatnych, jak i państwowych (tam gdzie mają znaczący udział w rynku), zgodnie z którym można by szukać inspiracji. Wręcz przeciwnie, to właśnie polski model, w którym duże państwowe koncerny lub grupy kapitałowe tworzą wyspecjalizowane podmioty zajmujące się bezpieczeństwem, a jednocześnie działające na w pełni rynkowych zasadach, może stanowić interesującą inspirację.

Każdy, kto zna środowisko menedżerów wyższego szczebla w spółkach Skarbu Państwa będących pracodawcami w branży ochrony, wie, że spotykają się tam zarówno menedżerowie z uznanymi nazwiskami i dokonaniami oraz osoby kontynuujące swoje kariery na rzecz służby państwowej właśnie w tych organizacjach. Być może jesteśmy świadkami budowania systemu, o którym mówi się od wielu lat, czyli prywatyzacji funkcji bezpieczeństwa w formule quasi-prywatnej. Rozumie się przez to prywatyzację, czyli oddanie pola bezpośredniej kontroli nad wrażliwymi obszarami gospodarki przez służby państwowe w ręce podmiotów, które – działając na zasadach rynkowych poprzez swoją strukturę właścicielską, standardy kreowane przez państwo w postaci rekomendacji nieobligatoryjnych, a także litery prawa – dają rękojmię pełnej transparentności i działania zgodnie z wytyczonymi zasadami.
Nie jest moją intencją sugerowanie braku transparentności i rzetelności wszystkich firm komercyjnych na rynku ochrony. Moim celem było zebranie w jednym miejscu podstawowych informacji na temat nabierającego znaczenia trendu tworzenia państwowych spółek ochrony.

W ostatnich 2–3 latach pojawiało się sporo publikacji na temat niepokoju komercyjnych firm ochrony w związku z powstawaniem firm ochrony z sektora Skarbu Państwa. Sporo było niesprawiedliwych w tonie i treści komunikatów na temat tego zjawiska. Tymczasem jesteśmy świadkami tworzenia się organizacji, które mają apetyt na odegranie dużej roli na rynku ochrony, szczególnie w sytuacji przyspieszonych zmian na tym rynku wywołanych rozwojem i rewolucyjnym poszerzeniem dostępności do technologii, wzrostem kosztów pracy ludzkiej i systematycznym zwiększaniem się zagrożeń bezpieczeństwa publicznego.
Sporo jeszcze musi się wydarzyć, żeby eksperyment pod nazwą „sektor bezpieczeństwa państwowych koncernów" stał się komponentem bezpieczeństwa państwa i gospodarki. Zadanie jest, szczerze mówiąc, niezwykle skomplikowane, karkołomne, dla wielu niepokojące, ale sprawiające wrażenie obiecującego.
Obserwujmy to zjawisko, bądźmy krytyczni, jeśli trzeba, ale w ocenach zawsze sprawiedliwi i nastawieni na szersze korzyści. □

BIO

Jacek Tyburek

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

Jakoś(ć) to będzie

BEZPIECZEŃSTWO TO PROCES WPŁYWAJĄCY NA PODSTAWOWĄ DZIAŁALNOŚĆ OPERACYJNĄ ORGANIZACJI. PO CZYM POZNAĆ, ŻE SYSTEM BEZPIECZEŃSTWA W FIRMIE MA WYSOKI POZIOM ALBO NA JAKIM JEST POZIOMIE?

Często zarządzający rozległymi obiektami zadają pytania o to, jaki poziom bezpieczeństwa mają ich systemy (z usługami włącznie). Bez odpowiedniego benchmarku rynkowego określanie tego poziomu jest niewdzięcznym zadaniem.

TEKST
Rafał Łupkowski

Od wielu już lat jestem przekonany, że ocena systemu bezpieczeństwa organizacji jedynie pod kątem realizacji jednej usługi, np. ochrony, jest niewystarczająca i nigdy nie da pełnego obrazu stanu bezpieczeństwa. Niestety uważa się często, że bezpieczeństwo to ochrona lub „kamera", zatem łatwo je zweryfikować – jeśli w ramach oferowanej usługi nie ma reklamacji, a kamery działają, czy to oznacza, że bezpieczeństwo jest na relatywnie wysokim poziomie. Czy na pewno?!

Posłużę się przykładem. W miarę standardowa usługa, np. dwóch pracowników ochrony i pracownik recepcji, kosztuje ok. 0,5 mln zł rocznie. Czy stać nas na „bylejakość" za takie pieniądze? Czy równie łatwo, jak akceptowanie takiego poziomu lub rażącego wręcz niedbalstwa przychodzi nam zarabianie na tak wysokie koszty? W przypadku rozległej struktury wielooddziałowej i zarządzania centralnym usługami i systemami roczne koszty usług ochrony wynoszą już miliony. Czy potrafimy uzasadnić zarządowi dużej spółki, że usługi, za które płacimy, są rzeczywiście na wysokim poziomie? Jeśli nie, pojawia się poważny problem dotyczący podstaw zarządzania bezpieczeństwem.
W ostatnich miesiącach zetknąłem się z przypadkami rażącego wręcz niedbalstwa i „bylejakości" za duże pieniądze. Zastanawia mnie, jak funkcjonuje rynek security, skoro w przypadku incydentów kradzieży, nie badając przyczyn zdarzenia, dokłada się kolejne kamery i zatrudnia nieskuteczną ochronę fizyczną, a jednocześnie nie mając świadomości (lub nie zwracając uwagi), że usługa za np. 700 tys. zł rocznie jest daleka od oczekiwań. „Nie moje, więc nie będę naprawiać świata"? Czy równie łatwo wydalibyśmy własne pieniądze? A może nie mamy oczekiwań?

Czy w obszarze bezpieczeństwa fizycznego jest możliwość badania jakości? Jeśli tak, to jak do tego podejść?
W moim przekonaniu każdy, kto choć kilka lat kierował rozległymi systemami bezpieczeństwa, ma świadomość mało proaktywnego poziomu realizacji usług, zwłaszcza usług ochrony. Uzasadnianie zbyt niskimi stawkami jest wszechobecnym panaceum w kontekście „bylejakości". Dlaczego jednak, wydając setki tysięcy lub miliony złotych, nie egzekwuje się minimum tego, do czego z tytułu umowy wspólnie się zobowiązano?
Często w umowach na świadczenie usług pojawia się zapis o wspólnych cyklicznych przeglądach stanu bezpieczeństwa obiektu realizowanych przez zleceniodawcę i zleceniobiorcę. Po ich przeprowadzeniu powinny powstać wnioski i rekomendacje. Tylko jak często zapis ten jest faktycznie realizowany, a jak często pozostaje nic nieznaczącą treścią w umowie? Przecież bezpieczeństwo to stan, do którego się dąży, który podobnie jak organizacja zmienia się, służąc podstawowej działalności operacyjnej.

Wiele lat temu dotarł do nas zza oceanu termin SLA (*Service Level Agreement*), który w dosłownym tłumaczeniu oznacza „umowę dotyczącą poziomu realizacji usług", czyli innymi słowy parametry umowy określające elementy jakościowe. Takie dość proste narzędzie pozwala na weryfikację poziomu jakości usługi, pod warunkiem że już na początku zostaną określone parametry (wymagania) dotyczące jej realizacji. Jeśli ich brak, warto zastanowić się nad rozpoczęciem postępowania ofertowego.
To samo dotyczy zakupu systemów zabezpieczeń. Coraz częściej spotykam się z sytuacją, że duże postępowania nie opierają się na rzetelnym *security concept* określającym podstawowe funkcje

Rynek ochrony ma spore problemy z rzetelną oceną jakości i jej egzekwowaniem prawdopodobnie dlatego, że nam samym trudno określić wymagania i nazwać ryzyka.

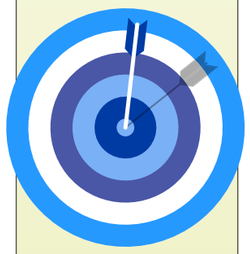
dla urządzeń, systemów i usług, a jedynie ograniczają się do wskazania liczby urządzeń lub stawki za roboczogodzinę bez wyraźnych założeń. Spotkałem się z przypadkami, że systemy zabezpieczeń nie wniosły wartości dodanej już w momencie ich uruchomienia... Czy nasz rynek na to stać?

