

SECURITY 50

NAJWIĘKSZE FIRMY SECURITY NA ŚWIECIE

Pandemia odbiła się na światowej gospodarce, wpływając również na branżę security. W obliczu spadku przychodów w latach 2020-2021 niektóre firmy wykazały się większą odpornością na recesję. Dojrzałe technologie pomogą w walce ze skutkami kryzysu.

BEZPIECZEŃSTWO W HANDLU

NIEKOMANDOS W CENTRUM HANDLOWYM

Centra handlowe nie potrzebują byłych komandosów w strukturach ochrony. Na froncie kontaktu z klientem sprawdzi się steward wspierany technologią, która podniesie efektywność jego pracy i dostarczy cennych danych zarządcowi.

BEZPIECZEŃSTWO BIZNESU

SYSTEM ZARZĄDZANIA CIĄGŁOŚCIĄ DZIAŁANIA

Każde przedsiębiorstwo musi przynosić dochody. Aby to zapewnić, należy zadbać o ciągłość jego funkcjonowania. Czy to oznacza, że musimy wdrożyć system zarządzania ciągłością działania?

ISSN 2451-5175



9 772451 517703

05 >

15 zł
(w tym 8% VAT)



TECHNOLOGIA NA KRYZYS

APLIKACJA
MOBILNA



04.30

SZYBKO ZNAJDŹ TO, CZEGO SZUKASZ!

Nie marnuj czasu, przeglądając godziny nagrań. Dzięki rozwiązaniu XProtect® Rapid REVIEW wspomaganemu technologią BriefCam masz łatwe w użyciu i zaawansowane rozwiązanie do analiz kryminalistycznych. Za jego pomocą możesz analizować treści wideo i szybko znaleźć to, czego szukasz.



Dowiedz się więcej na milestonesys.com

Drodzy Czytelnicy

W połowie roku 2020 COVID-19 wyhamował trwającą od dekady dynamikę wzrostu przychodów w branży security. Skutki pandemii w roku 2021 omawiamy w tegorocznym Raporcie Security 50 opracowanym przez portal asmag.com (s. 14). Po raz pierwszy w historii rankingu największych światowych firm branży security (s. 18) liczba firm zgłaszających spadek przychodów (28 firm) przewyższyła liczbę firm notujących wzrosty (22 firmy). Co spowodowało, że niektóre wykazały się większą odpornością na recesję? (s. 20).

Głównym narzędziem w rozwiązywaniu problemów spowodowanych przez COVID stał się dozór wizyjny. W odpowiedzi na wzrost zapotrzebowania na systemy z tego sektora nastąpił w ciągu kilku miesięcy niespotykane szybki postęp w rozwoju technologicznym. Przemodelowanie priorytetów przez klientów wpłynęło na popyt, zwłaszcza na usługi zdalne – doradztwo, obsługę i serwisowanie (s. 24). Również rynek kontroli dostępu musiał się do tej sytuacji dostosować (s. 26).

Tak było w tym roku. A jaki będzie kolejny? Technologicznie zapowiada się obiecująco. Analiza danych wizyjnych i inne możliwości automatyzacji stają się coraz bardziej powszechne, stanowiąc poligon innowacji dla systemów VMS. Technologia umożliwia już obsługę analityki, sztucznej inteligencji i innych zautomatyzowanych rozwiązań. Jakie nowości w obszarze VMS i jakie trendy pojawią się w nadchodzącym roku? Z pewnością będzie więcej aplikacji spoza zastosowań security (s. 28).

Eksperci, którzy uczestniczyli w badaniu asmag.com, są optymistami co do perspektyw na przyszłość. Wiele technologii, które pandemia upowszechniła, nadal będzie się cieszyło zainteresowaniem. Sektory, które wspierają te rozwiązania, mogą być motorem rozwoju branży zabezpieczeń (s. 32).

Nagłe zmiany wywołane pandemią obnażyły słabość światowej gospodarki i globalnych łańcuchów dostaw. Jak to wpłynęło na polski rynek zabezpieczeń technicznych? Dla dostawców rozwiązań to czas ciągłej walki z wydłużającymi się terminami dostaw, wyzwań związanych z wprowadzaniem zamienników produktów w trakcie realizacji projektu i odbudowy lokalnych stoków magazynowych. Jedną z tych słabości okazały się twarde realia rynku produkcji układów scalonych. Skomplikowaną sytuację zależności wyjaśniamy na s. 36.

Aż trudno uwierzyć, że minęło już pięć lat, odkąd na rynku pojawił się pierwszy numer „a&s Polska”. Przedstawiamy Czytelnikom kolejne, 30. wydanie. W tym czasie przygotowaliśmy też 54 odcinki programu telewizyjnego „Bezpieczny Biznes”, 4 edycje konferencji Warsaw Security Summit, 2 edycje Security BootCamp, kilkanaście spotkań na „Śniadaniach Ekspertów”, wiele filmów promocyjnych oraz niezliczoną liczbę publikacji na portalu i postów w mediach społecznościowych. Sukces, jaki osiągnęliśmy, nie byłby możliwy bez naszych Partnerów i Autorów. Dziękujemy za wsparcie i współpracę!

C całej branży życzymy, aby rok 2022 był lepszy niż dwa lata pandemii. Dostawcom systemów zabezpieczeń życzymy powrotu na właściwe tory, integratorom – żeby nie mieli żadnych opóźnień, a klientom końcowym – by mogli prowadzić swoją działalność bez przeszkód. A przede wszystkim zdrowych i bezpiecznych świąt Bożego Narodzenia i całego roku 2022!

Marta Dynakowska
REDAKTOR NACZELNA

Jan T. Grusznick
Z-C A REDAKTORA NACZELNEGO

Mariusz Kucharski
PREZES ZARZĄDU

Wydawca
SENS Group Sp. z o.o.
ul. Rondo ONZ 1
00-124 Warszawa

Prezes Zarządu
Mariusz Kucharski

Redaktor naczelna
Marta Dynakowska

**Z-ca redaktora
naczelnego**
Jan T. Grusznick

**Dział reklamy
i marketingu**
Iwona Krawiec

**Dział projektów
specjalnych**
Jolanta A. Kucharska
Aleksandra Czapska

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

Korekta
Jolanta Kucharska

Projekt graficzny i skład
Kalwala Studio

Adres redakcji
A&S Polska
ul. M. Rodziewiczówny 1 lok. 801
04-187 Warszawa
e-mail: info@aspolska.pl
www.aspolska.pl

Prenumerata
www.aspolska.pl/prenumerata

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

A&S Polska jest częścią grupy wydawniczej A&S International.
© Copyright by A&S Polska

A & S P O L S K A
Z Ł O T Y P A R T N E R

AXIS
COMMUNICATIONS

BCS

Linc
Polska Sp. z o.o.

nedap

**SCHRACK
SECONET**

smart-i

A & S P O L S K A
S R E B R N Y
P A R T N E R

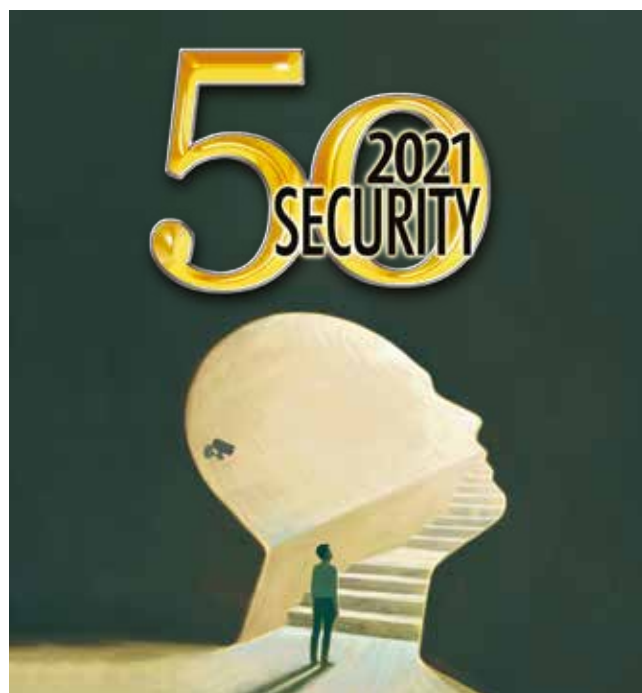
HIKVISION

A & S P O L S K A
W Y D A N I E
O N L I N E

www.aspolska.pl/czasopismo

S P I S T R E Ś C I

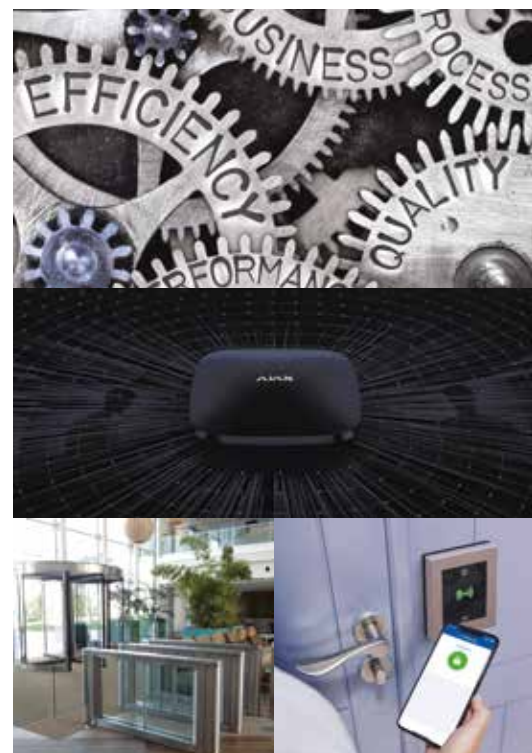
8 Produkty numeru



- 14** Security 50 – technologie, które dominowały w 2021 r.
WILLIAM PAO, ASMAG.COM
- 18** Największe firmy branży security na świecie – zestawienie tabelaryczne
- 20** Sekret firm odpornych na kryzys wywołany przez pandemię
PRASANTH ABY THOMAS, ASMAG.COM
- 24** Szanse i zagrożenia rynku dozoru wizyjnego
PRASANTH ABY THOMAS, ASMAG.COM
- 26** Kontrola dostępu – inwestycje napędzane popytem
- 28** VMS – spodziewane nowości w 2022 r.
WILLIAM PAO, ASMAG.COM
- 32** Technologie roku 2022
- 36** Na układy nie ma rady. Kryzys w dostawach mikroprocesorów
JAN T. GRUSZNIC



- 40** Rola inżyniera uruchomieniowego w procesie inwestycyjnym. Trudności, pułapki i szanse
MICHAŁ ZALEWSKI
- 44** Listopadowe nowości SATEL – SATEL
- 46** Weryfikacja fotograficzna przez stal i beton
AJAX SYSTEMS POLAND
- 48** Czy istniejące budynki biurowe mogą skutecznie walczyć o nowego najemcę?
BŁAŻEJ OŹGA, NEDAP SECURITY MANAGEMENT
- 50** Nowoczesny system kontroli dostępu
2N TELEKOMUNIKACE
- 52** Automatyczny skarbiec SafeStore Auto – czyli skrytki depozytowe jak z bankomatu
GUNNEBO POLSKA
- 54** Kamery nasobne w służbie
RAFAŁ BATKOWSKI
- 58** Kamery nasobne
AXIS COMMUNICATIONS I RTCOM



BCS®

dla profesjonalistów

*Wyjątkowych Świąt Bożego Narodzenia
oraz szczęścia w nadchodzącym
Nowym Roku
wszystkim sympatykom,
użytkownikom i czytelnikom życzy
zespół BCS*



www.bcs.pl
www.facebook.com/bcspl





BEZPIECZEŃSTWO W HANDLU

- 60 Niekomandos w centrum handlowym. Steward wsparty technologią zrobi różnicę
JACEK TYBUREK
- 64 Sieci handlowe dostosowane do potrzeb klienta
AXIS COMMUNICATIONS
- 66 Oferta Hikvision na pandemiczne czasy
PAWEŁ SOBOCIŃSKI, HIKVISION POLAND
- 68 Głos Branży



BEZPIECZEŃSTWO POŻAROWE

- 74 ARGUS RV-C – certyfikowana platforma do zarządzania bezpieczeństwem pożarowym
TELBUD
- 75 Adresowalne sygnalizatory akustyczne ZETTLER
JOHNSON CONTROLS INTERNATIONAL
- 76 Remote with Schrack Seconet – razem w czasach pandemii
SCHRACK SECONET POLSKA



BEZPIECZEŃSTWO BIZNESU

- 78 System zarządzania ciągłością działania (BCMS). Cz. 1. Czy w ogóle jest to komuś potrzebne?
TOMASZ GUZIKOWSKI
- 80 Przerwanie łańcucha dostaw. Zagrożenie tylko dla dużych przedsiębiorstw?
MIROSLAW LUKOWSKI



CYBERBEZPIECZEŃSTWO

- 82 Bezpieczna organizacja
TOMASZ DACKA



SERWIS INFORMACYJNY

- 86 Konferencja EBS Security 5.0
- 88 Security BootCamp 2021
- 90 Sicurezza 2021
- 92 Informacje firmowe/nowości produktowe



axxonsoft

EXPERIENCE THE NEXT®

Światowy lider w dziedzinie inteligentnego oprogramowania VMS i PSIM

Sztuczna Inteligencja i Sieci Neuronowe

AxxonSoft proponuje rozwiązania analityki wideo zapewniające wiele korzyści dla biznesu i bezpieczeństwa dzięki sieciom neuronowym zasilanym przez AI (sztuczną inteligencję) i algorytmy głębokiego uczenia. Inteligentna Analiza Obrazu AxxonSoft otwiera drogę do aktywnego, zautomatyzowanego nadzoru, który pomaga chronić własność poprzez wykrywanie i powstrzymywanie przestępstw. Aplikacje mogą wykrywać ludzi / pojazdy, ogień / dym lub nieprawidłowe zachowanie / warunki i automatycznie o tym powiadamiać.

- Analityka Behawioralna
- Identyfikacja Obiektów
- Rozpoznawanie Tablic Rejestracyjnych
- Rozpoznawanie Twarzy
- Detekcja Dymu i Ognia

www.axxonsoft.com/pl

www.axis.com/pl

AXIS COMMUNICATIONS

AXIS COMMUNICATIONS WPROWADZA NA RYNEK TRZY NOWE KAMERY KOPUŁKOWE DO PRACY W NAJTRUDNIEJSZYCH WARUNKACH ATMOSFERYCZNYCH I OŚWIETLENIOWYCH. DZIĘKI ZASTOSOWANIU PROCESORA ARPTEC-8 OBSŁUGUJĄ ZAAWANSOWANE APLIKACJE ANALITYCZNE OPARTE NA TECHNOLOGII GŁĘBOKIEGO UCZENIA. WSPÓŁPRACUJĄ TEŻ Z PLATFORMĄ ACAP (AXIS CAMERA APPLICATION PLATFORM), KTÓRA UŁATWIA PROJEKTOWANIE DEDYKOWANYCH APLIKACJI WYKORZYSTUJĄCYCH FUNKCJE AI.