Co w przypadku już istniejących systemów i podpisanych kontraktów – w jaki sposób podchodzić do kwestii jakościowych? Otóż najlepiej zacząć od podstaw. Jeśli założymy, że w dniu uruchomienia systemu czy usługi można o nim czy o niej zapomnieć, prawdopodobnie w pewnym momencie nie będziemy już zdolni do bezzwłocznej poprawy stanu, np. po incydencie lub w wyniku piętrzących się reklamacji – problem przekroczy dopuszczalny poziom.
Umowy podpisuje się na tzw. złe czasy – dopóki leżą w szafach, a ich strony mają bieżące relacje, dopóty wszystko wydaje się w porządku. Problemy zaczynają się w momencie, gdy zleceniodawca i zleceniobiorca zaczynają „przeciągać" zapisy umowy na swoją stronę – zapowiada to z reguły zerwanie kontraktu, często poprzedzone miesiącami przepychanek i wzajemnych obciążeń, a przecież nie po to umowa była podpisywana.
Zarządzający czy odpowiedzialny za obszar bezpieczeństwa powinien zatem wiedzieć, co jest przedmiotem umów, którymi zawiaduje, i jak są one realizowane. Ta wiedza nie ogranicza się jedynie do badania czasu dojazdu patrolu po uruchomieniu przycisku napadowego, ale także wielu innych elementów kontraktu, które z reguły, nawet jeśli strony nie zawarły załącznika w postaci SLA, występują w samej treści. Przykłady można by mnożyć: od umundurowania pracownika ochrony, poprzez czasy reakcji na usterki serwisowe, po skomplikowane elementy wynikające z gwarancji i rękojmi oraz ubezpieczenia.

Opracowana koncepcja Security Concept pozwala określić poszczególne funkcje, założenia techniczne i parametry usług

Mając tę wiedzę (i na bieżąco z niej korzystając), można badać odchylenia od warunków kontraktu i wpływać na jakość jego realizacji niemal na każdym etapie. Wymaga to jedynie działania nieco ponad stan typu „brak reklamacji równa się wysoka jakość". W strukturach rozległych do realizacji wystarczą relatywnie proste narzędzia, w mniejszych organizacjach warto po prostu wiedzieć, co się „kupiło" i czy to rzeczywiście działa.
Problemem jest często organizacja i wyznaczenie obszarów odpowiedzialności a także możliwości wpływania na proces realizacji poprzez właścicielstwo umowy i możliwość jej egzekwowania. To bardzo ważne, jeśli bowiem obszar merytoryczny jest oderwany od obszaru zakupowego, z reguły nadzór bezpośredni ogranicza się do weryfikacji wysokości faktury, a stwierdzone nieprawidłowości nie znajdują odzwierciedlenia w narzędziach dyscyplinujących, np. karach umownych.
Często zarządzający rozległymi obiektami zadają pytania o to, jaki poziom bezpieczeństwa mają ich systemy (z usługami włącznie). Bez odpowiedniego benchmarku rynkowego określanie tego poziomu jest niewdzięcznym zadaniem. W ostatnim czasie rysuje się wyraźna tendencja do wyrywkowego badania parametrów na zasadzie podobnej do obszaru cybersecurity, czyli tzw. fizycznych testów penetracyjnych, polegających na kontrolowanym złamaniu zasad (uprawnień) dostępu do danego obiektu. Moim zdaniem niewiele mówi to o samym systemie bezpieczeństwa, a jedynie o pewnej jego słabości i podatności na socjotechnikę. Skuteczność systemu bezpieczeństwa nie zależy bowiem tylko od zasad dostępu, ale od wielu aspektów organizacyjnych, w tym konieczności skutecznego zarządzania nim dzień po dniu na podstawie konkretnych czynności kontrolnych badających konkretne obszary.

Proces badania poziomu bezpieczeństwa (jakości) powinien odnosić się do dobrze przygotowanych parametrów określających wcześniej przedmiot zamówienia.



Solidny proces badania poziomu bezpieczeństwa (jakości) powinien bezwzględnie odnosić się do dobrze przygotowanych parametrów określających wcześniej przedmiot zamówienia – z uwzględnieniem specyfiki organizacji. Powinny także zostać określone konkretne mierniki, które w rezultacie ułatwią wskazanie odchyleń i słabych punktów Wcześniej opracowana koncepcja *Security Concept*, która określa poszczególne funkcje, a następnie założenia techniczne i parametry usług, zdecydowanie usprawnia działania. Trudno bowiem byłoby osiągnąć cel w postaci skutecznego i dobrze zarządzanego systemu bezpieczeństwa. Należy podkreślić konieczność zgodności projektu z wymogami prawa (jeśli występują), a także odniesienie jej do realnych potrzeb biznesowych.
Zaryzykuję tezę, że nasz rodzimy rynek ochrony ma spore problemy z rzetelną oceną jakości i jej egzekwowaniem prawdopodobnie dlatego, że nam samym trudno określić wymagania i nazwać ryzyka. Na zmaterializowanie się zagrożeń w ostatnich czasach nie trzeba zbyt długo czekać. Dużą rolę odgrywają także zleceniobiorcy, którzy niejednokrotnie wydają się podejmować wykonanie zadań na zasadzie „do pierwszej faktury", potem „jakoś" to będzie. Z dużą sympatią patrzę na firmy, które chętnie dzielą się wiedzą i niejako odkrywają karty przed zamawiającym, pokazując zarówno mocne, jak i słabe strony rozwiązań. Niestety takie podejście to jeszcze raczej rzadkość.

Warto, aby do kupowanych rozwiązań i usług podchodzić z należytą starannością na każdym etapie ich opracowywania i wdrażania, szczególnie tam, gdzie w grę wchodzą znaczne koszty, a ryzyko związane z niedopasowaniem systemu do realnych potrzeb biznesowych jest znaczące.
Marzy mi się rynek, na którym dostawcy rozwiązań i usług ochronnych wnoszą tylko wartość dodaną, a jasno określone parametry sprawiają, że zarządzanie bezpieczeństwem pozostaje przyjemnością. Na razie jednak mądre kontrolowanie tego, co kupujemy, wydaje się jedynym rozsądnym działaniem. Nie mam jednak wątpliwości, że z upływem lat JAKOŚĆ także i u nas będzie dobrze rozumianym i dostarczanym standardem.

BIO

Rafał Łupkowski

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

Kret w firmie

ASYSTENTKA, NAJLEPSZY MENEDŻER, ZAUFANY PRACOWNIK, NOWA STAŻYSTKA, HANDLOWIEC, KIEROWCA – KAŻDY MOŻE DZIAŁAĆ NA RZECZ TWOJEJ KONKURENCJI. DZIAŁAĆ PRZECIWKO TOBIE I TWOJEJ FIRMIE. JEŚLI SIĘ NIE BRONISZ, JEŚLI TEMU NIE PRZECIWDZIAŁASZ, WIELE TRACISZ. MOŻE JESZCZE NIE TERAZ, MOŻE DOPIERO ZA KILKA DNI. ALE JUŻ DZIŚ MUSISZ WIEDZIEĆ, ŻE TRZEBA SIĘ BRONIĆ I NIE WARTO Z TYM ZWLEKAĆ.

TEKST

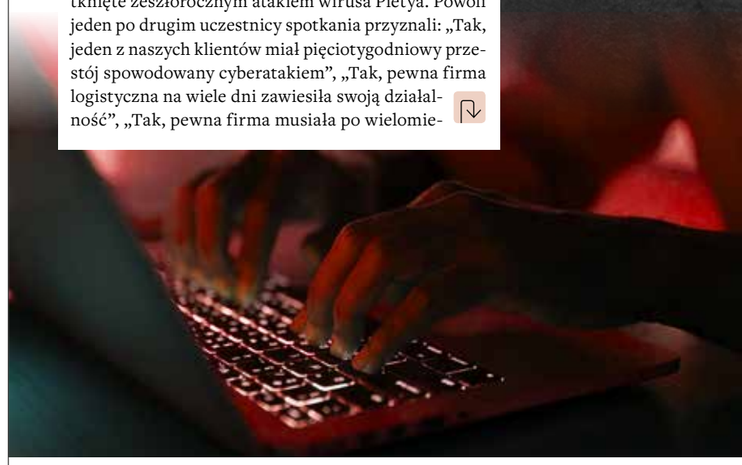
Michał Czuma

Dzisiejszy artykuł chciałbym rozpocząć od pewnej ciekawej historii, która się z nim wiąże.
Ilość spożywanych herbat w ostatniej dekadzie XXI w. spadła znacząco, bo aż o 20%. Często żartuję, że jest to efekt uprzemysłowienia wielu plantacji. Inni uważają, że zmiany klimatu oraz stosowanie pestycydów wpływają w dużym stopniu na zmianę smaku znanych gatunków herbat.
W XIX w. Wielka Brytania uwielbiała herbatę, a dokładnie herbatę i ciasta. Zanim brytyjska firma East India Company na przełomie wieków zdominowała handel herbatą, herbaciany napar był zmonopolizowany przez Chiny. Robert Fortune, szkocki botanik i poszukiwacz przygód, został zatrudniony przez brytyjską East India Company do przemycania wszelkich tajemnic chińskiej herbaty – roślin, nasion itp. z Państwa Środka do rządzonych przez Brytyjczyków Indii. Przebrany ponoć za chińskiego kupca wykradł największe tajemnice chińskiego imperium hedrbacianego. Według Sarah Rose, autorki *For All the Tea in China*, przemyt Roberta Fortune'a i wszystkie czyny z tym związane były największym aktem szpiegostwa korporacyjnego w historii.