Nowe kamery Axis z procesorem ARTPEC-8 i funkcją głębokiego uczenia

↓ Obraz z kamery **AXIS Q3538-LVE 4K** ma znakomitą jakość i wiernie odwzorowuje szczegóły. **AXIS Q3536-LVE 4 Mpix** ma do wyboru obiektyw szerokokątny 9 mm (dozór rozległych obszarów) lub teleobiektyw 29 mm (dozór z większej odległości). Oba modele mają kopułki z osłoną przed promieniowaniem IR, która zapobiega powstawaniu odblasków powodowanych przez

kurz, deszcz i śnieg. Axis OptimizedIR gwarantuje wyraźny obraz nawet w całkowitej ciemności. Wbudowane funkcje cyberbezpieczeństwa zapobiegają nieautoryzowanemu dostępowi i chronią przed atakami hakerów. Kamery są wyposażone w moduł TPM (Trusted Platform Module) z certyfikatem FIPS 140-2. Z kolei **AXIS Q1656-LE** typu box z przetwornikiem obrazu 1/1,8"



RACS 5 v2

Skalowalny system kontroli dostępu, bezpieczeństwa i automatyki klasy *Enterprise*

- Obsługa systemów rozproszonych
- Obsługa wind serwerowych KONE i Schindler
- Integracje PSIM, SMS, VMS, OFFICE
- Globalny anti-passback

www.bcsctv.pl

BCS

BCS i liczenie ludzi

FUNKCJE LICZENIA OSÓB SĄ DOSTĘPNE W KAMERACH BCS LINE JUŻ OD 2018 R. POCZĄTKOWO BYŁ TO JEDEN MODEL KAMERY SPECJALNIE DO TEGO CELU ZAPROJEKTOWANY. KAMERA CHARAKTERYZOWAŁA SIĘ DOSYĆ NIECODZIENNĄ OBUDOWĄ Z DWOMA OBIEKTYWAMI, CO UMOŻLIWIŁO POMIAR WYSOKOŚCI OBIEKTU, A CO ZA TYM IDZIE USTAWIANIE PROGU WZROSTU PRZY ZLICZANIU OSÓB WCHODZĄCYCH. KAMERA PCIP4301IR-I JEST CAŁY CZAS W OFERCIE, OD PREMIERY PRZESZŁA SZEREG MODYFIKACJI POPRAWIAJĄCYCH JEJ SKUTECZNOŚĆ I LICZBĘ DOSTĘPNYCH FUNKCJI.

↓ Prawdziwa rewolucja w liczeniu osób przyszła wraz z pojawieniem się kamer **BCS Line** serii Ai. Kamery tej serii są dostępne w obudowach tubowych, klasycznych kopułkach i kopułkach metalowych, dzięki czemu funkcje analizy wideo można zastosować w większej liczbie obiektów. Aby zliczanie było jak najbardziej sku-

teczne/poprawne, istotne jest, by kamera była w odpowiedni sposób zamontowana. Wieże są dostępne w dwóch wersjach: wieża w pierwszej wersji jest na stałe zintegrowana z przyczepą bez hamulców o masie 750 kg, w drugiej wersji jest na przyczepie z hamulcami o masie 1200 kg wyposażonej w podnośnik hydrau-

liczny, dzięki któremu można ją bezpiecznie postawić w miejscu, gdzie konieczne jest wykorzystanie monitoringu wizyjnego. Modele kamer z oznaczeniem **Ai2** potrafią liczyć osoby na dwa sposoby. Pierwszym jest kontrola przejścia i zliczanie osób wchodzących na dany obszar i wychodzących z niego. Połączenie kilku kamer z wykorzystaniem rejestratora **BCS Line NVR-4K-III** i śledzenie ruchu na obrazach z kolejnych kamer pozwala na kontrolę liczby osób w całym obiekcie. Do dyspozycji klienta pozostaje jeszcze drugi ze sposobów – możliwość monitorowania liczby osób znajdujących się w wyznaczonej strefie, również pod kątem czasu, jaki w tej strefie spędzają. Przekroczenie jednego ze wspomnianych parametrów może skutkować uruchomieniem alarmu. 📞



www: www.gde.pl

GDE POLSKA

BOBBY-AM – zewnętrzna czujka ruchu firmy Lince

LINCE ITALIA JEST LIDEREM W BRANŻY SYSTEMÓW ZABEZPIECZEŃ. FIRMA Z WIELOLETNIM DOŚWIADCZENIEM PROJEKTUJE UNIKATOWE KONSTRUKCJE DOPASOWANE DO POTRZEB INSTALATORÓW I W PEŁNI SATYSFAKCUJĄCE UŻYTKOWNIKÓW KOŃCOWYCH.

↓ Najważniejsze cechy czujek LINCE: włoskie projekty i produkcja, kompatybilność z każdym system alarmowym, solidna obudowa z poliwęglanu, doskonałe filtry światła słonecznego wyprodukowane w Japonii, najwyższej jakości soczewki Fresnela wyprodukowane w USA. Zwielokrotnione czujniki i zaawansowane algorytmy pracy minimalizują liczbę fałszywych alarmów. Wersje Low Power są zasilane z baterii, a po zamontowaniu modułu RF (w pozostawionym miejscu) mogą współpracować z dowolną centralą bezprzewodową.

Czujki zewnętrzne wykrywają intruza, zanim jeszcze znajdzie się w obiekcie. Tym samym zapewniają większe bezpieczeństwo niż tradycyjne rozwiązania z czujkami jedynie wewnątrz obiektu. **Bobby-AM** to zewnętrzna czujka ruchu wyposażona w dwa czujniki PIR oraz czujnik mikrofalowy, co pozwala zredukować liczbę fałszywych alarmów, a także regulować zasięg detekcji od 3 do 18 m. Szerokość pola detekcji wynosi 85°. Dzięki funkcji antymaskingu wykorzystującej dwa dodatkowe czujniki IR czujka jest zabezpieczona przed przystąpieniem (zamalowaniem, zastąpieniem) w celu zablokowania detekcji. Trzy czujniki są sterowane przez mikrokontroler, co pozwala wybierać różne tryby pracy i dopasować się do różnych warunków środowiska. Wyłącznym dystrybutorem firmy Lince jest GDE Polska. 📞



roger
Intelligence for Building

HXVR-16P102H2 – rejestrator z rozpoznawaniem ludzi i pojazdów

JEDNĄ Z FUNKCJI REJESTRATORÓW JEST REJESTRACJA OBRAZU URUCHAMIANIA DETEKCJĄ RUCHU. JEJ UŻYTECZNOŚĆ BYŁA OGRANICZONA, GDYŻ DOTYCHCZASOWE ROZWIĄZANIA WYKRYWAŁY KAŻDY RUCH, NIEZALEŻNIE CZY WYWOŁAŁ GO CZŁOWIEK, CZY PORUSZAJĄCE SIĘ GAŁĘZIE. DUŻA LICZBA FAŁSZYWYCH ALARMÓW UTRUDNIAŁA PRZESZUKIWANIE NAGRAŃ.

Rozwiązaniem jest zastosowanie elementów uczenia maszynowego do rozpoznawania ludzi i pojazdów. Uczenie maszynowe sukcesywnie trafia do kolejnych rejestratorów MAZI. Przykładem jest MAZI HXVR-16P102H2 z zaawansowaną detekcją ruchu bazującą na uczeniu maszynowym i rozpoznaniem ludzi i pojazdów na wszystkich kanałach. Opcjonalnie na czterech kanałach dostępna jest detekcja przekroczenia linii i wtargnięcia w obszar, a na jednym kanale detekcja nagłej zmiany sceny lub rozpoznawanie twarzy.

Zaawansowana detekcja ruchu dzięki możliwości rozpoznawania ludzi i pojazdów zmniejsza liczbę fałszywych alarmów, a przeszukiwanie nagrań jest dużo łatwiejsze i szybsze. HXVR-16P102H2 jest wyposażony w 16 uniwersalnych wejść obsługujących standardy HD-TVI/HD-CVI/AHD/CVBS, ob-

sługuje rozdzielczość 4Mpix lite, 2 Mpix full HD i mniejsze. Dodatkowo można podłączyć do 8 kamer IP lub nawet 24, gdy wyłączymy kanały analogowe. Długi czas zapisu umożliwiają najnowszy kodek H.265Pro+ i dwa dyski o pojemności do 10TB. Ciekawą funkcją jest możliwość zapisu na dyskach OneDrive, Google Drive i Dropbox. Wyłącznym partnerem firmy MAZI Security Systems jest GDE Polska.



Technologia HeatPro w kamerach IP

TERMOWIZJA NIESIE ZE SOBĄ WIELE KORZYŚCI DLA SYSTEMÓW ALARMOWYCH, OCHRONY OBWODOWEJ I PRZECIWOPOŻAROWEJ. TECHNOLOGIA ZASTOSOWANA W KAMERACH SERII HEATPRO JEST OPARTA NA ANALITYCE WYKORZYSTUJĄCEJ ALGORYTMY GŁĘBOKIEGO UCZENIA. DZIAŁA NIEZALEŻNIE OD WARUNKÓW ATMOSFERYCZNYCH I OŚWIETLENIA, ZAPEWNIĄC WYSOKĄ DOKŁADNOŚĆ W IDENTYFIKACJI LUDZI I POJAZDÓW, CO W EFEKCIE PROWADZI DO ZMNIJSZENIA LICZBY FAŁSZYWYCH ALARMÓW.



Funkcja wykrywania ognia, w jaką zostały wyposażone kamery serii HeatPro, pozwala na detekcję zagrożenia pożarowego w bardzo wczesnym stadium jego rozwoju. Ponadto zastosowano funkcję kontroli urządzeń, które są narażone na ryzyko przegrzania, np. pomp wodnych, silników elektrycznych i spaliny-
wych, akumulatorów oraz innych urządzeń o wysokiej podatności na przegrzanie. W kamerach zainstalowano, wykorzystując aplikację Hik-Connect, alarmy dźwiękowe i wizyjne z funkcją ustawiania alarmów domyślnych, własnych dźwięków alarmowych lub alarmu w czasie rzeczywistym. Dodatkowo kamery mają wbudowaną diodę LED światła



białego stosowaną jako wizualizacja alarmu. Algorytmy detekcji zastosowane w nowej serii kamer z technologią HeatPro działające na obrazie termowizyjnym ostrzegają użytkownika o potencjalnych zagrożeniach. Dzięki temu mogą być stosowane w systemach zabezpieczeń zarówno w domach, willach czy budynkach biurowych, jak i w rozwiązaniach rozbudowanych skierowanych do przemysłu.

Kamery Q71 i D71 – nowości od MOBOTIX

W LISTOPADZIE MOBOTIX WPROWADZIŁ NA RYNEK DWIE ZUPEŁNIE NOWE, DOSKONAŁE WYPOSAŻONE I ODPORNE NA WARUNKI ATMOSFERYCZNE KAMERY Z SERII MOBOTIX 7: Q71 I D71. TECHNOLOGIA KAMER HEMISFERYCZNYCH (360°) JESZCZE NIGDY NIE BYŁA TAK KOMPAKTOWA I ELASTYCZNA.

MOBOTIX Q71 rejestruje każdy obszar całego pomieszczenia, zastępując nawet cztery konwencjonalne kamery. Po raz pierwszy w jednej kamerze hemisferycznej połączono czujnik dzień-noc, oświetlacz podczerwieni i światła diodowe (diody LED). Kamera o rozdzielczości 12 Mpix z funkcją WDR zapewnia kolorowe obrazy o doskonałej jakości i im-

ponującą szczegółowości – nawet w nocy. Zintegrowana w kamerze funkcja audio pozwala nadać komunikaty głosowe.

MOBOTIX D71 to kompaktowa kamera jednoobiektywowa w odpornej na warunki atmosferyczne i wstrząsy kopule z poliwęglanu. D71 może być wyposażona w przetworniki obrazu 4K UHD i 4 Mpix Ultra LowLight do pracy w dzień

i w nocy oraz obiektyw HD o kącie widzenia od 15° do 95° w poziomie. Regulacja w trzech osiach umożliwia precyzyjne ustawienie obiektywu.

Platforma MOBOTIX7 pozwala na zainstalowanie indywidualnych aplikacji i wzbogacenie obu kamer o nowe funkcje. Odpowiednia ich konfiguracja zastosowana w obiektach handlowych może zapobiec kradzieżom, ale również dostarczyć nowych informacji o preferencjach klientów. Kamera może śledzić ich ruch i tworzyć mapy cieplne, oferując pełną świadomość sytuacyjną.



VCS

ECO POWER
iTOWER III SOLAR

WWW.VCS.PL

www.nedapsecurity.com/pl/

Integracja AEOS z czytnikami firmy STiD

ZARZĄDZAJ MOBILNYMI IDENTYFIKATORAMI WPROST Z SYSTEMU KONTROLI DOSTĘPU AEOS. JESZCZE NIGDY WCZEŚNIEJ NIE BYŁO TO TAKIE PROSTE. TERAZ JEST MOŻLIWE DZIĘKI INTEGRACJI CZYTNIKÓW ARCHITECT FIRMY STiD Z SYSTEMEM KONTROLI DOSTĘPU AEOS.

↓ Wymagania stawiane przez klientów nowoczesnym systemem kontroli dostępu ciągle się zmieniają, ale wyraźnie zauważalna jest tendencja ułatwiania dostępu i wygody użytkownika przy jednoczesnej poprawie bezpieczeństwa. Wydawałoby się, że te dwa elementy mogą pozostawać ze sobą w sprzeczności, ale nie wtedy,

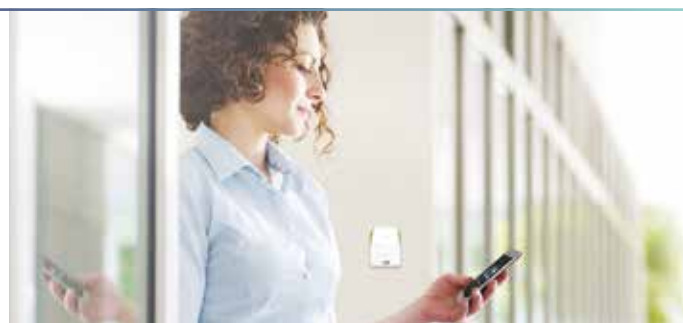
kiedy korzystamy z najnowszej integracji systemu **AEOS** z czytnikami **Architect** za pomocą aplikacji **STiD Mobile**.