W świadomości wielu szefów firm i osób odpowiadających za zarządzanie nimi pojęcie cyberbezpieczeństwa wiąże się wyłącznie z bezpieczeństwem systemów, sieci oraz zastosowanych przez osoby odpowiedzialne za bezpieczeństwo zaawansowanych technologii zabezpieczających sieci firmowe, bazy danych i pocztę korporacyjną przed penetracją zewnętrzną. Wiele osób koncentrowało się na poszukiwaniu swoistego cyber-Graala – systemu, który w sposób najbardziej doskonały zabezpieczyłby ich firmy przed atakiem. Niestety pewne fakty nie zawsze docierają do zainteresowanych.
Najsłabszym ogniwem w całym łańcuchu zabezpieczeń jest człowiek, który siedzi przed monitorem i ma dostęp do systemu. Albo jest gotowy złamać system, gdy ktoś go do tego wynajmie. Pracownik, menedżer, analityk, administrator systemu, osoba odpowiedzialna za stosowane w firmie zabezpieczenia są celem dla tych, którzy szukają słabych punktów w systemie, by je wykorzystać do swoich celów. Niestety podejmuje się niewiele starań o zabezpieczenie tego ogniwa w odróżnieniu od coraz większej troski o IT.

Wielokrotnie w swoich wystąpieniach i tekstach potwierdza to Kevin Mitnick, najbardziej znany na świecie haker, który przyznał, że głównie „łamał" ludzi, a nie hasła. Gdy wchodził do systemów informatycznych takich gigantów technologicznych, jak Nokia, Fujitsu czy Sun, częściej dokonywał tego dzięki chwytom socjotechnicznym, a nie wiedzy informatycznej. Zwykle wystarczyło, że po zdobyciu numeru telefonu dzwonił do administratora systemu i przedstawiwszy się jako menedżer nowego projektu, który nie może się zalogować na swoje konto, uzyskiwał dostęp do interesujących go danych. Wiedza, jaką zdobywał od lekceważących procedury asystentek, stażystów czy pracowników niższego szczebla, wystarczyła, by uzyskać najważniejsze informacje strzeżone przez sprzęt i oprogramowanie kosztujące często setki milionów dolarów.
W tym miejscu każdy powinien zastanowić się nad tym, czy w jego firmie są informacje, które nie powinny trafić w niepowołane ręce, np. do konkurencji, jej klientów czy kontrahentów albo opinii publicznej. Pewne informacje, które dla jednych mogą być nieistotne, ale dla innych mają duże znaczenie.

Podczas śniadania organizowanego przez a&s Polska, na które zostali zaproszeni dostawcy rozwiązań security oraz ich klienci – firmy logistyczne i produkcyjne, ze strony przedstawiciela jednej z globalnych marek z branży FMCG (dobra szybkozbywalne) padło pytanie, czy ktoś słyszał o cyberatakach, które w ostatnim czasie dotknęły ich firmy w Polsce. Obserwowałem uczestników, gdyż zapadła kłopotliwa cisza. Mam świadomość, że prawie 90% polskich firm jest słabo chronione przed penetracją ze strony hakerów lub osób parających się szpiegostwem gospodarczym. Zainicjowałem dyskusję, podając listę firm, które zostały dotknięte zeszłorocznym atakiem wirusa Pietya. Powoli jeden po drugim uczestnicy spotkania przyznali: „Tak, jeden z naszych klientów miał pięciotygodniowy przestój spowodowany cyberatakiem", „Tak, pewna firma logistyczna na wiele dni zawiesiła swoją działalność", „Tak, pewna firma musiała po wielomie-



Kevin Mitnick, najbardziej znany na świecie haker, przyznał, że głównie „łamał" ludzi, a nie hasła.

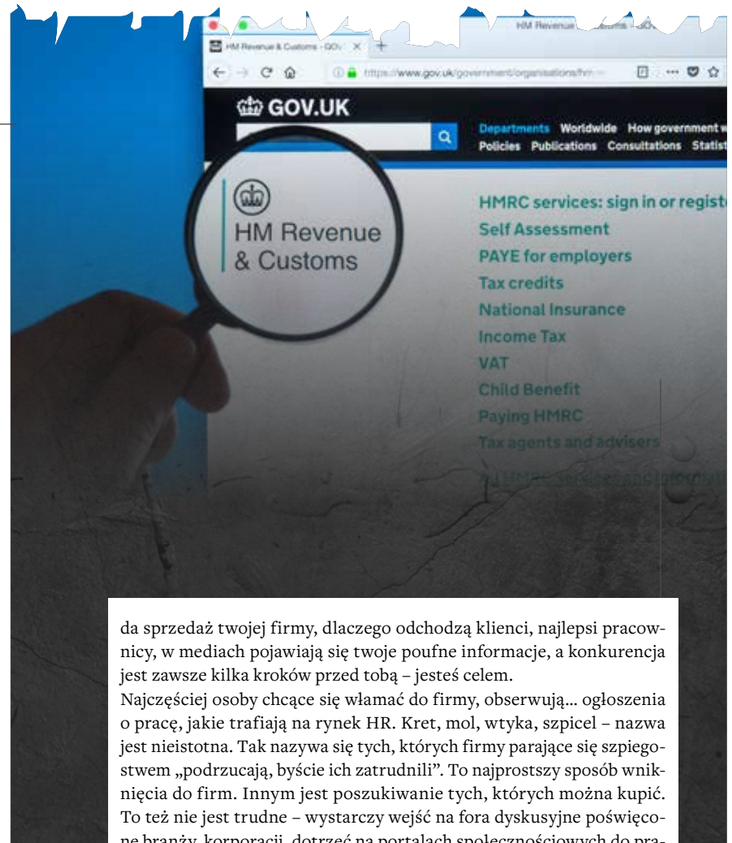
sięcznym ataku rozwiązać poważne problemy". I padło kilka informacji o skutecznych atakach. To zapewne uzmysłowiło zadającemu pytanie i wszystkim obecnym, że biznes w Polsce ma dzisiaj spory problem. Potwierdziło się, że firmy najsłabiej chronią swoje zasoby, wiedzę, tajemnice, natomiast pilnie strzegą tylko tej tajemnicy, że... grasował w nich haker albo szpieg. Zapewne większość firm nawet nie wie, „jak wyciekają" z nich cenne dane.
Dzisiaj szpiegostwo i działania hakerów są zbieżne – jedni i drudzy starają się przełamać zabezpieczenia, by uzyskać dojście do systemu, informacji i ludzi, by później zrobić z nich tylko sobie znany użytek. Zablokowanie systemu jest równoznaczne z zablokowaniem firmy, zawieszeniem albo utrudnieniem jej działania i daniem przewagi innym. Haker czy szpieg zawsze mają cel i jeśli podejmują ryzyko zagrożone wieloma latami więzienia, nie jest to zabawa czy chęć zaimponowania dziewczynie lub kolegom. Obecnie można przyjąć, że jedyna różnica pomiędzy cyberatakiem mającym na celu wykradzenie danych a działalnością szpiegowską polega na tym, iż część hakerów w szantażu okradzionej z danych firmy widzi główny cel zarobków. Częściej do szantażu przystępuje po tym, gdy konkurencja okradzionego nie wyraziła zainteresowania zakupem wykradzionych danych. W szpiegostwie gospodarczym firma lub organizacja wynajmuje bądź zatrudnia ekspertów, w tym hakerów, w celu uzyskania określonych informacji od konkurencji. Gdy prześledzi się najgłośniejsze afery związane w wykradzeniem danych, okazuje się, że wszystko zaczyna się od przeglądania śmieci wyrzucanych z firmy.