Seria Architect firmy STiD to jedne z najbardziej elastycznych i zaawansowanych czytników kontroli dostępu na rynku. Aplikacja STiD Mobile zainstalowana w telefonie użytkownika systemu AEOS umożli-

wia jego identyfikację z wykorzystaniem aż pięciu możliwych trybów uwierzytelniania i odblokowanie przejścia. Wszystko z zapewnieniem zachowania bardzo wysokiego poziomu bezpieczeństwa: - zbliżenie telefonu z aplikacją STiD Mobile do czytnika; - przesunięcie ręki nad czytnikiem bez wyjmowania telefonu z kieszeni;

- stuknięcie dwa razy w telefon, gdy znajdujemy się przy czytniku; - użycie ikon w aplikacji, aby otworzyć wybrane drzwi; - użycie aplikacji na Apple Watch w celu otwarcia drzwi.

Mobilny identyfikator wydawany jest bezpośrednio z interfejsu systemu AEOS.



www.schrack-seconet.pl

Centrala sterująca urządzeniami ppoż. Integral EvoxX M



INTEGRAL EVOXX M PEŁNI FUNKCJE:

- centrali sygnalizacji pożarowej (zgodność z EN 54-2997+A1:2006),
 - zasilacza urządzeń ppoż. (EN 54-4:1997+A1:2002+A2:2006),
 - centrali sterującej urządzeniami ppoż. w systemach kontroli rozprzestrzeniania dymu i ciepła (KOT zgodnie z prEN 12101-9),
 - zasilacza do systemów kontroli rozprzestrzeniania dymu i ciepła (EN 12101-10:2005),
 - centrali sterującej SUG gazowymi (EN 12094-1:2003), wodnymi, pianowymi, aerozolowymi (KOT),
 - centrala sterująca i nadzorująca w ramach instalacji wodociągowych ppoż. (KOT).
- Centralę charakteryzuje niezawodność działania i elastyczna architektura systemu, praca w sieci - Integral LAN (do 16 central) i Integral WAN (do 4049 central), sterowanie i nadzorowanie SUG, zdalny dostęp do systemu - Integral Remote, współdziałanie z systemem integrującym urządzenia ppoż. SIS-FIRE.

STEROWANIE URZĄDZEŃ PPOŻ.

- przez we/wy centrali oraz moduły we/wy X-LINE,
- dowolne algorytmy sterowania dla wyjść sterujących,
- wyjścia sterujące z funkcją przełączenia w pozycję pożarowo-bezpieczną w przypadku uszkodzenia „fail-safe”,
- możliwość równoległego stosowania kilku kryteriów sterujących z konfigurowanymi priorytetami wykonywania zależnie od stanu pracy obiektu,
- sterowanie: wyjść w trybie ciągłym lub impulsowym, grupowe urządzeń (np. klapy ppoż.) do 8 A, kłapami z siłownikami w standardzie MP-BUS, z funkcją potwierdzenia zwrotnego,
- nadzór ciągłości przewodów zasilających sterujących urządzenia ppoż.,
- sterowanie ręczne umożliwiające przesterowanie wyjść uruchomionych automatycznie,
- blokowanie (zatrzaskiwanie) stanów występowania zależnie od stanu pracy systemu.

www.tp-link.com.pl

TP-Link EAP615-Wall – kompaktowy naścienny punkt dostępowy Wi-Fi 6

EAP615-WALL TO URZĄDZENIE O NOWOCZESNYM WZORNICTWIE, KTÓRE ŚWIETNIE SPRAWDZA SIĘ W POKOJACH HOTELOWYCH. JE- GO OBUDOWA MA ZALEDWIE 20 MM GRUBOŚCI. URZĄDZENIE IDE- ALNIE WKOMPONUJE SIĘ W KAŻDE WNĘTRZE, ZAPEWNIAJĄC PRZY TYM SILNY SYGNAŁ SIECI BEZPRZEWODOWEJ.

↓ Nowe technologie sieci Wi-Fi standardu **802.11ax**, takie jak modulacja **1024QAM** oraz długi symbol **OFDM**, umożliwiają urządzeniu osiągnięcie bardzo dużych prędkości, łącznie aż do 1800 Mb/s (do 574 Mb/s w paśmie 2,4 GHz oraz do 1201 Mb/s w paśmie 5 GHz).

Instalacja punktów dostępowych **EAP615-Wall** jest niezwykle prosta. Obsługa zasilania PoE w standardzie 802.3af/at całkowicie eliminuje dodatkowe okablowanie, a konstrukcja urządzeń umożliwia łatwy montaż w ściennej puszcze elektrycznej. EAP615-Wall nie jest standardowym punktem do-

stępowym. Działa także jak przełącznik, ponieważ zawiera trzy gigabitowe porty Ethernet, dzięki którym może zapewnić zasilanie PoE urządzeń przewodowych, takich jak telefony IP, kamery IP czy interkomy.

EAP615-Wall pozwala na utworzenie aż 16 niezależnych sieci Wi-Fi (SSID) z możliwością autoryzacji dostępu z uwierzytelnianiem przez Facebook albo SMS oraz logowaniem za pomocą strony powitalnej, jednorazowych haseł dostępu lub voucherów. Takie rozwiązanie znacząco zwiększa bezpieczeństwo całej sieci i wrażliwych danych.

EAP615-Wall może być centralnie zarządzany przez chmurę dzięki integracji z platformą Omada SDN. Produkt jest objęty 5-letnią gwarancją producenta.



NOWOCZESNY SYSTEM SYGNALIZACJI POŻAROWEJ



- ➔ 2286 urządzeń pętlowych w centrali (18 pętli x 127 urządzeń)
- ➔ Sygnalizatory adresowalne, w tym sygnalizatory w gniazdach czujek
- ➔ Zaawansowane czujniki chemiczne z detekcją dymu / temperatury / CO / COHb
- ➔ **ekho** – urządzenia bezprzewodowe z samokonfigurującą się siecią kratową (mesh network)
- ➔ Sieciowanie do 127 central
- ➔ Centrale z funkcją sterowania gaszeniem
- ➔ Szeroka gama urządzeń, w tym urządzenia iskrobezpieczne z certyfikatem ATEX
- ➔ Zaawansowane możliwości programowania sterowań przyczyna - skutek
- ➔ Certyfikaty: CNBOP, VdS, SIL2



50 2021 SECURITY

W roku 2021 obserwowaliśmy znaczny wzrost zainteresowania nowymi technologiami. Największym popytem cieszyły się rozwiązania w chmurze. Prognozuje się, że ten poziom w najbliższym czasie się utrzyma. Ale czy chmura jest panaceum na bieżące wyzwania związane z bezpieczeństwem użytkowników? Czy to idealna technologia, która sprawi, że problemy użytkowników znikną?

SECURITY 50

TECHNOLOGIE, KTÓRE DOMINOWAŁY W 2021 r.

T E K S T
William Pao
a&s International

W ykorzystanie chmury w zastosowaniach security, w formie dozoru wizyjnego jako usługi lub kontroli dostępu jako usługi, nabiera tempa. Według prognoz MarketsandMarkets wydatki na usługi VSaaS wzrosną z 2,2 mld USD w 2020 r. do 4,7 mld USD do 2025 r., przy CAGR wynoszącym 16%.

Rzeczywiście, wielu użytkowników przeniosło się do chmury ze względu na różne korzyści. – Model VSaaS zmniejsza koszty użytkowników, upraszcza zarządzanie aplikacjami i sprawia, że infrastruktura jest bardziej elastyczna. Sprawdza się nie tylko w scentralizowanym dozorze wizyjnym, ale także w centralizowanym zarządzaniu obsługą i konserwacją urządzeń oraz scentralizowanym przetwarzaniu sygnałów alarmowych – mówi Pan Lingyu, dyrektor produktu VSaaS w Dahua Technology.

– VSaaS sprawia, że użytkownicy końcowi ze wszystkich branż, bez względu na wielkość firmy, mogą posiadać zaawansowane rozwiązanie dozoru, które zaspokoi potrzeby w zakresie bezpieczeństwa, a przy tym jest łatwe w utrzymaniu w dłuższej perspektywie i może okazać się najbardziej opłacalne w całym cyklu życia systemu zabezpieczeń. Model partnerstwa i usług, jakie VSaaS udostępnia użytkownikom końcowym, producentom i integratorom, tworzy również znacznie trwalsze relacje i wskaźniki zwrotu z inwestycji, zapewniając jednocześnie klientom dostęp do najlepszych funkcji, dopasowanych do ich działalności. Klienci wiedzą, że zaufany partner jest tam, aby ich wspierać, jeśli pojawią

się jakiegokolwiek problemy lub obawy – podkreśla Danielle VanZandt, analityk branżowy ds. bezpieczeństwa we Frost and Sullivan.

Co więcej, wdrażanie chmury przyspieszyła pandemia. – Migracja do chmury na potrzeby analizy danych i kryminalistyki odbyła się szybciej, niż się spodziewałem. Pandemia zmusiła firmy do monitorowania wskaźników obłożenia budynków, rozmieszczenia miejsc siedzących i wielu innych tematów związanych ze zdrowiem. Ogólnie rzecz biorąc, chmura pozwoliła na szybszy rozwój tych produktów oraz szybszą dystrybucję i dostęp do nich – wyjaśnia Jason Glover, wiceprezes ds. sprzedaży w BCD.

– VSaaS nie jest koncepcją nową, od wielu lat jest stosowana w branży zabezpieczeń. W ostatnim czasie stała się znacznie bardziej popularna, ponieważ pandemia wymusiła działania online. Wdrażanie VSaaS przyspieszył również rozwój mobilnego Internetu, technologii IoT i 5G – mówi Keen Yao, wiceprezes Hikvision. – Oparta na chmurze usługa VSaaS umożliwia użytkownikom przeglądanie zdarzeń alarmowych w czasie rzeczywistym za pośrednictwem aplikacji i wykonywanie zdalnych zadań inspekcyjnych. Daje to ogromne korzyści w zakresie wydajności, elastyczności, opłacalności i bezpieczeństwa. Od rynków małych firm aż po poziom przedsiębiorstw widzimy znaczny wzrost firm korzystających z VSaaS.

POPULARNOŚĆ CHMURY WZRASTA, ALE CZY TO PANACEUM NA WSZYSTKIE WYZWANIA ZWIĄZANE Z BEZPIECZEŃSTWEM?

Większe zainteresowanie nie oznacza, że chmura jest idealnym rozwiązaniem, które zaspokaja wszystkie potrzeby użytkowników. Faktycznie, niedawne badanie asmag.com Technologie, które wpływają na bezpieczeństwo pokazało, że VSaaS plasuje się tylko nieznacznie powyżej średniego poziomu przydatności i dojrzałości.



– Oferta chmurowa uznanych głównych dostawców monitoringu wizyjnego zazwyczaj stanowi niewielką część ich działalności. Specjalistyczne oferty od nowych dostawców dopiero zaczynają konkurować z dawnymi rozwiązaniami. Obecnie uważamy, że wiele ofert dozoru wizyjnego w chmurze jeszcze nie dojrzało do potrzeb rynku – twierdzą Josh Woodhouse, główny analityk i założyciel Novaira Insights, oraz Jon Cropley, główny analityk w Novaira Insights. Chmura ma potencjał wysokiego wzrostu, ale małą bazę dostawców. Istnieją pewne wyzwania związane z wdrażaniem rozwiązań chmurowych. Przechowywanie nagrań w chmurze przez długi czas, zgodnie z wymaganiami branży, może być dość kosztowne, nie wspominając o tym, że niektóre branże nawet nie zezwalają na zdalne przechowywanie. Istnieją też obawy dotyczące ochrony danych osobowych i cyberbezpieczeństwa.

– Obawy związane z cyberbezpieczeństwem monitoringu wizyjnego w chmurze zostały spotęgowane włamaniem się hakerów do 150 tys. kamer Verkada wiosną 2021 r. – mówi Joon Jun, prezes IDIS Global Business Division. – Jest również sporo innych problemów do pokonania, ponieważ większość dostawców VSaaS oferuje tylko niewielką gamę kamer 2-Mpix, które nie nadają się do każdego zastosowania. Przykładowo kamera 2-Mpix z obiektywem typu rybie oko lub kamera panoramiczna nie zapewnią menedżerom ds. bezpieczeństwa wydajności potrzebnej do niezawodnej detekcji, rozpoznania i identyfikacji przestępcy. Brak specjalistycznych kamer, a także bardziej popularnych obecnie modeli, takich jak 5-Mpix i 8-Mpix PTZ, ograniczy wdrożenia do zastosowań wewnętrznych, które nie wymagają pokrycia rozległych obszarów.

W rezultacie dla wielu użytkowników najlepszym wyborem stały się rozwiązania hybrydowe. – Rozwiązania hybrydowe najlepiej wykorzystują chmurę, środowiska on-premise i edge computing w odniesieniu do potrzeb klienta. Wiele czynników będzie wpływać na jego decyzję. Specyficzny charakter i funkcjonalność potrzebna w rozwiązaniach bezpieczeństwa, polityka i regulacje dotyczące przetwarzania i ochrony danych, cyberbezpieczeństwo, zasoby systemu, zarządzanie i konserwacja oraz wiele innych kwestii będzie wpływać na wybór najbardziej odpowiedniego połączenia środowisk pracy. Wierzymy, że większość rozwiązań dozoru wizyjnego będzie

oparta na modelu hybrydowym – podkreśla Ray Mauritsson, dyrektor generalny Axis Communications.

W tym kontekście większość ekosystemu kontroli dostępu opiera się na formie rozwiązania chmury hybrydowej. – Na przykład udostępnianie urządzeń odbywa się poprzez chmurę, podobnie jak dystrybucja oprogramowania. Kontrola i zarządzanie dostępem są zwykle wdrażane częściowo lokalnie, częściowo w chmurze. Najważniejsze są niewielkie opóźnienia i wysoka niezawodność, ale coraz istotniejsze stają się również zdalne monitorowanie, kontrola i analityka. Nasze platformy są otwarte na obsługę tych i innych modeli pracy – mówi Vince Wenos, SVP i CTO Allegion.

Zapewne model chmury hybrydowej nie straci na popularności w najbliższych latach. – Rozwiązania oparte na chmurze już się pojawiły i będą się rozwijać. Myślę, że niektóre przepisy prawa i zasady korzystania z chmury należy zweryfikować. W niektórych sektorach wertykalnych nie wolno przenosić danych z systemu dozoru wizyjnego do chmury. Nie oznacza to jednak, że nie można zarządzać tymi systemami przez chmurę. Wierzę, że zarządzanie katalogami, użytkownikami itp. przeniesie się do chmury, a cała pamięć masowa pozostanie na razie na miejscu – wyjaśnia J. Glover.

INNE ISTOTNE TRENDY TECHNOLOGICZNE

Oprócz chmury na rynku zabezpieczeń technicznych w 2021 r. stosowano szerzej także inne technologie, które będą wpływać na bezpieczeństwo w najbliższym czasie. Oto one.

AI w monitoringu wizyjnym

W badaniu asmag.com sztuczna inteligencja (AI) zajmuje wysoką pozycję pod względem zarówno dojrzałości, jak i podatności. Przewiduje się, że zainteresowanie użytkowników nie osłabnie. – Zainteresowanie rozwiązaniami sztucznej inteligencji w dozorcze wizyjnym znacznie wzrosło od 2019 r. Z powodu zamknięcia lub tylko częściowego otwarcia wielu obiektów menedżerowie ds. bezpieczeństwa mieli więcej czasu na ocenę oprogramowania opartego na AI i głębokim uczeniu się. Wcześniejsze zastosowania były hamowane przez przedwczesne premiery, a niektórzy dostawcy przesadzili z obietnicami. Ale dzisiaj algorytmy znacznie się poprawiły – mówi J. Jun. – Przykładowo, kiedy po raz pierwszy wpro-



wadziłyśmy nasze rozwiązanie AI, osiągałyśmy dokładność 96–97%. Dziś najnowsza wersja IDIS Deep Learning Analytics zapewnia 98-proc. precyzję. Na początku 2021 r. nasi integratorzy systemów i użytkownicy końcowi wyrazili przekonanie, że sztuczna inteligencja nie tylko usprawni operacje związane z bezpieczeństwem, ale także będzie w stanie zapewnić dodatkową wartość wielu interesariuszom.

Popyt na sztuczną inteligencję zwiększył się w ostatnich latach i ta tendencja ma się utrzymać również w 2022 r. – Implementacje AI w urządzeniach końcowych, brzegowych i chmurowych zwiększyły popyt na nie w pokrewnych dziedzinach i różnych branżach. Wraz z ewolucją technologii analityka oparta na AI będzie stopniowo implementowana w produktach z coraz niższej półki, co z pewnością ucieszy użytkowników – zapowiada Yin Jun, wiceprezes centrum badawczo-rozwojowego w Dahua Technology.

AI, a dokładniej głębokie uczenie się, to bez wątpienia dziedzina, która napędza rozwój innowacji, na którą istnieje znaczne zapotrzebowanie. Korzyści płynące z głębokiego uczenia się nie tylko zwiększą możliwości rozwiązań dozorowych zaprojektowanych z myślą o bezpieczeństwie i ochronie, ale także otworzą nowe zastosowania w zakresie wydajności operacyjnej i skuteczności – prognozuje R. Mauritsson.

Coraz częściej sztuczna inteligencja będzie implementowana w urządzeniach brzegowych, napędzana przez bardziej wydajne układy SoC kamer obsługujących złożone algorytmy. – W systemach zabezpieczeń popularne stają się aplikacje AI umożliwiające np. automatyczne rozpoznawanie tablic rejestracyjnych, ostrzeganie o zdarzeniach, zliczanie osób, tworzenie map ciepła, wykrywanie nieprawidłowego parkowania, kasków na głowie, a także wiele innych. Dzięki szybszemu przetwarzaniu w urządzeniach brzegowych i zopty-

malizowanym algorytmom sztucznej inteligencji upowszechni się wykorzystanie kamer dozorowych do bardziej inteligentnych zadań – mówi Yao.

Najnowsza generacja chipsetów, które będą szerzej dostępne na rynku w 2022 r., pozwalają na większe przetwarzanie w urządzeniach brzegowych. Niektórzy dostawcy zintegrowali już te chipsety z najnowszymi liniami kamer. Inni wkrótce pójdą w ich ślady. Nadal rozwija się środowisko systemowe, umożliwiające instalowanie w kamerach różnych aplikacji opartych na AI. To nie jest nowa koncepcja. Jednak poprawa wydajności analityki w połączeniu z większymi możliwościami przetwarzania najnowszych chipsetów sprawia, że koncepcja ta staje się atrakcyjniejsza dla integratorów i użytkowników końcowych – podkreślają Woodhouse i Cropley.

Technologie bezdotykowe

Rozwiązania bezdotykowe cieszą się wzmożonym popytem ze względu na nadal odczuwalne skutki pandemii. – Identyfikacja biometryczna i inne technologie bezdotykowe były bardziej popularne przez cały 2021 rok, gdyż wielu użytkowników końcowych zaczęło opracowywać swoje strategie powrotu do pracy i zrestartowania wielu unormowanych operacji w dobie pandemii – wyjaśnia VanZandt. – Zmiana nastrojów klientów z dala od miejsc pracy, a także wzrost liczby zdalnych operacji i zarządzania stworzyły również nowe modele operacyjne dla wewnętrznych zespołów bezpieczeństwa poprzez zintegrowane operacje zarówno zdalne, jak i na miejscu.

Cyberbezpieczeństwo

W badaniu asmag.com cyberbezpieczeństwo i związane z nim rozwiązania również znalazły się wysoko. – Wraz z nasileniem się ataków ransomware i killware cała branża będzie musiała zwiększyć wysiłki na rzecz ochrony systemów, urządzeń i klientów. O ile technologie bezpieczeństwa chmury i sieci rozwijają się i są szybko wdrażane, o tyle cyberzabezpieczenia na poziomie urządzeń i systemów zabezpieczeń mogą w 2022 r. pozostać daleko w tyle. Wbudowane uwiarytelnianie sprzętowe i technologie potrzebne do jego zapewnienia staną się znacznie bardziej powszechne w ciągu najbliższych kilku lat – mówi V. Wenos.

– Coraz większy nacisk musi zostać położony na bezpieczeństwo i ochronę danych. Liczba cyberataków rośnie, a szkody nimi wywołane są teraz ogromne. Tutaj widzę rolę MOBOTIX jako pioniera w branży. Cyberbezpieczeństwo „Made in Germany” jest częścią DNA naszej firmy – informuje Thomas Lausten, dyrektor generalny MOBOTIX. – Cyberbezpieczeństwo ma najwyższy priorytet w MOBOTIX. Jest realizowane i wdrażane w całej koncepcji MOBOTIX Cactus. Elementarne dla nas jest również bezpieczeństwo danych w odniesieniu do niemieckiej ustawy o ochronie danych osobowych (DSGVO).

Cyfrizacja i integracja

Ważne są technologie, które rozszerzają zastosowanie systemów dozoru wizyjnego poza systemy zabezpieczeń. – Analityka wizyjna jest typowym przykładem, jednak specjalistyczne urządzenia IoT też mają do odegrania dużą rolę na rynku. Przykładowo zintegrowanie czujników (IoT) parametrów środowiskowych z systemem dozoru wizyjnego wniesie nowe typy danych, co w efekcie przyniesie nowe zastosowania i dodatkowe wartości – zapowiadają J. Woodhouse i J. Cropley.

Ten trend do integracji również ma związek z pandemią, która zmusiła użytkowników do ograniczenia pracochłonnych procesów i cyfrowego modelu pracy. – Nic dziwnego, że na całym świecie istnieje zapotrzebowanie na integrację różnych systemów zabezpieczeń, m.in. wykrywania intruzów, sygnalizacji pożarowej, bezdotykowej kontroli dostępu i zarządzania gośćmi, z popularnymi bazami danych, takimi jak Microsoft Active Directory, a także systemami specyficznymi dla danego sektora, np. point-of-sale (POS) w handlu detalicznym, logistyki i operacji produkcyjnych – mówi Jun. ☉



Największe firmy

branży security na świecie

2021	2020	NAZWA FIRMY	SIEDZIBA	GŁÓWNY OBSZAR DZIAŁANIA	PRZYCHODY W 2020 R. (MLN USD)	PRZYCHODY W 2019 R. (MLN USD)	WZROST PRZYCHODÓW (2020-2019)
1	1	HIKVISION DIGITAL TECHNOLOGY (Video Surveillance)	CHINY	różne	8309,4	7713,2	7,7%
2	2	DAHUA TECHNOLOGY	CHINY	różne	3835,7	3789,8	1,2%
3	3	ASSA ABLOY (Electromechanical and electronic locks)	SZWECJA	kontrola dostępu	2951,8	3166,7	-6,8%
4	5	AXIS COMMUNICATIONS	SZWECJA	różne	1256,2	1281,9	-2,0%
5	N/D	MOTOROLA SOLUTIONS (Video Security and Analytics)	USA	różne	927,0	709,0	30,8%
6	7	UNIVIEW TECHNOLOGIES	CHINY	telewizja dozorowa	765,2	715,9	6,9%
7	6	TIANDY TECHNOLOGIES	CHINY	telewizja dozorowa	688,9	620,9	10,9%
8	8	ALLEGION (Electronic Products and Access Control)	USA	kontrola dostępu	571,2	599,3	-4,7%
9	10	TKH GROUP (Vision & Security Systems)	HOLANDIA	różne	459,3	468,3	-1,9%
10	9	HANWHA TECHWIN	KOREA	telewizja dozorowa	448,6	492,0	-8,8%
11	11	AIPHONE	JAPONIA	interkomy	432,3	454,3	-4,8%
12	12	INFINOVA	CHINY	telewizja dozorowa	423,4	394,7	7,3%
13	14	ZKTECO	CHINY	różne	261,1	253,7	2,9%
14	15	STREAMAX TECHNOLOGY	CHINY	mobilna telewizja dozorowa	233,2	226,6	2,9%
15	N/D	SMARTSENS TECHNOLOGY	CHINY	telewizja dozorowa (obiektyw)	221,3	98,4	124,8%
16	N/D	INTELBAS	BRAZYLIA	różne	217,1	190,5	14,0%
17	18	DONGGUAN YUTONG OPTICAL TECHNOLOGY	CHINY	telewizja dozorowa (obiektyw)	213,3	178,4	19,6%
18	16	VIVOTEK	TAJWAN	telewizja dozorowa	188,2	213,0	-11,6%
19	17	KEDACOM (Video Surveillance)	CHINY	telewizja dozorowa	161,3	201,0	-19,8%
20	20	NEDAP	HOLANDIA	różne	158,8	167,6	-5,3%
21	19	CP PLUS	INDIE	telewizja dozorowa	158,0	164,5	-4,0%
22	21	MILESTONE SYSTEMS	DANIA	telewizja dozorowa	155,5	157,0	-0,9%
23	25	RAYSHARP	CHINY	telewizja dozorowa	136,1	121,1	12,3%
24	29	IDIS	KOREA	telewizja dozorowa	125,7	91,6	37,2%
25	22	TAMRON (Commercial / Industrial use optics)	JAPONIA	telewizja dozorowa (obiektyw)	125,5	134,7	-6,768%
26	27	WANJIAAN INTERCONNECTED TECHNOLOGY	CHINY	telewizja dozorowa	114,3	112,7	1,4%
27	30	TVT DIGITAL TECHNOLOGY	CHINY	telewizja dozorowa	114,3	92,2	24,0%

28	24	OPTEX (Security Sensors)	JAPONIA	sygnalizacja włamania	113,1	124,19	-8,9%
29	23	COMMAX	KOREA	Automatyzacja i Home Security	110,6	121,35	-8,9%
30	36	NAPCO SECURITY TECHNOLOGIES	USA	różne	101,4	102,93	-1,5%
31	28	BCD	USA	telewizja dozorowa	101,1	93,96	7,6%
32	26	KOCOM	KOREA	Automatyzacja i Home Security	100,9	113,55	-11,2%
33	37	IDENTIV	USA	kontrola dostępu	86,9	83,76	3,8%
34	34	FUJIAN FORECAM OPTICS	CHINY	telewizja dozorowa (obiektyw)	84,7	83,54	1,3%
35	32	ZENITEL	NORWEGIA	interkomy	83,2	86,95	-4,3%
36	35	MOBOTIX	NIEMCY	telewizja dozorowa	80,2	79,71	0,6%
37	38	C-PRO ELECTRONICS	KOREA	telewizja dozorowa	71,9	72,41	-0,7%
38	33	SUPREMA	KOREA	kontrola dostępu	71,3	83,35	-14,5%
39	N/D	GALLAGHER	NOWA ZELANDIA	kontrola dostępu	70,1	81,17	-13,7%
40	40	COSTAR TECHNOLOGIES	USA	telewizja dozorowa	60,4	69,53	-13,1%
41	N/D	FOCTEK PHOTONICS	CHINY	telewizja dozorowa (obiektyw)	52,9	57,89	-8,7%
42	N/D	BLUESKY TECHNOLOGIES	CHINY	telewizja dozorowa	47,8	38,23	25,0%
43	41	DYNACOLOR	TAJWAN	telewizja dozorowa	39,9	61,17	-34,7%
44	44	GEOVISION	TAJWAN	telewizja dozorowa	39,3	46,88	-16,2%
45	42	SYNECTICS (System Division)	WLK. BRYTANIA	telewizja dozorowa	30,4	52,03	-41,7%
46	48	HI SHARP ELECTRONICS	TAJWAN	telewizja dozorowa	28,7	28,13	2,2%
47	47	ITX AI	KOREA	telewizja dozorowa	27,3	27,02	0,9%
48	31	SENSTAR TECHNOLOGIES	IZRAEL	różne	23,7	25,26	-6,2%
49	45	HITRON SYSTEMS	KOREA	telewizja dozorowa	23,1	31,66	-27,0%
50	50	ACTI	TAJWAN	telewizja dozorowa	14,5	18,26	-20,9%

→ 0 RAPORCIE

a&s Security 50 to coroczny ranking 50 największych producentów systemów zabezpieczeń na świecie, oparty na przychodach i zyskach ze sprzedaży urządzeń i rozwiązań bezpieczeństwa. Jeden z najczęściej czytanych i długoletnich rankingów branżowych. Analizując dane notowane w publicznych lub przesłanych raportach finansowych za rok 2020, wyróżniam zarówno światowych liderów, jak i nowe podmioty na rynku. Ranking ma odzwierciedlać dynamikę i rozwój branży, która porusza się w ciągłe zmieniającym się krajobrazie biznesowym i technologicznym. Naszym celem jest

przedstawienie obrazu rynku i ułatwienie podejmowania decyzji o strategiach biznesowych, zarządzaniu przedsiębiorstwem, badań i rozwoju, rozwoju biznesu i innych ważnych tematów.

W RANKINGU „SECURITY 50” MOGŁY WZIĄĆ UDZIAŁ NASTĘPUJĄCE FIRMY:

- Dostawcy elektronicznych urządzeń i systemów opartych na oprogramowaniu z zakresu: dozoru wizyjnego, kontroli dostępu i sygnalizacji włamania, specjalizujących się zarówno w kluczowych elementach, jak i wielu segmentach produktowych.
- Przedsiębiorstwa z branży ochrony lub zajmujące się wyłącznie produkcją, posiadające własne produkty, systemy, marki lub rozwiązania.

- Wyłączone zostały przychody z dystrybucji i integracji systemów, z działalności resellerskiej i dealerskiej, instalacji, usług ochrony, ochrony danych (informacji) i zabezpieczania ppoż. oraz inne powiązane.