Od lat obserwujemy szybki postęp technologiczny, a mimo wszystko skandal polegający na próbie szpiegowania przez Procter & Gamble (P&G) swojego rywala w dziedzinie pielęgnacji włosów – spółki Unilever do dzisiaj wydaje się czymś wyjątkowym. Procter & Gamble nie dokonało żadnego wielkiego wyczynu, nie zastosowało drogiego sprzętu do nagrywania setek różnych linii telefonicznych należących do Unilever, nie penetrowało systemów firmy armią hakerów – to nie był „Cyber-Pearl Harbor". W 2001 roku „agenci operacyjni" P&G, udając śmieciowych „nurków z wysypiska", przeczesywali śmieci Unilever w poszukiwaniu informacji i danych (w tym wszelkich nośników danych), które mogłyby umożliwić firmie zdobycie przewagi nad konkurentem. Cała operacja trwała ponad sześć miesięcy, a agenci zdobyli prawie 80 stron poufnych dokumentów ze śmietnika z biura Unilever w Chicago.
Jak ujawnił „New York Times", Procter & Gamble zapłacił Unileverowi 10 mln USD zadośćuczynienia i zgodził się na przeprowadzenie audytu zewnętrznego w celu pełnego wyjaśnienia afery szpiegowskiej. – To był niefortunny incydent – powiedział John E. Pepper, prezes firmy. – Działania te nie były zgodne z zasadami i polityką P&G.

Technologia utrudnia osobom nieuczciwym dostęp do wiedzy i zasobów firm, ale sposób postępowania z technologią czasami zdumiewa. Wysypiska śmieci wciąż są przeszukiwane pod kątem wyrzucanych dysków twardych czy starych urządzeń elektronicznych – bo nieodpowiedzialność jednych jest źródłem bogactwa innych. Ci, których interesują nasze zasoby informacyjne, rzadko próbują je sami przełamać. Ale firma, będąca ich celem, musi korzystać z danych i wiedzy gromadzonej w systemach, dlatego szpiedzy i hakerzy wykorzystują ludzkie słabości, ich psychikę oraz wiedzę o ludziach, ich nieuwagę, lekceważące podejście do procedur, by poprzez nich dotrzeć do zasobów firmy. To jest dzisiaj o wiele łatwiejsze i tańsze.

Najsłabszym ogniwem w całym łańcuchu zabezpieczeń jest człowiek, który siedzi przed monitorem i ma dostęp do systemu – pracownik, menedżer, analityk, administrator, osoba odpowiedzialna za zabezpieczenia

Problem szpiegostwa gospodarczego dotyczy właściwie wszystkich firm. Każde przedsiębiorstwo powinno założyć, że poza dozwolonym obiegiem informacji istnieje też ten nielegalny i dane trafiają do tego, kto więcej za nie zapłaci. Zdrady często z prozaicznych powodów może się dopuścić nawet najbardziej zaufany pracownik. Nieudany biurowy romans może w konsekwencji kosztować firmę dziesiątki milionów dolrów. Wszystko jest kwestią ceny i świadomości samego pracownika. Bo wielu pracowników może nawet nie wiedzieć, iż jest nieświadomym źródłem informacji dla konkurencji. Jeśli z gabinetu ginie laptop lub smartfon, a nie zginęły inne cenne rzeczy, możesz być niemal pewien, że jesteś na celowniku. Jeśli ktoś próbował włamać się do twojego mieszkania, ale nic nie zginęło, możesz być czyimś celem. Jeśli widzisz porozrzucane śmieci koło twoich koszy, ktoś pakował worki z dokumentami albo wprost złożył ci ofertę, że będzie odbierał makulaturę z twojej firmy w atrakcyjnej cenie, jesteś na celowniku. Jeśli nie wiesz, dlaczego spadała sprzedaż twojej firmy, dlaczego odchodzą klienci, najlepsi pracownicy, w mediach pojawiają się twoje poufne informacje, a konkurencja jest zawsze kilka kroków przed tobą – jesteś celem.



Najczęściej osoby chcące się włamać do firmy, obserwują... ogłoszenia o pracę, jakie trafiają na rynek HR. Kret, mol, wtyka, szpicel – nazwa jest nieistotna. Tak nazywa się tych, których firmy parające się szpiegostwem „podrzucają, byście ich zatrudnili". To najprostszy sposób wniknięcia do firm. Innym jest poszukiwanie tych, których można kupić. To też nie jest trudne – wystarczy wejść na fora dyskusyjne poświęcone branży, korporacji, dotrzeć na portalach społecznościowych do pracowników dzielących się swoimi emocjami z całym światem. Potem tylko kilka prostych zabiegów socjotechnicznych, by menedżer pominięty przy awansie lub podwyżkach, asystentka, handlowiec czy technik, który ma nieukrywane pretensje, albo zaufany pracownik, który ma jakąś słabość, coś ukrywa przed firmą, bo się tego wstydzi – wszystkie te osoby przez umiejętnego speca od pozyskiwania takich źródeł informacji mogą zostać zamienione w „krety" pracujące na rzecz konkurencji. Ostatni „kret", jakiego ujawniłem w jednej z firm, był uzależniony od osoby ze świata przestępczego. Wędrował z jednej firmy do drugiej tylko po to, by pomóc w wyłudzeniach. W ciągu roku udało mu się w dwóch firmach wyłudzić ponad 13 mln zł. Czy było warto? Tym, którzy go „podrzucali" – tak, tym, którzy go potem zwalniali – nie.

Wyrafinowani hakerzy i szpiedzy rzadko pozostawiają po sobie wystarczająco obciążające dowody, aby ich złapano. Mark Lanterman, dyrektor ds. technologii w Computer Forensic Services, szacuje, że jest to mniej niż 1% wszystkich parających się tą profesją. W ciągu ostatnich kilku lat doszło do kilku głośnych ataków cybernetycznych na firmy, w tym Target, Home Depot i Sony, które dają pewien obraz sytuacji. Jeszcze więcej firm zostało ofiarami szpiegostwa gospodarczego. Począwszy od 2006 r., czyli od rozpoczęcia zbierania danych o atakach na firmy, 70 firm, rządów i organizacji non profit zostało zhakowanych, a szpiedzy kontynuowali zbieranie informacji przez kolejne lata. Te trwające ataki cybernetyczne zostały po raz pierwszy zgłoszone przez Dmitrija Alperovitcha i od tego czasu nazwano je *Operation Shady Rat*.

W 2009 r. hakerzy ukradli zastrzeżone informacje z amerykańskich i europejskich firm energetycznych Exxon Mobil, Royal Dutch, Shell i BP. Zhakowano ich poufne mapy topograficzne. Te skomputeryzowane mapy lokalizują potencjalne rezerwy ropy naftowej, a wg śledczych atak doprowadził do utraty „informacji o finansowaniu projektów w odniesieniu do ofert i operacji dotyczących pól naftowych i gazowych". Ten atak został nazwany „Nocnym Smokiem". I chociaż wskazuje się, że Operation Shady Rat i Night Dragon pochodzą „głównie" z Chin, informacje te nigdy nie zostały zweryfikowane. Wiele podobnych ataków na korporacje zachodnie nie przez przypadek zwróciło uwagę na chińskie korporacje technologiczne i znane nam oskarżenia kierowane pod adresem m.in. koncernu Huawei są skutkiem m.in. tego rodzaju „wycieków".