- Podmioty, które przedstawiły sprawozdania finansowe za rok budżetowy 2020 i rok budżetowy 2019, zbądane i zatwierdzone przez biegłego księgowego lub firmę księgową.
- Publicznie notowane spółki giełdowe, a także niewielka liczba prywatnych, międzynarodowych firm, które wyraziły zgodę na udostępnienie swoich certyfikowanych raportów rocznych. Przed zakwalifikowaniem ich do rankingu są one szczegółowo weryfikowane przez zespół redakcyjny a&s pod kątem rozpoznawalności marki i udziałów w globalnym rynku.

UWAGI DO DANYCH FINANSOWYCH:

a&s nie ponosi odpowiedzialności za informację finansowe dostarczone przez poszczególne firmy.

W celu rzetelnego porównywania waluty spoza USA zostały one przeliczone na podstawie średnich rocznych kursów walut podanych przez Internal Revenue Service (IRS), działający według uchwalonej przez Kongres USA ustawy *Internal Revenue Code*.

W rezultacie powstało jak najbardziej obiektywne zestawienie firm, które podzieliły się swoimi wynikami sprzedaży za lata 20219-2020.

SEKRET FIRM

ODPORNYCH NA KRYZYS
WYWOŁANY PRZEZ PANDEMIE

Sektor security od dawna jest uznawany za niepoddający się kryzysom, osiągając wzrosty nawet w najtrudniejszych czasach. W roku 2020 wydarzyło się coś bezprecedensowego, po raz pierwszy bowiem w historii „Security 50” z 2021 r. liczba firm zgłaszających mniejsze zyski w przychodach (rok do roku) przewyższyła liczbę firm notujących wzrost, gdyż aż 28 firm zgłosiło spadek przychodów, a tylko 22 odnotowały wzrost.

Pandemia odbiła się na światowej gospodarce, wpływając na różne sektory, m.in. zabezpieczeń technicznych. W obliczu spadku przychodów w 2020 r. odnotowanych przez firmy branży security niektóre z nich wykazały się jednak większą odpornością na recesję. Pogorszenie koniunktury miało wiele wspólnego ze zmianami w przychodach.

– Rok 2020 był okresem niespotykanych globalnych wyzwań i odczuliśmy to również w Milestone. Pomimo trudnych warunków udało nam się jednak osiągnąć przychód netto powyżej 1 mld DKK (134 mln euro) już drugi rok z rzędu. Nadal rozwijamy naszą organizację – powiedział Thomas Jensen, dyrektor generalny Milestone Systems.

– Pierwsza połowa roku fiskalnego 2020/21 charakteryzowała się trudnymi warunkami, szczególnie w regionie Azji i Pacyfiku (APAC), który ucierpiał z powodu wielu powtarzających się blokad spowodowanych pandemią COVID-19. W szczególności zmalała liczba nowych projektów, mocno ucierpiały hotelarstwo i handel detaliczny. Te straty trudno będzie zrekomensować – podkreślił Thomas Lausten, dyrektor generalny MOBOTIX. – Z kolei w regionie DACH, krajach skandynawskich i na Bliskim Wschodzie zgodnie z oczekiwaniami firmy sprzedaż wzrosła w porównaniu z poprzednim rokiem budżetowym.

NAJBARDZIEJ ODPORNE FIRMY
(WZROST PRZYCHODÓW W LATACH 2020–2019)

S50 Ranking	Firma	Siedziba	Wzrost (%)
15	Smartsens Technology	Chiny	124,9
24	IDIS	Korea Płd.	37,2
5	Motorola Solutions (Video Security and Analytics)	Stany Zjednoczone	30,8
43	Bluesky Technologies	Chiny	25
27	TVT	Chiny	24
17	YTOT	Chiny	19,5
16	Intelbras	Brazylia	14
23	Raysharp	Chiny	12,4
7	Tiandy Technologies	Chiny	11
1	Hikvision Digital Technology	Chiny	7,7

FIRMY, KTÓRE WYKAZAŁY SIĘ ODPORNOŚCIĄ

Mimo tych wyzwań niektóre firmy branży security nadal wykazywały odporność na przeciwności losu i odnotowały w tym czasie znaczny wzrost. Niektórym udało się zachować rentowność. Jaki jest klucz do ich sukcesu?

ZARZĄDZANIE DOBRZE REALIZOWANYM
ŁAŃCUCHEM DOSTAW

Kluczowe znaczenie ma gwarancja dostarczania klientom zamówionych produktów na czas. – Podczas gdy wielu dostawców systemów zabezpieczeń zmagano się z problemami zakłócenego łańcucha dostaw, ponieważ zaopatrujące je zakłady produkcyjne zostały zamknięte, fabryka IDIS w Korei Południowej działała przez cały czas pandemii. Strategicznie ukierunkowaliśmy dostawy na regiony o ciągłym wzroście, jednocześnie upewniając się, że nasi partnerzy w Europie, na Bliskim Wschodzie i w USA mają zapasy potrzebne do kontynuowania projektów bez przeszkód – stwierdził Jon Jun, prezes IDIS Global Business Division.

BCD z siedzibą w USA notująca wzrost przychodów wykazała się elastycznością i szybkością działania. – Mieliliśmy dużo szczęścia, ponieważ wszystko mogło pójść w przeciwnym kierunku. Nasz wiceprezes ds. globalnych operacji łańcucha dostaw wcześniej pracował dla dystrybutora/dostawcy jako kierownik ds. zamówień obejmujących towary z Chin. Dlatego miał już doświadczenie w tym, jak szybko Chiny zamykają się, gdy coś dzieje się nie tak. W styczniu 2020 r. wyciekły informacje, że Światowa Organizacja Zdrowia interesuje się Wuhan w Chinach. Następnego dnia zamówiliśmy cztery regularne miesięczne dostawy produktów OEM firmy Dell. Trzy dni później Chiny zostały zamknięte. Byliśmy w stanie wykorzystać zapasy firmy Dell w Meksyku, ponieważ wszystkie chińskie komponenty tam dotarły. Dzięki szybkiej reakcji byliśmy z dostawą na czas, nigdy nie spóźniliśmy się i choć brzmi to zaskakująco, nasz średni czas dostawy do klienta podczas pandemii w 2020 r. skrócił się o 2,5 proc. (z 4,77 do 4,65 dni) w porównaniu z poprzednim nie COVID-owym rokiem 2019. Średnia 4,65 dnia pozostała niezmienna w 2021 roku. Mówimy o dniach, a nie tygodniach. To niespotykane nie tylko na rynku zabezpieczeń technicznych, ale także wszędzie indziej – ocenił Jeff Burgess, dyrektor generalny BCD.

ROZWIĄZANIA DOSTOSOWANE DO POTRZEB KLIENTA

Kluczowe znaczenie miało również oferowanie rozwiązań, które zaspokajały specjalne potrzeby klientów. – W niektó-

rych przypadkach pandemia zwiększyła popyt na rozwiązania security. Zaobserwowaliśmy np. wzrost liczby 24-godzinnych sklepów bezobsługowych w Korei Południowej. W tych punktach sprzedaży kamery IDIS monitorują ruch klientów w sklepie, a materiał filmowy w czasie rzeczywistym jest wyświetlany na ekranach. Rozwiązanie dla obiektów handlowych IDIS IoT bazuje na rozpoznawaniu twarzy do celów rejestracji, dostępu, płatności i wyjścia. Sklepy te korzystają również z coraz większego wyboru innych urządzeń i czujników IoT, które można łatwo zintegrować z naszymi rejestratorami NVR, aby zdalnie alarmowały personel i służby ratunkowe w przypadku zagrożeń – podkreślił J. Jun.

Zgodność ze standardem NDAA jest kolejnym przykładem przytoczonym przez prezesa IDIS Global Business Division. – Przez cały 2020 r. koncentrowaliśmy się na migracji naszych kamer, rejestratorów i serwerów korporacyjnych, aby nie korzystać z chińskich chipsetów (SOC) i innych chińskich komponentów. To była strategia, która się opłaciła – powiedział. – W Stanach Zjednoczonych istniał już znaczny popyt na urządzenia zgodne z NDAA, ale po wyjściu z pierwszej fali pandemii wiele większych organizacji w regionie EMEA również zdało sobie sprawę z konsekwencji zaostrzenia przepisów dla ich handlu ze Stanami Zjednoczonymi i ryzyka, jakie zainstalowanie chińskich urządzeń do dozoru wizyjnego może stanowić dla ich przyszłych planów handlowych z USA.

INWESTOWANIE W LUDZI I TECHNOLOGIE

Choć w ub.r. koniunktura się pogorszyła, to niektóre firmy utrzymały rentowność. Zamiast obniżać koszty, zainwestowały w ludzi i technologię, co według nich było kluczem do sukcesu.

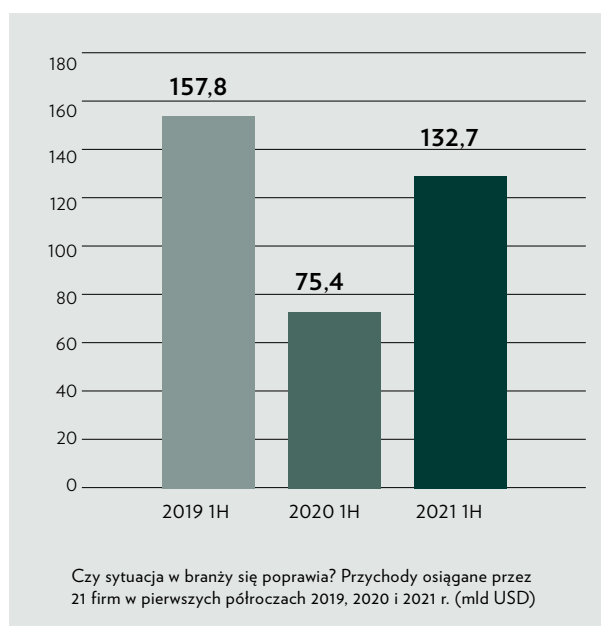
– Pomimo zysku niższego od oczekiwań nie odnotowaliśmy spadku obrotów. Oprócz oszczędności wynikających z rygorów pandemii (koszty podróży, koszty marketingu, odwołane targi) nie uruchomiliśmy programu oszczędnościowego, ale więcej inwestowaliśmy w innowacje i pozycjonowanie MOBOTIX jako kompletnego i kompleksowego dostawcy usług w zakresie inteligentnych technologii wizyjnych – przyznał T. Lausten. – Przez trzy lata, nawet w czasie pandemii, rygorystycznie dążyliśmy do naszego celu, jakim jest uznanie MOBOTIX za dostawcę technologii wizyjnych do każdego projektu na całym świecie, elastyczność na przyszłość i cyberbezpiecznych niezależnie od wielkości, liczby lokalizacji, wymagań lub branży.

– Atutem Senstar są pracownicy, dlatego w czasie pandemii kierownictwo przyjęło podejście propracownicze, utrzymując wynagrodzenia i poziom zatrudnienia. Senstar prowadził również przejrzystą wobec pracowników politykę dot. strategii, którą popierali. Jesteśmy wdzięczni, że nasi pracownicy pozostali oddani Senstar i dawali z siebie wszystko, aby utrzymać firmę na dobrej drodze w tym trudnym czasie – podkreśli Fabien Haubert, dyrektor zarządzający Senstar. – Ogólnie rzecz biorąc, Senstar działał ostrożnie. Nie podjęliśmy żadnych konkretnych kroków w celu redukcji kosztów, ale zamiast tego ściśle monitorowaliśmy niestrawne koszty i wydatki. Jednocześnie kontynuowaliśmy inwestycje w badania i rozwój oraz innowacje, utrzymując także sprzedaż, by udowodnić, że możemy nadal zaspokajać potrzeby klientów.

– Kluczem do sukcesu Milestone są przede wszystkim nasi ludzie. Z punktu widzenia przywództwa ważne było unikanie restrukturyzacji i dbanie o bezpieczeństwo pracowników oraz ich dobre samopoczucie w zespole. Aby to wesprzeć, uruchomiliśmy program Grow Together, który koncentruje się na zdrowiu psychicznym i fizycznym oraz dzieleniu się wiedzą na temat ćwiczeń, jedzenia i snu. Ponadto udało nam się sprostać ambicjom inwestowania w ludzi i rozwój, zwiększając liczbę pracowników o 69 osób, osiągając w końcu 2020 r. zatrudnienie na poziomie prawie 1000 pracowników – powiedział T. Jensen. – W pewnym sensie pandemia posłużyła jako test warunków skrajnych dla kultury naszej firmy i podejścia „People First”, które okazały się silne i odporne. Potrafimy przetrzymać kryzys w branży i poza nią.

PERSPEKTYWY WZROSTU W ROKU BUDŻETOWYM 2021/22

Patrząc na dane z raportu, szybkie porównanie przychodów firm (liczba firm $n = 21$) w pierwszych półroczach (1H) ostatnich 3 lat pokazuje, że firmy osiągnęły lepsze wyniki w pierwszej połowie 2021 r. w porównaniu z tym samym okresem w 2020 r. Wzrost nie osiągnął jednak poziomu z 2019 r.



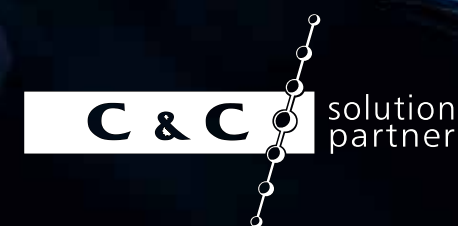
Większość firm pytana o perspektywy wzrostu na ten i przyszły rok wyrażała optymizm.

– Byliśmy nieco rozpieszczeni, ponieważ przez ostatnie dziesięć lat odnotowywaliśmy z roku na rok wzrosty. Dlatego poniekąd tego oczekujemy. Trzeci kwartał 2020 r. był dla nas najlepszym kwartałem do tej pory. Wielkość osiągniętych wówczas przychodów dzięki zatrudnieniu cudzoziem-



ców powinna zostać przekroczona w IV kwartale – przyznał J. Burgess z BCD. – Ponieważ pandemia wciąż jest z nami, mamy oczy szeroko otwarte, wiedząc, że wszystko może nagle zostać zamknięte. Blokady mogą zostać ogłoszone przez władze zarówno stanowe, jak i lokalne, zamknięcie może też dotyczyć różnych rynków wertykalnych. Wtedy integrator systemu zabezpieczeń nie może wykonać instalacji z powodu wstrzymania działalności. Tak więc trzymamy rękę na pulsie i kontrolujemy wszystko, co możemy. Zawsze oczekujemy wzrostu, a teraz bardziej niż kiedykolwiek tego samego oczekują również inwestorzy!

– Mamy duże oczekiwania na lata 2021–2022, widząc, że branża odzyskuje siły po blokadach i ograniczeniach. Spodziewamy się, że będziemy w stanie wznowić projekty, które zostały wstrzymane z powodu COVID-19, chociaż podróże do niektórych miejsc nadal stanowią problem. Senstar ma doskonałą platformę pozwalającą przewyższyć ograniczenia podróży i zapewnić najlepszą obsługę oraz wsparcie dla klienta, ponieważ 50 proc. naszych pracowników działa na rynkach lokalnych, w pobliżu baz naszych klientów – podkreślił F. Haubert. ●



30
lat na rynku

24
lata w holdingu



www.ccpartners.pl

SZANSE I ZAGROŻENIA RYNKU

DOZORU WIZYJNEGO

Rok 2020 przyniósł zmiany, których nikt nie mógł przewidzieć. COVID-19 diametralnie zmienił nasze życie. Po dwóch latach pandemii przed nami wciąż wiele wyzwań. Zarządzanie zaburzonym łańcuchem dostaw, nowe zagrożenia bezpieczeństwa cyfrowego i fizycznego, zmieniające się oblicze biznesu – wszystko to wymagało wprowadzenia innowacji.

TEKST
Prasanth Aby Thomas

W roku 2020 pandemia doprowadziła do niemal całkowitego wstrzymania aktywności fizycznej. Klienci przerwali rozpoczęte projekty, odłożyli nowe inwestycje i zaczęli szukać sposobów na zminimalizowanie strat. Integratorzy nie mogli podjąć pracy w terenie, musieli więc znaleźć sposoby na funkcjonowanie w nowej rzeczywistości.

DZIAŁANIA PRODUCENTÓW W 2020 R.

Niektórzy producenci swoją szansę dostrzegli w rozwiązaniach do pomiaru temperatury ciała. Wykorzystanie kamer dozorowych do kontroli zachowania dystansu

społecznego i zarządzania liczbą osób mogących przebywać w pomieszczeniu stało się powszechne. Przemysł i biznes musiały się zmienić. Badano nowe modele biznesowe. Poszukiwano nowych zastosowań dla starych produktów. Czasami wydawało się, że jest dużo czasu, a mało pracy, innym razem, że jest za dużo pracy, a zbyt mało czasu. Być może chęć położenia kresu zamieszaniu była motywacją dla wielu firm, które podwoiły wysiłki, by – inwestując w badania i rozwój – sprostać zmieniającym się potrzebom klientów.

Według Matta Tengwalla, dyrektora generalnego ds. oszustw i rozwiązań bezpieczeństwa w firmie Verint, by nadal prosperować i się rozwijać, firmy na całym świecie modyfikują metody działania.

COVID-19 PRZYSPIESZYŁ POSTĘP NA RYNKU

ZABEZPIECZEŃ TECHNICZNYCH.

PRZEMODELOWANIE PRIORYTETÓW PRZEZ

KLIENTÓW WPŁYNĘŁO NA POPYT,

OGRANICZENIA EPIDEMICZNE NATOMIAST

UNIEMOŻLIWIŁY REALIZACJĘ WIELU

PROJEKTÓW

– Skorzystaliśmy z okazji, aby wesprzeć naszych kontrahentów w obsłudze ich klientów i zapewnić im pomoc techniczną – powiedział M. Tengwall. – W miarę pojawiania się nowych wyzwań, dzięki wiodącej pozycji Verint na rynku bankowym wiedzieliśmy, jak zareagować na wyzwania związane z pandemią za pomocą konkretnych ukierunkowanych rozwiązań.

TELEWIZJA DOZOROWA ZYSKAŁA NA ZNACZENIU

Priorytetem dla wielu klientów stały się systemy telewizji dozorowej umożliwiające obsługę zdalną – monitorowanie dystansu społecznego, przeciwdziałanie nowym zagrożeniom i zarządzanie budynkami o różnym poziomie zajętości. Firmy zainwestowały więcej w ten segment i dostrzegły znaczące innowacje, jakie można wprowadzić w odpowiedzi na potrzebę obsługi większej liczby danych.

– Technologia szybko ewoluuje, a to może utrudnić klientom nadążanie za nią – zauważył Dilen Thakrar, dyrektor ds. produktu w firmie Oncam. – Kiedy organizacje wdrażają nowe rozwiązania monitoringu wizyjnego, powinny dokładnie rozważyć, jak będą się zmieniały ich potrzeby technologiczne: wdrażane rozwiązanie musi być elastyczne i modułowe, by w przyszłości nie była konieczna całkowita zmiana inwestycji.

NIEDOBÓR SIŁY ROBOCZEJ

Pandemia spowodowała chaos na całym świecie i zmusiła ludzi do pozostania w domu. Niedobór siły roboczej stał się poważnym problemem dla wielu klientów, zwłaszcza z sektora ochrony fizycznej. Wiele firm musiało obniżyć koszty operacyjne, redukując etaty i wysyłając część pracowników na urlopy. Związany z tym niedobór siły roboczej dotknął głównie organizacje wznawiające inwestycje, szczególnie w rejonach, w których ograniczenia dotyczące działalności pozostają rygorystyczne.

Na szczęście dostawcy zabezpieczeń elektronicznych wkroczyli z rozwiązaniami łagodzącymi tę niedogodność.

– Chcieliśmy pomóc naszym integratorom w zaspokojeniu popytu tam, gdzie użytkownicy końcowi borykają się z brakiem siły roboczej. Rozszerzyliśmy ofertę szkoleniową i profesjonalne usługi, wydłużając godziny pracy i udostępniając zdalny dostęp do naszych ekspertów wspomagających zdalną instalację i konfigurację – podkreślił Alan Stoddard, prezes Cognity w Ameryce Północnej.

ROK 2021 W NOWEJ RZECZYWISTOŚCI

Po zakończeniu w 2020 r. firmy szukały powrotu na właściwy kurs, by budować lepszą przyszłość. Miniony rok uwypuklił zmiany dotyczące funkcjonowania firm i życia ludzi. Chociaż chęć powrotu do poprzednich modeli pra-

cy może być kusząca, rok 2020 uświadomił menedżerom potrzebę nowego podejścia.

POSTĘP SZYBSZY NIŻ KIEDYKOLWIEK

Dozór wizyjny stał się głównym narzędziem w rozwiązywaniu problemów wywołanych przez COVID-19. W odpowiedzi na wzrost zapotrzebowania na te systemy nastąpił w ciągu kilku miesięcy znaczący postęp w rozwoju technologicznym, który przed pandemią zająłby lata. Niemal z dnia na dzień nieodzowna w codziennym życiu stała się spójność cyfrowa.

– Jako specjaliści ds. bezpieczeństwa wiemy, jak ważna jest rola systemów dozoru wizyjnego monitorujących obiekty i zapewniających bezpieczeństwa ludziom – wyjaśnił John Rezzonico, założyciel i dyrektor generalny Surveill. – W szczycie zapotrzebowania na dane wiele organizacji było zmuszonych zredukować personel, obniżyć ogólne koszty, usprawnić procesy i przestrzegać zmieniających się przepisów. Ruchy te bezpośrednio wpłynęły na wzrost popytu na technologie wizyjne.

– Nawet w najbardziej niepewnych czasach w Surveill wciąż wprowadzaliśmy innowacje, ponieważ wiedzieliśmy, że jesteśmy w stanie zapewnić organizacjom o znaczeniu krytycznym skalowalne rozwiązanie do zarządzania materią wizyjną – podkreślił J. Rezzonico. – Zaprojektowany i zoptymalizowany pod kątem konsolidacji obciążenia zestaw rozwiązań wideo Surveill zapewnia przyjazną dla IT infrastrukturę o wydajności, skali i odporności do obsługi współczesnych wysokich wymagań w zakresie bezpieczeństwa oraz IoT.

POJAWIAJĄCE SIĘ ZAGROŻENIA I ROZWIĄZANIA JE ELIMINUJĄCE

Matt Tengwall z firmy Verint w 2021 r. zaobserwował większy popyt na rozwiązania zabezpieczające przed oszustwami. Pomagały one klientom w radzeniu sobie z nowymi zagrożeniami, takimi jak ataki typu Hook and Chain na bankomaty. Przestępczość związana z bankomatami od pewnego czasu rośnie, a zwiększenie liczby incydentów są przypisywane przez organy ścigania „niskiemu ryzyku i wysokiej opłacalności” przestępstwa. To sprawia, że dozór wizyjny jest niezbędnym wymogiem każdej strategii ochrony bankomatów.

– Rozwiązania do monitoringu wizyjnego firmy Verint chronią przed takimi atakami. Oferują bankom możliwość ochrony bankomatów dzięki połączeniu oprogramowania operacyjnego z funkcjami analitycznymi – stwierdził M. Tengwall. – Opracowanie technologii, która sprostą nowym wyzwaniom w zakresie bezpieczeństwa i wesprze rozwój biznesowy, jest podstawą naszej misji.

Zapotrzebowanie na rozwiązania zabezpieczające wynika przede wszystkim z obaw użytkowników końcowych, którzy chcą zaradzić pojawiającym się zagrożeniom, a równocześnie spełniać zasady dotyczące ochrony zdrowia.

PODSUMOWANIE

Dwa lata panowania COVID-19 przyniosły radykalne zmiany i postęp na rynku zabezpieczeń technicznych. Zmiany te nastąpiły w bezprecedensowym tempie. Przemodelowanie priorytetów przez klientów wpłynęło na popyt, ograniczenia epidemiczne natomiast uniemożliwiły realizację wielu projektów.

Na szczęście postęp technologiczny wpłynie na rozwój branży w znacznie szybszym tempie, niż przewidywano. Już dzisiaj widać, że branża potrafi radzić sobie w czasach pandemii. 🕒

KONTROLA DOSTĘPU

INWESTYCJE NAPĘDZANE
POPYTEM

Pandemia COVID-19 postawiła przed branżą zabezpieczeń sporo wyzwań, jednocześnie otwierając nowe możliwości, co dało się zauważyć w segmencie kontroli dostępu. Klienci byli zainteresowani zastąpieniem tradycyjnego systemu dotykowego bezdotykowym.

T E K S T
Prasanth Aby Thomas

COVID-19 znacznie przyspieszył zastosowanie rozpoznawania twarzy jako metody potwierdzania tożsamości w systemach kontroli dostępu. Eksperci prognozują, że ta metoda identyfikacji biometrycznej stanie się popularniejsza niż rozpoznawanie odcisków palców. W latach 2020-2021 firmy działające na rynku KD na całym świecie zauważyły zmiany w popycie i postanowiły tę sytuację wykorzystać. Zaangażowane technologicznie w rozwój biometrii twarzy szybko dostosowały swoją ofertę. Pozostałe skupiły się na uwierzytelnianiu mobilnym, rozpoznawaniu tęczy oka i innych technologiach, które pozwalają uniknąć kontaktu fizycznego z urządzeniem. To niejedynie istotne czynniki. Firmy podjęły działania, aby poradzić sobie z wyzwaniami pandemii, a także obecną sytuacją rynkową.

KLUCZEM Wczesne wykrycie ryzyka

Dla wielu firm problemem nie był COVID-19, ale jego nieprzewidywalność. Pandemii nie można było poddać analizie matematycznej, aby opisać ją wzorem i przewidzieć przyszłość. Oczywiście firmy, które potrafiły interpretować liczby, przyglądać się trendom i wyciągać wnioski oparte na posiadanych skąpych informacjach, mogły lepiej się przygotować. – *Zespół operacyjny w AMAG przewidział ryzyko zakłócenia łańcucha dostaw już w grudniu 2020 r.* – wyjaśnia John Becker, wiceprezes ds. globalnej sprzedaży w AMAG. – *Podjęliśmy niezbędne kroki i odpowiednio wcześniej zgromadziliśmy zapasy surowców potrzebnych do produkcji, aby nie zakłócić terminów dostaw towaru do klientów. Ścisłe współpracujemy z naszymi partnerami nad zminimalizowaniem wpływu pandemii, zachęciliśmy ich do odejścia od zamówień w modelu just-in-time na rzecz bardziej strategicznego podejścia. Ponieważ zakłócenia łańcucha dostaw nadal stanowią problem, zachęcamy klientów do wczesnego składania zamówień i uwzględniania opóźnień.*

WZMOŻONY POPYT, WIĘCEJ INWESTYCJI

Pandemia COVID-19 zakłóciła pracę wielu firmom, ale innym stworzyła możliwości do rozwoju działalności. Wymagało to wprowadzenia nowej technologii pozwalającej spełniać oczekiwania dynamicznego rynku. Według Prabhuraj Patil, dyrektora handlowego PACS w Azji Południowej w HID Global, w ostatnim roku rynek security osiągnął znacznie większe dochody w reakcji na wzrost zapotrzebowania na bezproblemową i bezpieczną pracę zdalną. Ponieważ coraz więcej krajów łagodzi ograniczenia, a pracownicy wracają do pracy, kluczowe znaczenie będzie miało dostosowanie się do nowych wymogów sanitarnych. – *Inwestowanie w najlepszą technologię kontroli dostępu jest warunkiem krytycznym w tworzeniu strategii bezpiecznego powrotu do pracy* – uważa P. Patil. – *Rośnie za-*

PRODUCENCI SYSTEMÓW ZABEZPIECZEŃ

OCZEKUJĄ, ŻE FIRMY WRÓCĄ NA WŁAŚCIWE

TORY, INTEGRATORZY, ŻE NIE BĘDZIE JUŻ

ŻADNYCH BLOKAD, A KLIENCI KOŃCOWI,

ŻE BĘDĄ MOGLI PROWADZIĆ SWOJĄ

DZIAŁALNOŚĆ BEZ PRZESZKÓD



potrzebowanie na technologie dostępu bezdotykowego, takie jak uwierzytelnianie mobilne, rozwiązania bluetooth czy narzędzia do zarządzania wizytami. Organizacje chcą zapewnić pracownikom rozwiązania, które promują zdrowe i bezpieczne środowisko pracy.

W roku 2022 można oczekiwać kontynuacji trendu wzrostowego. Przewiduje się, że rynek rozwiązań korzystających z uwierzytelniania mobilnego wzrośnie o 70% CAGR w latach 2020-2025. Będzie to najszybciej zaadaptowana technologia w branży kontroli dostępu.

POWROTY DO PRACY POBUDZAJĄ POPYT

Według J. Beckera, wiceprezesa AMAG, firma odnotowała wzrost zapotrzebowania na kontrolę dostępu w 2021 r. w porównaniu z rokiem 2020. Klienci na całym świecie nieprzerwanie inwestowali w bezpieczeństwo.