Ochrona związana z prawem autorskim i ochroną patentową ma za zadanie chronić interesy firm. Ale szpiegostwo korporacyjne było dla wielu kolejnym wielowymiarowym sposobem prowadzenia działalności gospodarczej. Właśnie oferowane w Darknecie usługi hakerskie, po które bez większych oporów sięgają poszukujące zysków firmy detektywistyczne, oraz zakładane przez byłych oficerów służb prywatne agencje wywiadowcze, wciąż próbują zdobyć tajemnice handlowe, oferując swoje usługi tym, którzy chętnie zapłacą za informacje dające im często znaczną przewagę konkurencyjną. Niezmiernie rzadko firmy bezpośrednio wzajemnie się hakują – najczęściej poprzez sieć pośredników docierają do osób prowadzących działalność szpiegowską, by ukryć swoje powiązania. Często zajmują się tym agencje detektywistyczne. Dla wielu firm tego typu zlecenia są tylko kwestią pieniędzy.
Coraz więcej firm, które zetknęły się bezpośrednio z działalnością szpiegowską albo były celem ataków i penetracji ze strony szpiegów lub hakerów, wynajmują ekspertów, którzy chronią firmy przed tego typu działaniami. Firmy, które odczuły ataki, bez wahania sięgają po ekspertów od kontrwywiadu kor-

Dzisiaj szpiegostwo i działania hakerów są zbieżne – jedni i drudzy starają się przełamać zabezpieczenia, by uzyskać dojście do systemu, informacji i ludzi, by później zrobić z nich użytek.

poracyjnego i tworzą komórki antyfraudowe, rozbudowując ich zadania o działania wzmacniające ludzki czynnik swojej infrastruktury. Wiedzą, że jest to „dobre dla biznesu". Jednocześnie, nawet jeśli jest naprawdę niewielki odsetek szansy na złapanie hakerów, szpiegów, pracujących w firmach „kretów" i ich mocodawców, firmy coraz chętniej zmieniają swoją taktykę, zwłaszcza gdy dowiadują się, ile i co stracili inni, gdy zbagatelizowali problem. Metody ataków są coraz bardziej przemyślane, ale metody przeciwdziałania im i ich wykrywania też do prostych nie należą. Ale na pewno warto po nie sięgać.

Na początku XXI wieku Doliną Krzemową wstrząsnęła afera, w której wykorzystano w działaniach korporacyjnych swoiste gry szpiegowskie. W 2000 roku Larry Ellison, szef Oracle, starał się udowodnić, iż konkurencyjny Microsoft finansuje różne grupy interesu publicznego. Oracle nazwał nawet swoją decyzję o zatrudnieniu agencji detektywistycznej działaniem w ramach prowadzonej „służby publicznej". Próbując odkryć rzekome powiązania finansowe pomiędzy Microsoftem a jego rzekomymi niezależnymi sojusznikami, agencja detektywistyczna Investigative Group International przekupiła personel sprzątający, by zdobyć wszelkie dokumenty, jakie trafiły w ręce sprzątających. Próbowali również kupić śmieci biurowe ze wszystkich biur Microsoftu. Mimo że prowadzone działania przekroczyły pewną granicę działań etycznych, większość kadry kierowniczej w innych firmach dochodzeniowych zatrudnionych przez Larry'ego Ellisona stwierdziła, że nie przekroczono granic prawnych.

Coraz więcej firm, które zetknęły się bezpośrednio z działalnością szpiegowską albo były celem ataków i penetracji ze strony szpiegów lub hakerów, wynajmują ekspertów, którzy chronią firmy przed tego typu działaniami.

W 1997 r. Pin Yen Yang, prezes firmy Four Pillars Enterprise Company na Tajwanie, został oskarżony o oszustwa pocztowe, oszustwa związane z praniem brudnych pieniędzy, przejmowanie skradzionej własności oraz kradzież tajemnic handlowych od Avery Dennison Corp., jednego z największych amerykańskich producentów produktów klejących w latach 1989–1997. Yang zapłacił pracownikowi Avery Dennison, doktorowi Ten Hong Lee, 150 000–160 000 USD za dane badawcze i poufne informacje dotyczące produkcji. Avery Dennison Corp. szacuje, że skradziona technologia klejenia kosztowała ich dziesiątki milionów dolarów straconych przychodów.

Innym przypadkiem, który warto przytoczyć, jest historia z kwietnia 2009 r. Sieć hoteli Starwood Hotels & Resorts Worldwide wniosła pozew sądowy przeciwko Hiltonowi i oskarżyła ten koncern hotelowy o działania szpiegowskie, zmuszając sieć do zaprzestania rozwoju swojej marki Denizen. W pozwie twierdzono, że dwóch byłych dyrektorów Starwood zatrudnionych przez Hiltona ukradło ponad 100 tys. poufnych dokumentów. Zawierały one informacje o sieci Starwood i zgodnie z pozwem miały być wykorzystane do pomocy Hiltonowi w replikacji niszowej marki Starwood w hotelach typu lifestyle. Według Starwood „ładunek ciężarówek" z dokumentami zdobytymi przez konkurenta zawierał „informacje poufne z punktu widzenia konkurencji". Sieci hotelowe zawarły porozumienie w 2010 r. Hilton zgodził się na zapłatę w gotówce zadośćuczynienia w wysokości 75 mln USD na rzecz Starwood, a sędzia federalny zakazał sieci hoteli marki Hilton otwierania jakichkolwiek „hoteli typu lifestyle" przez dwa lata.

To tylko kilka przykładów z dziesiątek spraw, które poznała opinia publiczna. Chociaż nieco już trącą myszką, podobne incydenty już w szerszym zakresie i mocniej wsparte technologią są prowadzone wobec innych firm i korporacji w kraju i za granicą także dzisiaj. Przed wieloma centrami technologicznymi i logistycznymi montuje się ukryte kamery liczące i namierzające samochody przywożące i wywożące ładunki. Często do obserwacji używa się dronów. W ten sposób konkurencja otrzymuje dokładne dane o produkcji i sprzedaży oraz sieci dystrybucyjnej ofiary.

W Darknecie wynajmuje się hakerów, którzy kradną zawartość skrzynek pocztowych, billingi telefoniczne konkretnych menedżerów wybranych firm. Wielu kluczowych menedżerów jest stale inwigilowanych, dane o ich działaniach i kontaktach oraz treść ich rozmów są spisywane i analizowane, by trafiać w postaci raportów do zarządów konkurencyjnych firm. Wiele firm dokładnie analizuje ogłoszenia o firmowych eventach, by wysłać tam swoich zaufanych agentów. W sieci pojawiają się tysiące ogłoszeń pracy na konkretne stanowiska, gdzie fikcyjne agencje HR polują na CV zawierające dane konkretnych menedżerów, osób zatrudnianych w konkretnych strukturach konkretnych firm. Do wielu menedżerów dzwonią wynajęte i nieświadome faktu ich wykorzystania firmy headhunterskie. A później w ramach rozmów kwalifikacyjnych wydobywa się najskrytsze tajemnice firmowe.

Asystentka, najlepszy menedżer, zaufany pracownik, nowa stażystka, handlowiec, kierowca – każdy może działać na rzecz twojej konkurencji. Działać przeciwko tobie i twojej firmie. Jeśli się nie bronisz, jeśli temu nie przeciwdziałasz, wiele tracisz. Może jeszcze nie teraz, może dopiero za kilka dni. Ale już dziś musisz wiedzieć, że trzeba się bronić i nie warto z tym zwlekać. □

BIO

Michał Czuma

Niezależny ekspert, prowadzący własną działalność doradczą pod nazwą Michał Czuma MC Consulting. Stworzył i zarządzał pierwszymi w kraju Biurami Antyfraudowymi w spółkach grupy PKO BP. Były wieloletni z-ca dyrektora Departamentu Bezpieczeństwa PKO BP.

Dzień Kobiet Security

ZA NAMI DRUGA EDYCJA SPOTKANIA NAJBARDZIEJ WPŁYWOWYCH KOBIET BRANŻY SECURITY. W TYM ROKU PANIE Z CAŁEJ POLSKI ŚWIĘTOWAŁY W PAŁACU MAŁA WIEŚ POD WARSZAWĄ.

Dzień Kobiet Security to wspólna inicjatywa redakcji A&S Polska oraz firm Axis Communications, Nedap Security Management i Satel. Podczas spotkania odbyły się warsztaty z zarządzania sobą w czasie i efektywności osobistej. Dziękujemy wszystkim uczestniczkom i partnerom za wspaniałą atmosferę w tym wyjątkowym dniu. Do zobaczenia za rok!