– *Duże firmy, które przesunęły kapitał z powodu zamknięcia biur podczas pandemii, teraz pracują nad ukończeniem projektów, zanim rozpoczną się powroty z pracy zdalnej. Z kolei mniejsze firmy, które wstrzymywały się z inwestycjami w 2020 r., wyznaczyły systemom zabezpieczeń wyższy priorytet ze względu na nowe wyzwania wynikające z pandemii. Zaobserwowaliśmy wzrost inwestycji w globalnych firmach branż medycznej i edukacyjnej oraz w biznesie samorządów lokalnych* – podkreśla J. Becker.

– *Najszybciej w tym roku rozwijają się rynek centrów danych w związku z potrzebą zarządzania wieloma systemami zabezpieczeń. W rezultacie przyjęto model otwartych rozwiązań do zarządzania tożsamością i sterowania różnymi systemami zainstalowanymi w obiekcie. Klienci mogą używać jednej karty do wszystkich systemów i zarządzać wszystkimi alarmami za pomocą jednego GUI, co ogranicza koszty, gdyż nie muszą zgrywać danych i wymieniać systemów. Działania podjęte w trakcie pandemii spowodowały również większe zapotrzebowanie na nasze mobilne rozwiązanie uwierzytelniające, które ułatwia pracownikom zdalny dostęp, bez konieczności uzyskania identyfikatora przy wjeździe do lokalizacji centralnej* – dodaje J. Becker.

PRZYGOTOWANIA DO 2022 R.

Nikt nie rozpoczyna biznesu, spodziewając się złego roku. W czasach, w jakich żyjemy, wielu z nas wierzy, że rok 2022 będzie lepszy niż poprzednie dwa lata. Producenci systemów zabezpieczeń oczekują, że firmy wrócą na właściwe tory, integratorzy, że nie będzie już żadnych blokad, a klienci końcowi, że będą mogli prowadzić swoją działalność bez przeszkód. Inwestycje w kontrolę dostępu z pewnością będą kontynuowane, ponieważ otoczenie biznesowe rozwija się po pandemii. Na razie możemy nie być w stanie przewidzieć tempa tego rozwoju, ale mamy nadzieję, że najgorsze już minęło. 📍

VIDEO MANAGEMENT SYSTEM

SPODZIEWANE NOWOŚCI W 2022 R.

Systemy zarządzania materiałem wizyjnym (*Video Management System – VMS*) są integralną częścią nowoczesnego systemu dozoru wizyjnego. Wprawdzie wielu producentów kamer oferuje własny VMS, lecz oprogramowanie firm wyspecjalizowanych pod jego kątem zapewnia zaawansowaną funkcjonalność.

T E K S T
William Pao

Przedstawiamy nowości w obszarze VMS, które mają trafić na rynek w 2022 r. Przyglądamy się nowym funkcjom, możliwościom integracji sprzętu oraz trendom.

NOWE FUNKCJE

Rok 2022 zapowiada się obiecująco w zakresie automatyzacji i inteligencji. Analiza treści obrazu i inne możliwości automatyzacji stają się coraz bardziej powszechne. Są obszarem innowacji dla systemów zarządzania materiałem wizyjnym. Ponieważ VMS może pozyskiwać duże ilości różnych informacji, analityka potrafi odfiltrować wiadomości nieistotne dla użytkownika, aby dostarczyć te we wskazanym przez niego zakresie.

ZWIĘKSZONA PRZYDATNOŚĆ

Według Laurenta Villeneuve, Product Marketing Managera w firmie Genetec, następnym krokiem będzie przedsta-

wienie tych informacji w formie jeszcze bardziej przydatnej lub łatwiejszej do przetworzenia, aby wyzwolić odpowiednie działania w systemie.

– Silniki korelacji oparte na zdefiniowanych wcześniej regułach i inne procesy przebiegające w tle, które pomagają wyzwolić alarmy lub prezentować odpowiednią ilość informacji we właściwym czasie, będą kluczem do transformacji w inteligentniejsze systemy zarządzania wizją – uważa L. Villeneuve. – Na podstawie ewolucji w zarządzaniu operacjami i zwiększania liczby użytkowników korzystających z tych systemów przypuszczamy, że warstwa wizualizacji stanie się również bardziej intuicyjna i elastyczna.

WIĘCEJ APLIKACJI MOBILNYCH

Genetec spodziewa się także znaczących ulepszeń w aplikacjach internetowych i mobilnych, które wyjdą poza obszar tradycyjnego udostępniania i odtwarzania nagrań. Niezależnie od tego, czy chodzi o interfejsy map, czy pulpity nawigacyjne, stają się one potężnymi narzędziami do reagowania na żywo i przeszukiwania nagranych materiałów w celach dochodzeniowych.

– Wkrótce użytkownicy będą mogli wykonywać tyle samo operacji telefonicznie lub zdalnie na laptopie, co w centrum monitorowania – przewiduje L. Villeneuve.

ŁATWOŚĆ OBSŁUGI I DOSTĘPNOŚĆ

Beniamin Low, wiceprezes ds. Azji i Pacyfiku w Milestone Systems, twierdzi, że nowe funkcje oprogramowania VMS prawdopodobnie skupią się na użyteczności i dostępności dla interesariuszy.

– Wraz z rosnącym zapotrzebowaniem na większą liczbę kamer i łatwiejszą integrację z innymi systemami firm trzecich od kontroli dostępu po zaawansowane systemy analityczne bezpośredni użytkownicy i operatorzy będą musieli wybrać odpowiedni VMS: zunifikowany, inteligentny, skalowalny i scentralizowany system zarządzania materiałem wizyjnym, zdolny do wysokiej wydajności i długoterminowej ochrony danych – podkreśla B. Low. – Co ważne, przyjazny dla użytkownika interfejs sprawi, że operator wykorzysta VMS w maksymalnym stopniu.

ŁATWIEJSZA INTEGRACJA APLIKACJI

Systemy dozоровe stają się coraz bardziej złożone, zatem VMS będzie musiał ewoluować, by stać się bardziej otwartym, głównym motorem rozwoju technologii wizyjnych. Technologia umożliwia już obsługę analityki, sztucznej inteligencji i innych zautomatyzowanych rozwiązań. Z punktu widzenia programisty integracja musi być prostsza i łatwiejsza w implementacji. Zachęci to innych programistów

do pracy nad tworzeniem przydatnych aplikacji budynkowych wykorzystujących VMS. Dzięki przyjaznym w użyciu interfejsom API nawet programiści nieobeznani z VMS szybko znajdą dla niego zastosowanie.

NOWE MOŻLIWOŚCI INTEGRACJI SPRZĘTU

Ważnym obszarem rozwoju VMS jest dodanie nowego urządzenia. Systemy zabezpieczeń obejmują już nie tylko kamery czy czytniki kontroli dostępu. Każdego roku na rynek wchodzi nowe rozwiązania i urządzenia, które pomagają klientom zapewnić bezpieczeństwo obiektu i wgląd w biznes. W roku 2022 zostaną udostępnione nowe możliwości integracji sprzętu dzięki VMS.

URZĄDZENIA I ŹRÓDŁA DANYCH NIEZWIĄZANE Z ZABEZPIECZENIAMI

Podstawową opcją platform bezpieczeństwa i VMS nowej generacji jest pozyskiwanie danych nie tylko z czujników systemów zabezpieczeń. Klienci staną się bardziej kreatywni i rozszerzą zasięg zarządzania materiałem wizyjnym. – W przyszłym roku prawdopodobnie pojawi się więcej urządzeń i źródeł danych zintegrowanych z VMS do zadań, które wykraczają poza bezpieczeństwo i ochronę – prognozuje L. Villeneuve. – W obiektach jest zainstalowanych wiele czujników i urządzeń, które można zintegrować w celu monitorowania np. ich wydajności bądź poprawy zarządzania zużyciem energii czy procesami produkcyjnymi.

Genetec przewiduje, że dzięki VMS klienci zaczną też integrować detektory zużycia wody, temperatury, oświetlenia, HVAC, windy i inne urządzenia IoT, które pozwolą im lepiej poznać parametry środowiska i sterować nimi.

WYŻSZE ROZDZIELCZOŚCI I WIĘCEJ DANYCH

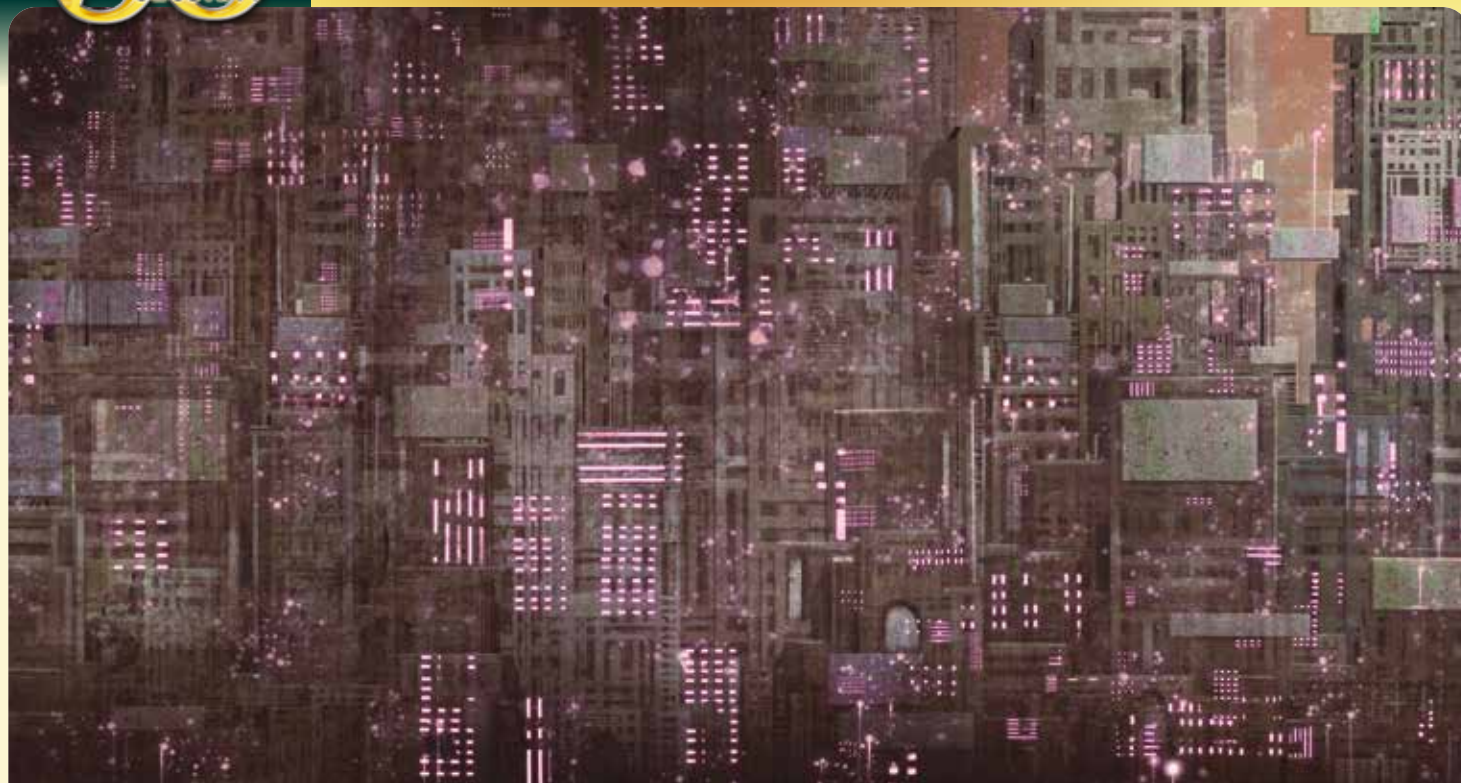
B. Low wyjaśnił, że w miarę, jak użytkownicy są coraz bardziej świadomi korzyści zapewnianych przez obraz wideo, usprawniają dozór wizyjny i działania operacyjne. Zwiększa się zapotrzebowanie na obrazy wideo o wyższej jakości (od full HD do 4K), by lepiej rozpoznawać i przewidywać zdarzenia.

Zapotrzebowanie na informacje i dane uzyskiwane z obrazów kamer dozоровych będzie rosnąć. Złożone formy metadanych mogą być generowane na podstawie takich cech, jak kształty i rozmiary obiektów, dane czasowe czy zachowanie osób.

– Trendy te przekładają się bezpośrednio na wzrost zapotrzebowania na bardziej wydajne systemy, z zaawansowanymi możliwościami przetwarzania i wydajnymi pamięciami masowymi spełniającymi wymagania oprogramowania – ocenił B. Low. – Dlatego zapewne producenci wprowadzą nowe rozwiązania sprzętowe serwerów i pamięci masowej, które będą się integrować z odpowiednim VMS. Pozwoli to optymalizować duże ilości rejestrowanych i przechowywanych danych, aby zapewnić klientom satysfakcjonujący produkt.

POPYT I TRENDY, KTÓRE GO NAPĘDZAJĄ

Pandemia zmieniła sposób, w jaki działamy jako społeczeństwo i jednostki. Nastąpiło przyspieszenie integracji zaawansowanych funkcji zabezpieczeń i ochrony w wielu sektorach, od hoteli, poprzez służbę zdrowia, edukację, po inteligentne miasta. Gdy coraz więcej osób będzie świadomych korzyści, jakie systemy wizyjne mogą zapewnić na obszarach gęsto zaludnionych, wystąpi wzrost zapotrzebowania na integrację systemów biznesowych z dozоровymi, co ułatwi kontrolowanie np. zachowania dystansu społecznego, dostępu do wyznaczonych stref czy zarządzania personelem.



INTELIGENTNE MIASTA

Zaawansowana analityka dostarcza kluczowych informacji operacyjnych, które właściciele firm mogą wykorzystywać do zwiększenia wydajności i utrzymania przychodów. – Przykładowo, inteligentne miasta wdrażają wysoko wydajne systemy dozoru wizyjnego zintegrowane z analizą danych w celu zarządzania przepływem ruchu, zmniejszania korków czy poprawy sytuacji na drogach – mówi B. Low. – Funkcje analityczne, takie jak rozpoznawanie obiektów czy twarzy, mapowanie ciepła czy wykrywanie dźwięku będą coraz częściej implementowane w kamerach dozoru, umożliwiając szybszą reakcję, analizę zachowań lub lepsze zarządzanie incydentami, np. w hotelu. B. Low zwraca też uwagę, że poszczególne sektory mają różne cele zastosowania zaawansowanej analityki. Rozwiązania VMS muszą być napędzane, rozwijane i dostosowywane zgodnie z konkretnymi potrzebami klientów w ich branżach.

ROZWÓJ 5G

Infrastruktura sieci 5G się rozwija i można już wykonywać więcej połączeń między urządzeniami 5G a IoT. To korzystne dla użytkowników VMS, ponieważ 5G pozwala na fragmentyzację sieci, aby zaoferować wydzielone części przepustowości dla pokrewnych aplikacji związanych z technologią wizyjną, np. do analizy behawioralnej, rozpoznawania tablic rejestracyjnych itp.