Mariusz Kucharski
a&s Polska

***→Dzień Kobiet Security to wyjątkowy dzień**, w którym Panie z branży bezpieczeństwa mogą miło spędzić czas we wspólnym gronie. Wszystkim Paniom życzę wszystkiego dobrego, radości, uśmiechu i miłej zabawy.*

Anna Twardowska
Nedap Security Management

***→Jesteśmy współorganizatorem spotkania kobiet w branży security.** Jestem bardzo dumna, że nasza inicjatywa zorganizowania tego wydarzenia spotkała się z tak dobrym odzewem kobiet z branży security. To, co się udało i co mnie bardzo zaskoczyło, to otwartość uczestniczek spotkania. Duża część Pań się nie znała, natomiast podczas warsztatów każda była skłonna do opowiadania różnych historii, nawet ze swojego życia prywatnego, dzielenia się tym na forum. Spotkanie upłynęło w atmosferze wzajemnego zaufania.*

Agnieszka Pitrus
SATEL

***→Jestem tutaj dlatego, że bardzo sobie cenię ciekawe spotkania i interesujących ludzi. Z przyjemnością nasza firma dołączyła jako współorganizator tego wydarzenia.** Uważam, że takie inicjatywy należy wspierać. Serdecznie zapraszamy na 3. edycję. W planach mamy wiele atrakcji oraz kolejną porcję wiedzy z zakresu rozwoju osobistego. Mam nadzieję, że w przyszłym roku będzie nas więcej i wspólnie, we wspaniałym gronie, będziemy świętować ten wyjątkowy dzień.*

Dagmara Pomirska
Axis Communications

***→Kobiety są wspaniałe, należy je promować.** Zawsze warto na nie postawić. Robią dużą różnicę w firmie. To bardzo pozytywny znak, że po raz kolejny DKS cieszy się tak dużym zainteresowaniem Pań z branży, szczególnie, że 2 lata temu orędowniczkami takiego spotkania były m.in. moje koleżanki z firmy Justyna Puławska i Agata Majkucińska. Potwierdza to nasze przekonanie, że Axis Communications to firma, która potrafi dobrze identyfikować oczekiwania rynku w zakresie oferowanych przez nas rozwiązań i szeroko rozumianych potrzeb ludzi.*

Sylwia Wyrzykowska
ADI Global

***→ To było bardzo udane spotkanie.** Ciekawe rozmowy, ciekawi ludzie, możliwość poznania ciekawych kobiet. Słowem: same plusy.*

Katarzyna Grudniewska
Anixter

***→Myślę, że propozycje na przyszły rok zrodzą się właśnie dziś.** Spotkanie było pełne twórczych, konstruktywnych pomysłów, które zostają w pamięci na następne lata.*

Michał Obszarski
Akademia Gier

***→ Pracowaliśmy z bardzo fajną, dynamiczną grupą trzydziestu bardzo energicznych kobiet.** Zastosowaliśmy niestandardowy sposób prowadzenia szkolenia. Poprowadziliśmy je, wykorzystując ciekawe gry. To spowodowało, że wszyscy bardzo się zaangażowali i mam nadzieję, że też się przy tym dobrze bawili.*

Beata Idziak
Wagner Poland

***→Nie ukrywam, że staram się zasady zarządzania czasem stosować,** ale nie zawsze mi to wychodzi. Po dzisiejszych warsztatach z pewnością będzie łatwiej.*

Dorota Żechowicz
SPIE

***→To był naprawdę świetny dzień.** Forma kameralnego szkolenia sprawiła, że atmosfera była luźna, a piękny pałac i jego otoczenie dodały mu szczególnej aury. Nie mogę się doczekać kolejnego Dnia Kobiet Security.*

Klaudia Nowowiejska
EBS

***→Mam taki charakter, że chciałabym jak najwięcej zrobić, jak najwięcej stworzyć,** jak najwięcej sobie wziąć na głowę i czasem mnie to przerasta. Więc myślę, że to jest taki dobry dzień szkoleniowy dla mnie, żeby popatrzeć na to trochę krytycznym okiem.*

Katarzyna Pikuła

Arpol

→Już po pierwszej edycji miałam bardzo pozytywne doświadczenia *i czekałam na kolejną edycję. Tym razem także się nie zawiodłam. Spotkaniom towarzyszy moc pozytywnej energii generowanej przez silne i błyskotliwe kobiety. Liczę, że DKS stanie się wieloletnią tradycją.*

Anna Sadłowska

Gunnebo Polska

→Na pewno dużo wyniosę z dzisiejszego spotkania, *za co serdecznie dziękuję. Spotkanie kobiet branży security pozwala na wymianę doświadczeń, daje siłę i chęć do działania nad kolejnymi projektami.*

Dominika Mazurek

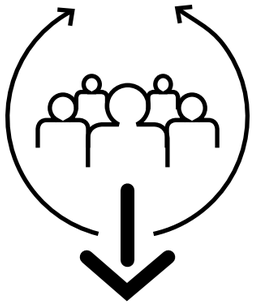
Hikvision Poland

→ To przede wszystkim bardzo mile spędzony dzień, *ale też dzień pełen wrażeń, dzień, który możemy spędzić w przemiłym gronie, a także dużo się dowiedzieć i nauczyć wielu ciekawych rzeczy.*

Magdalena Kolańska

Energa Operator

→I życie prywatne, i zawodowe to jeden wielki plan. *Ważne, aby ćwiczyć planowanie i realizację tych planów. Podoba mi się temat spotkania i na pewno szkolenie z zarządzania czasem przyda mi się w przyszłości* □



Spotkanie najlepszych Autoryzowanych **Partnerów Schrack Seconet** w Polsce

Co roku Schrack Seconet Polska organizuje spotkanie dla swoich najlepszych Autoryzowanych Partnerów. Tegoroczna edycja odbyła się w pierwszym tygodniu marca, tym razem na południu Polski, w stylowym hotelu Młyn Jacka w Wadowicach.

Spotkania mają już długoletnią tradycję. Ich celem jest przede wszystkim podsumowanie minionego roku oraz wspólne opracowanie i omówienie najważniejszych planów i strategii działania na rynku systemów zabezpieczeń w Polsce.
Rok 2018 był dla Schrack Seconet wyjątkowy pod wieloma względami. Lista referencyjna producenta powiększyła się o kolejnych kilkaset obiektów, sprzedano rekordową liczbę systemów bezpieczeństwa i komunikacji, a grono certyfikowanych specjalistów powiększyło się do blisko 1,4 tys.!
W tegorocznym spotkaniu wzięło udział prawie 90 przedstawicieli firm partnerskich – głównie członków szczebla zarządzającego. Oprócz prezentacji przygotowanych przez zespół Schrack Seconet, dotyczących m.in. analizy rynku, nowości produktowych i działań marketingowych, najważniejszym punktem spotkania była dyskusja nt. możliwości rozwoju branży bezpieczeństwa pożarowego w Polsce oraz znaczenia firm partnerskich w tworzeniu nowych wartości dla całego rynku krajowego.
Firma Schrack Seconet, podsumowując ubiegłoroczne wyniki i działania, przyznała tytuł **Partnera Roku firmie RS-SYSTEM z siedzibą w Michałowicach** za najlepszy wynik w sprzedaży systemów sygnalizacji pożarowej Schrack Seconet w 2018 r. oraz wysoką jakość usług.
Ponadto przyjęto do grona Autoryzowanych Partnerów i wyróżniono kolejne, znane i cenione firmy, takie jak: **GEO-KAT z Warszawy, IB Systems z Poznania, INLOGIC ze Szczecina, MAAT4 z Warszawy oraz SECURA z Poznania**.
Za wysoką jakość usług i kompetencje nagrodzono 17 dotychczasowych Partnerów producenta – Autoryzowanych Partnerów Wiodących, którzy istotnie przyczynili się do rozwoju organizacji w Polsce. Do tego elitarnego grona zostały zaproszone w tym roku trzy firmy, dotychczasowi Autoryzowani Partnerzy: **FIRE STOP Serwis ze Szczecina, InGas z Józefowa oraz ZBAR z Łodzi**.
Autoryzowani Partnerzy Schrack Seconet, wraz z wąską grupą Partnerów Wiodących i szerokim wsparciem Partnerów Preautoryzowanych, stanowią największą zorganizowaną grupę specjalistów – przedstawicieli konkretnego producenta w branży systemów przeciwpożarowych, których kompetencje są dokumentowane stosownymi certyfikatami, a wiedza regularnie (nie rzadziej niż co 24 miesiące) aktualizowana. □

Szczegóły dotyczące polityki sprzedaży oraz zakresu uprawnień każdej z trzech grup partnerów biznesowych Schrack Seconet w Polsce są zamieszczone na stronie www.schrack-seconet.pl

9. Smart City Forum Miasta na miarę potrzeb i możliwości

Dziewiąta już edycja Smart City Forum odbyła się pod koniec marca w hotelu Westin w Warszawie. Podczas dwóch dni w konferencji wzięło udział ponad 600 osób.

Pierwsza debata, w myśl hasła przewodniego „Odkryj miasto na nowo", dotyczyła zrealizowanych projektów, planów na przyszłość oraz efektów tych działań. Pamiętając o tym, że miasto to przede wszystkim platforma, która pomaga komunikować się władzom z mieszkańcami i otoczeniem, prezydenci miast rozmawiali o tym, jak wdrażać innowacje, biorąc pod uwagę zdanie obywateli. Smart Citizen to zagadnienie, które często pojawiało się w ramach rozmów o koncepcji Inteligentnych Miast.
Nie zabrakło też konkretnych przykładów strategii rozwoju małych i średnich miast oraz rozmów o finansowaniu inwestycji. Dynamicznym urozmaiceniem standardowej formy przekazania wiedzy był „sparing" technologii *smart city*. Uczestnicy mogli wysłuchać siedmiu przykładów konkretnych wdrożeń innowacyjnych i niezwykle ciekawych rozwiązań dla miast.
Odkrywać miasta na nowo można było także podczas sesji *round tables*. Ta część agendy, w której licznie wzięli udział uczestnicy kongresu, stanowiła idealną okazję do swobodnej wymiany myśli i zapoznania się z opinią na różne kwestie z wielu perspektyw.

PRZY OKRĄGŁYCH STOŁACH MOŻNA BYŁO POSZERZYĆ SWOJĄ WIEDZĘ I WYMIENIĆ SIĘ DOŚWIADCZENIEM W PONIŻSZYCH TEMATACH:

- Zeroemisyjny transport w praktyce – wyzwania a obowiązki
- Jak finansować działania z zakresu efektywności energetycznej i ochrony środowiska?
- Bikesharing dobre praktyki współpracy samorząd – operator
- Korzyści łatwo integrowalnej infrastruktury, dostarczającej i analizującej dane w czasie rzeczywistym
- Miejska infostrada jako narzędzie Smart City służące do zarządzania informacją oraz przestrzenią miejską
- Mobilność współdzielona: hulajnogi elektryczne – wspólne rozwiązanie jako uzupełnienie dla transportu publicznego w miastach

PRELEGENCI 9. SMART CITY FORUM:

- Krystyna Danilecka-Wojewódzka, prezydent Słupska
- Beata Moskal-Słaniewska, prezydent Świdnicy
- Wojciech Bakun, prezydent Przemyśla
- Piotr Grzymowicz, prezydent Olsztyna
- Piotr Kuczera, prezydent Rybnika
- Tadeusz Krzakowski, prezydent Legnicy
- Bartłomiej Pawlak, wiceprezes Polskiego Funduszu Rozwoju
- Roman Szełemej, prezydent Wałbrzycha
- Bogdan Wenta, prezydent Kielc

Bezpieczeństwo infrastruktury krytycznej tematem spotkania w Ambasadzie Australii

W jaki sposób skutecznie zabezpieczyć obiekt infrastruktury krytycznej przed współczesnymi zagrożeniami, zastanawiano się na spotkaniu, które w marcu br. zorganizowały Ambasada Australii w Warszawie oraz firma z firmą Linc Polska.

Promowanie współpracy handlowej i inwestycyjnej oraz pozytywnego wizerunku Australii w Polsce jest jednym z zadań ambasady. Organizowane tu spotkania stanowią platformę do wymiany informacji i doświadczeń, są też doskonałą okazją do nawiązania nowych kontaktów i relacji biznesowych.
Data i miejsce spotkania nie były przypadkowe, bowiem 21 marca br. gościli w Warszawie przedstawiciele australijskiej firmy Future Fibre Technologies (FFT), specjalizującej się w światłowodowych systemach detekcji zagrożenia. Jej portfolio obejmuje rozwiązania do ochrony perymetrycznej obiektów IK. Na ich bazie zrealizowano ponad 1200 instalacji na świecie, m.in. w bazach wojskowych, na granicach państw, lotniskach, w kopalniach, rafineriach, petrochemiach, bazach paliwowych czy w przemyśle gazowym i ciężkim.
Druga część spotkania była poświęcona systemom radarowym marki Blighter Surveillance Systems (Blighter), które wraz z kamerami termowizyjnymi stanowią doskonałe uzupełnienie systemów napłotowych marki FFT. Połączenie tych elementów umożliwia skuteczną detekcję intruza, jego śledzenie i weryfikację na terenie chronionego obiektu.
Duże zainteresowanie wzbudził też system antydronowy AUDS zaprezentowany przez przedstawiciela firmy Blighter. To połączenie trzech elementów: kamery termowizyjnej, radaru i zakłócacza sygnałów. W zależności od potrzeb i oczekiwań można wybrać jeden, dwa lub trzy moduły systemu AUDS.
Oficjalnym przedstawicielem firm FFT oraz Blighter w Polsce jest Linc Polska. □

Nowe Centrum B+R firmy **Ambient System**

W Gdańsku powstanie Centrum Badawczo-Rozwojowe Innowacyjnych Systemów Komunikacji w Sytuacji Zagrożenia firmy Ambient System. Nowy obiekt będzie miał powierzchnię ponad 3 tys. m². Koszt realizacji przedsięwzięcia i wyposażenia laboratorium wyniesie ok. 20 mln zł. Projektowi przyznano wsparcie finansowe Ministerstwa Rozwoju.

Ambient System jest jednym z czołowych europejskich producentów m.in. dźwiękowych systemów ostrzegawczych i innych rozwiązań z zakresu komunikacji cyfrowej. Firma prowadzi prace badawczo-rozwojowe nad innowacyjnymi technologiami w zakresie zaawansowanych algorytmów przetwarzania sygnałów audio. Część laboratoriów badawczych zostanie wyposażona w środowiska testowe rozległych sieci dystrybucji sygnałów audio oraz laboratoria akustyczne pozwalające badać rozwijane algorytmy w warunkach rzeczywistych. W nowym centrum technologicznym docelowo zatrudnienie znajdzie ponad 100 pracowników.

– *Decyzję o uruchomieniu inwestycji podjęliśmy w 2017 r., kiedy to pojawił się pomysł stworzenia algorytmów poprawy zrozumiałości komunikatów w sytuacji zagrożenia. Skala wyzwania technologicznego jest na tyle duża, że wymaga budowy sporego laboratorium akustycznego odwzorowującego warunki rzeczywiste. Jeżeli uda się nam osiągnąć zamierzony cel, będzie to przełom w systemach komunikacji i powiadamiania* – powiedział Marcin Starzyński, prezes Ambient System.

HAC-EW2501 5 Mpix **kamera fisheye HDCVI**

Dahua Technology Poland wprowadziła do oferty kamerę z obiektywem fisheye działającą w standardzie analogowym HDCVI o wysokiej rozdzielczości 5 Mpix. Urządzenie to wyróżnia nowoczesny wygląd oraz wysokiej jakości obraz, który zawdzięcza przetwornikowi Starlight, charakteryzującemu się wysoką czułością oraz szczegółowym odwzorowaniem detali.

Urządzenie umożliwia pracę w trybie widoku dookólnego 360° „rybie oko", współpracuje także z rejestratorami XVR i ich interfejsem web (prostowanie obrazów: 10+ trybów). Wbudowany promiennik podczerwieni doświetla scenę na odległość 10 m. Kamera ma również zintegrowany mikrofon.

Dzięki technologii HDCVI kamera może przesyłać 4 sygnały (obraz, dźwięk, sterowanie i zasilanie PoC) jednym przewodem koncentrycznym. Panoramiczny widok i rozdzielczość 5 Mpix sprawiają, że kamera jest idealną propozycją dla dużych firm i sprawdzi się w takich miejscach, jak lotniska, stadiony, parkingi czy centra handlowe.

Tworząc system ochrony ppoż., warto wykorzystać kamery termowizyjne umożliwiające radiometryczny pomiar temperatury. Jednym z takich rozwiązań jest termowizyjna głowica obrotowa typu PTZ z serii AERON marki Silent Sentinel.

AERON marki Silent Sentinel a

Automatyczna detekcja punktów o podwyższonej temperaturze, a w konsekwencji ich identyfikacja i weryfikacja w wielu przypadkach pozwala uniknąć zagrożenia, jakim jest pożar. Gdy temperatura dla konkretnego punktu pomiarowego przekroczy dopuszczalny poziom, informacja o tym zostaje automatycznie przekazana do operatora, który po jej zweryfikowaniu podejmuje odpowiednie działania. Sygnał alarmowy może być przekazywany w postaci zarówno wizualnej, jak i dźwiękowej. Dzięki temu operator może szybko zareagować na zdarzenie. Zaletą termowizyjnych kamer PTZ serii AERON jest ponadto duży zakres detekcji oraz możliwość wyeliminowania niepożądanych źródeł ciepła. To bardzo interesujące rozwiązanie szczególnie dla przedsiębiorstw zajmujących się gospodarką odpadami, recyklingiem oraz odnawialnymi źródłami energii. Kamery bardzo dobrze sprawdzają się np. w spalarniach śmieci.

Więcej informacji:
Linc Polska
www.linc.pl

Światłowodowy system **ochrony obwodowej**

W ofercie OPTEX Security znajduje się system ochrony obwodowej Fiber Defender® produkowany przez amerykańską firmę Fiber SenSys Inc. należącą do OPTEX CO. LTD.

Koncepcja systemu jest oparta na aktywnym światłowodzie mocowanym do ogrodzenia. Drgania ogrodzenia wywołane ingerencją intruza (wspinanie, cięcie, podnoszenie) są analizowane w procesorze wysyłającym sygnał alarmowy. W zależności od modelu jeden procesor może obsługiwać nawet 25 stref detekcji, każda o maks. długości 2,3 km.

Dopasowanie do wymogów instalacji ułatwia zastosowanie dodatkowego kabla nieaktywnego, który pozwala na zamontowanie procesora sterującego w odległości do 20 km od ochranianego fragmentu ogrodzenia. Strojenie systemu odbywa się z wykorzystaniem dedykowanych aplikacji komputerowych. W odróżnieniu od rozwiązań opartych na detektorach mechanicznych, światłowód jest odporny na działanie czynników środowiskowych (np. promieniowanie UV i elektromagnetyczne, wilgoć, sól czy wyładowania atmosferyczne). System pracuje stabilnie we mgle, zapyleniu czy w ciemności. Można go stosować w strefach zagrożonych wybuchem.

Parametry techniczne i niezawodność rozwiązania potwierdza certyfikat najwyższej klasy ochrony armii USA, zezwalający na instalację w obiektach, w których przechowuje się materiały nuklearne. System jest również rekomendowany przez brytyjski urząd ochrony infrastruktury krytycznej (CPNI).

Więcej informacji o Fiber Defender® na www.fibersensys.com.

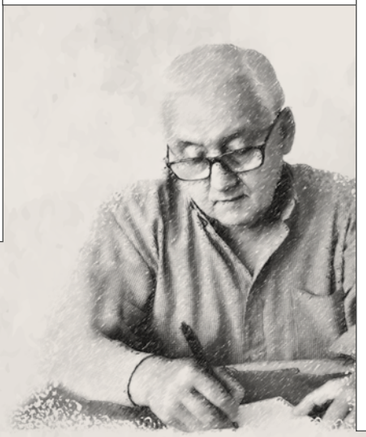
Kontakt z OPTEX Security: optex@optex.com.pl

Ciężkie **życie** bogatego

Wystarczyło lat kilkanaście, by powstały firmy IT o zasięgu światowym, mające realny wpływ na stan bezpieczeństwa. Jedną z nich jest Facebook codziennie zajmujący uwagę dwóch, może trzech miliardów ludzi. Dla wielu internautów treści portalu społecznościowego są ważniejsze od śniadania.

W mediach jest zawsze sporo doniesień o informatycznym kolosie. Łatwego życia nie ma, walczy z wieloma problemami, często nieskutecznie. Choćby z tzw. złymi treściami wciskającymi się na platformę. Niedawno terrorysta z Nowej Zelandii nadawał transmisję przez FB. Zdarzają się w firmie historie kryzysowe dotyczące awarii, luk i błędów, ataków hakerskich oraz wycieków danych osobowych liczonych w milionach poszkodowanych klientów. Chyba najgłośniejsza była afera Cambridge. Słychać było o perturbacjach z dostosowaniem się Facebooka do prawa unijnego dot. ochrony danych osobowych. Korporacja musi chronić pomysły i prototypy, zderza się z zagrożeniami sieciowymi i kryminalnymi (fizycznymi). FB miał też wziąć się za likwidację 1,5 mld fałszywych kont! Nie zdziwiłem się, kiedy usłyszałem, że chce kupić firmę zajmującą się cyberbezpieczeństwem. Realizacji zapowiedzi nie dostrzegłem w mediach, może przegapiłem.

Mark Zuckerberg, genialny młodzieniec, a teraz już „podstarzały" 35-letni wyjadacz i multimiliarder, posiadacz idealistycznych poglądów nt. naprawy świata za pomocą swojego produktu – platformy łączącej ludzi – musiał zderzyć się z rzeczywistością. Niemiło jest, gdy ktoś obcy zagląda człowiekowi do łazienki, a tu we własnym Facebooku obserwuje go ponad 100 mln osób. Jak to mówią: *life is brutal*. W tłumie mogą zdarzyć się i tacy, którzy by go np. chcieli zabić, nie tylko za coś, ale i za nic. Do prezesa podobno napływają listy z pogróżkami. Pod kątem jego zagrożeń monitorowane są media społecznościowe. Przyjęto, że desperat może znaleźć się nawet w macierzystej firmie. Zuckerberg ma całodobową ochronę, jak np. prezydent, i to mocarstwa. Anioły stróże fruwają przy nim stale, a w biurze przed ekranami komputerów udają programistów. Mark Zuckerberg nie korzysta podobno z tradycyjnego dyrektorskiego gabinetu, a urzęduje w kolejnym firmowym *open space*. W biurze ma zjeżdżalnię (rynnę) do garażu – do szybkiej ewakuacji. Sala konferencyjna jest wyposażona w kuloodporne szyby i tzw. przycisk paniki. W jednym z domów prywatnych prezesa jest schron. Przed jego pojawieniem się gdziekolwiek miejsce jest sprawdzane wcześniej przez zespół ochrony. Oczywiście to są informacje plotkarskie. Ale znana jest roczna skala wydatków na bezpieczeństwo jego i rodziny – ponad 20 mln dolarów. Dla porównania – na ochronę prezesa Jarosława Kaczyńskiego podobno idzie tylko skromne 1,5 mln zł. Ale on jest sam i nie ma tylu pięter w biurowcach.



RODO ma coraz większą siłę oddziaływania na życie codzienne. Ministerstwo Zdrowia zrezygnowało – po uwagach Prezes UODO – z projektu wyposażenia ratowników medycznych w tzw. kamery nasobne, takie jak noszone przez policyjne patrole prewencji i ruchu drogowego. Bez wchodzenia w prawnicze szczegóły wyobraźmy sobie sytuację, gdy w karetce nagrywany jest obraz i dźwięk. Może dojść do ujawnienia tajemnicy lekarskiej? Nie można wykluczyć, że nagranie dźwiękowe z karetki mogłoby zostać wykorzystane w celu postawienia osoby, której udzielono pomocy medycznej, w stan oskarżenia i możliwego jej skazania. Pacjent, wiedząc o monitorowaniu, mógłby zataić informacje ważne dla jego zdrowia, np. o zażyciu substancji zakazanej (narkotyków), przebywaniu w miejscu niedozwolonym itd.

Niech żyje przyjaźń między narodami, a zwłaszcza zrzeszonymi w UE. Przeczytałem, chyba w Onecie, że w parlamencie niemieckiego landu Saksonii projektują nowe prawo, które pozwoli na zainstalowanie kamer w pasie 30 km na styku z granicami Polski i Czech. Monitoring ma posiadać automatyczny system rozpoznawania twarzy. Praktyczni Niemcy tłumaczą to walką z przestępczością, ale organizacje pozarządowe widzą w projekcie naruszenia praw obywateli.

Drony w branży security nie są pomysłem nowym, to pożyteczne narzędzie zwłaszcza przy dozorze terenów rozległych. Według Urzędu Lotnictwa Cywilnego w Polsce lata już 100 tys. dronów, a uprawnienia do operowania nimi ma ok. 10 tys. osób. Za 10 lat rynek dronowy ma osiągnąć wartość 3 mld zł i generować o wiele większe korzyści. Podobno realne jest nieodległe w czasie przyjęcie przez rząd strategii jego rozwoju. □

TEKST
Andrzej Popielski

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

IVSS Dahua - rejestrator NVR

Rozpoznawanie i zaawansowana analiza twarzy w czasie rzeczywistym

- Analiza wideo w czasie rzeczywistym: algorytm głębokiego uczenia umożliwia wykrywanie obiektu i przewidywanie potencjalnego zagrożenia.
- Wyszukiwanie wideo według obrazu: jednocześnie wyszukuje do 10 twarzy.
- Szybka analiza twarzy z informacją, gdzie i kiedy się pojawiły.
- Urządzenie wielofunkcyjne: zarządzanie wideo, przechowywanie, analiza z wykorzystaniem interfejsów AI.

Polecane modele

IVSS7012-2T

IVSS7024DR-8T

ISO 9001:2000

www.dahuasecurity.com/pl

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