– Zwiększa to wydajność aplikacji w zastosowaniach na szeroką skalę, ponieważ wydzielone części przepustowości sieci nie muszą być współdzielone do innych celów – wyjaśnia B. Low. – Nie zapominajmy, że rozwój 5G zwiększa również możliwość realizowania dozoru wizyjnego jako usługi (VSaaS) dla większej liczby użytkowników końcowych. Jest to możliwe dzięki lepszej obsłudze przesyłania sygnałów wizyjnych do scentralizowanej lokalizacji za miast systemów lokalnych.

Ponieważ rynek ewoluuje, a technologie wizyjne są coraz częściej wdrażane, firmy współpracują z organami regulacyjnymi w celu zapewnienia ochrony danych osobowych obywateli. Firmy technologiczne, które gromadzą i przetwa-

rzają dane do własnych celów biznesowych, współdziałają z organami regulacyjnymi i partnerami technologicznymi, aby respektować prywatność jednostki i przestrzegać lokalnych przepisów o ochronie danych osobowych.

TECHNOLOGIE CHMURY I CHMURY HYBRYDOWEJ

Kolejnym ważnym trendem jest migracja do technologii chmury i chmury hybrydowej. Wiele rozwiązań VMS jest obecnie budowanych na zasadzie systemu hybrydowego.

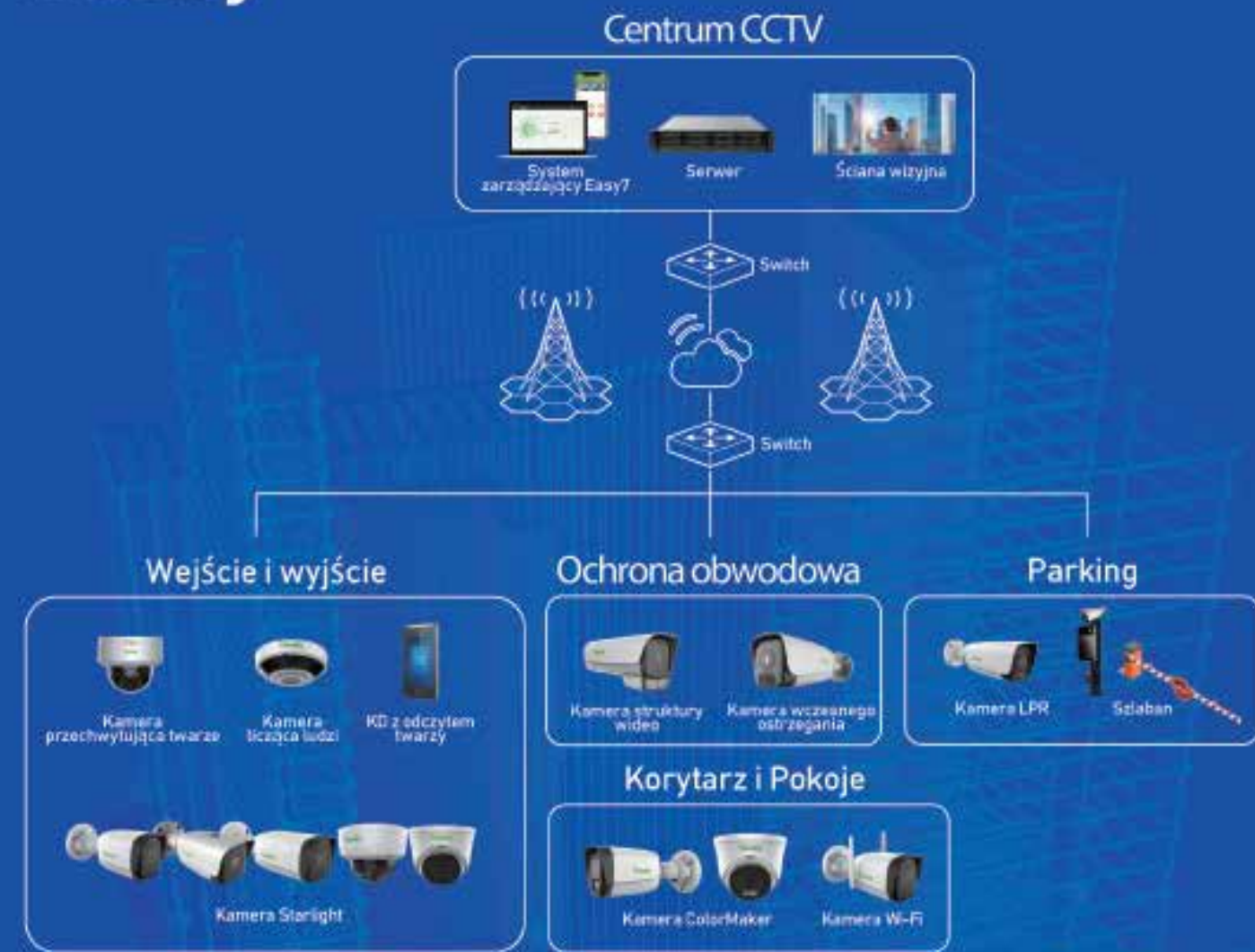
– Oferujemy to, co najlepsze z obu rozwiązań: prawo własności i kontrolę klientów nad ich systemem i danymi, gdy jest to wymagane, z linią aplikacji w chmurze, które pomagają im rozszerzać działalność – podkreśla L. Villeneuve. – Niezależnie od tego, czy jest to portal w chmurze do zarządzania materiałem wizyjnym, czy długoterminowe przechowywanie w chmurze materiałów, mogą one migrować do chmury hybrydowej we własnym tempie. To, w połączeniu z ogólnym ruchem w kierunku RMR, zachęci klientów do wyboru otwartych rozwiązań VMS, które nie ograniczają wyboru kupującego i zapewniają długoterminową rentowność.

Wdrożenie chmury hybrydowej to dla wielu klientów najlepsze rozwiązanie. Zapewnia większą elastyczność, szybki powrót do pracy po awarii systemu, szybkie zarządzanie zdalnymi lokalizacjami na jednej platformie. Umożliwia przestrzeganie zasad bezpieczeństwa przechowywanego materiału wizyjnego. Oferuje doskonałą równowagę między wydajnością i zestawem funkcji systemów lokalnych a łatwością wdrażania rozwiązań w chmurze.

PODSUMOWANIE

W roku 2022 w systemach do zarządzania materiałem wizyjnym zapewne pojawi się więcej aplikacji spoza zastosowań security. VMS umożliwi też lepszą integrację z chmurą. Będą kontynuowane zabiegi zmierzające do zwiększenia zastosowania analityki. Należy oczekiwać przyspieszonego rozwoju w zakresie zarówno sprzętu, jak i oprogramowania.

Tiandy



ROZWIĄZANIE DLA BUDYNKÓW



Genway oficjalny Dystrybutor Tiandy

Email: info@genway.pl

Tel: +48-24-264-77-33

Strona: www.genway.pl

Fax: +48-24-268-12-29

TECHNOLOGIE ROKU 2022

W roku 2021 branża security odbudowywała się po problemach, jakie spowodował COVID-19. W rok 2022 gracze rynkowi i klienci wchodzi z nadzieją, że ożywienie gospodarki będzie się utrzymywało. Branżowi eksperci pozostają optymistami co do perspektyw w nadchodzącym roku.

Ważnym czynnikiem umożliwiającym rozwój branży zabezpieczeń technicznych, szczególnie podczas pandemii, stała się technologia, zmieniając sposób, w jaki firmy prowadzą działalność oraz przyspieszając rozwój nowych rozwiązań i aplikacji. Ale nie wszystkie rozwiązania mogą być odpowiednie lub gotowe do natychmiastowego wdrożenia. Zapytaliśmy firmy z branży security o trendy technologiczne, które wg ich przewidywań będą miały największy wpływ na rozwój rynku w 2022 r., i odpowiedzi skorelowaliśmy z wynikami ankiety, którą przeprowadził wśród czytelników portal asmag.com. Połączenie tych danych może wskazać, które technologie warto wdrożyć, aby uzyskać przewagę konkurencyjną w branży.

1. INTEGRACJA WIĘKSZEJ LICZBY URZĄDZEŃ

W przyszłym roku prawdopodobnie jeszcze więcej urządzeń i źródeł danych będzie zintegrowanych z systemami zabezpieczeń technicznych do celów wykraczających poza safety i security.

– W budynkach jest wiele czujników i urządzeń, które można ze sobą zintegrować, by monitorować ich parametry pracy i sprawność, albo np. zarządzać zużyciem energii czy procesami produkcyjnymi – powiedział Laurent Villeneuve, Product Marketing Manager w Genetec. – Przewidujemy, że integracja danych zostanie rozszerzona poza tradycyjne czujniki, a klienci zaczną monitorować zużycie wody, temperaturę, oświetlenie, HVAC, zarządzać windami i innymi urządzeniami IoT.

2. TECHNOLOGIA 5G WYGLĄDA OBIECUJĄCO, MIMO ŻE NIE JEST W PEŁNI GOTOWA

Jedną z technologii, która przyspieszy rozwój Internetu rzeczy, jest łączność bezprzewodowa 5G. Mimo różnego tempa jej wdrażania na świecie (wiele krajów ma zaległości w porównaniu z innymi) sieci 5G zostały uznane za rozwiązanie problemów dotyczących przepustowości i opóźnień transmisji.

Technologia 5G stała się tematem rozmów o monitoringu wizyjnym. Dodanie obsługi Wi-Fi oraz 5G do kamer oznacza możliwość prowadzenia zdalnego dozoru wizyjnego w czasie rzeczywistym odległych lokalizacji przy użyciu aplikacji mobilnych. Może to być wyzwaniem ekonomicznym dla większości użytkowników końcowych korzystających ze starszych technologii.

Mimo opinii, że 5G nie jest jeszcze gotowa do wdrożenia, producenci zachowują optymizm.

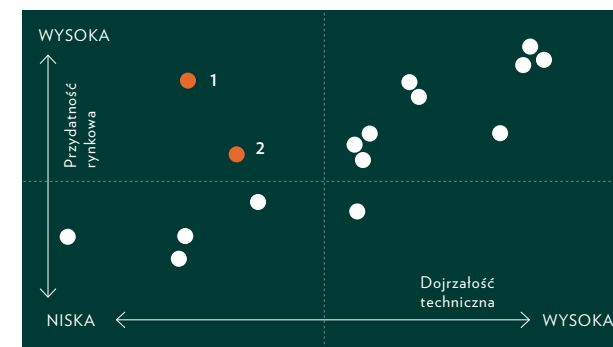
– Zintegrowanie tego poziomu łączności z kamerą może zapewnić zwiększoną świadomość sytuacyjną i wczesne ostrzeżenie z odległych niestrzeżonych lokalizacji, a w efekcie skuteczniejsze zapobieganie incydentom w krótszym czasie reakcji – wyjaśniła Kinnera Angadi, dyrektor ds. bezpieczeństwa w Honeywell Building Technologies. – Duża dostępność danych wizyjnych umożliwia również jednoczesną obsługę wielu algorytmów realizowanych na brzegu sieci i zmniejsza opóźnienia przesyłania do chmury. Może również mieć wpływ na obniżenie kosztów instalacji istotnych w takich obszarach, jak inteligentne miasta lub miejsca wymagające dużej liczby kamer.

Fabio Marti, wiceprezes ds. marketingu w firmie Azena finansowanej przez firmę Bosch, powiedział, że jego firma nie może się już doczekać finału trwającego wdrażania technologii 5G, która ma znacząco zmienić sposób transmisji i wykorzystania danych wizyjnych, zwłaszcza z odległych lokalizacji, przy znacznie niższych niż obecnie kosztach. – Ogólnie rzecz biorąc, 5G udostępni bogatsze strumienie danych do bardziej wyrafinowanej analizy metadanych w chmurze, co ma znaczenie w przypadkach, gdy wstępne przetwarzanie odbywa się w kamerze, a pełne przetwarzanie w chmurze – stwierdził F. Marti. – Nowe możliwości 5G pozwolą również na wykorzystanie dodatkowych strumieni wizji do zaawansowanej wieloalgorytmowej analizy wizyjnej lub obsługi większej liczby kamer przy jednoczesnym zmniejszeniu opóźnień transferu danych.

Miliardy zbierających informacje czujników i urządzeń, połączonych w sieci i zintegrowanych ze sobą, dostarczają pokaźny wolumen metadanych wymagany do opracowania zaawansowanych algorytmów sztucznej inteligencji (AI) i przetrenowania nowych modeli analitycznych w celu uzyskania praktycznych rozwiązań.

Nowe standardy kompresji i kodowania wizji, takie jak H.266 i MPEG5, po badaniach zostały uznane za bardziej odpowiednie dla branży (rys. 1), ale złożoność kodeków, rozdzielczość obrazów i prędkość przesyłania (liczba klatek na sekundę) podnie-

sione skokowo na wyższy poziom zaawansowania potencjalnie zwiększają wyzwania dla koderów i tradycyjnych serwerów.



Rys. 1. Odpowiednie, ale niedojrzałe: 1 – H.266, MPEG5; 2 – komunikacja bezprzewodowa 5G

3. ZWIĘKSZONA MIGRACJA DO CHMURY I CHMURY HYBRYDOWEJ

Z perspektywy rynku zabezpieczeń w nadchodzących latach oczekujemy większego popytu na dozór wizyjny, inteligentne rozwiązania IoT i usługi w chmurze. Ten wzrost będzie widoczny zwłaszcza w przypadku rozwiązań w chmurze, ponieważ technologia staje się coraz bardziej niezawodna i przystępna cenowo. – Dozór wizyjny oparty na chmurze jest cenną opcją dla wielu rynków wertykalnych – wyjaśnił Nigel Waterton, CRO z Arcules. – Chmura okazała się wysoce funkcjonalną, elastyczną i wygodną metodą dla firm, które chcą ją wykorzystać w ramach swojej strategii bezpieczeństwa i modernizacji obiektów. Pozwala organizacjom przyspieszyć operacje i tworzyć proaktywną, niezawodną strategię analizy danych ograniczającą ryzyko i umożliwiającą podejmowanie inteligentnych decyzji, a w efekcie właściwe zarządzanie.

Ta opinia jest zbieżna z wynikami ankiety przeprowadzonej na początku tego roku (rys. 2). Badanie wykazało duże zainteresowanie branży usługami dozoru wizyjnego i kontroli dostępu w chmurze – 42% respondentów potwierdziło, że już wdraża projekt w chmurze, a znaczna liczba odpowiedziała twierdząco, gdy zapytano, czy zdecydują się na usługi w chmurze w nad-

chodzącym roku (45% w przypadku dozoru wizyjnego i 34% w przypadku kontroli dostępu).

Jakie jest prawdopodobieństwo wdrożenia rozwiązania w chmurze w nadchodzącym roku?

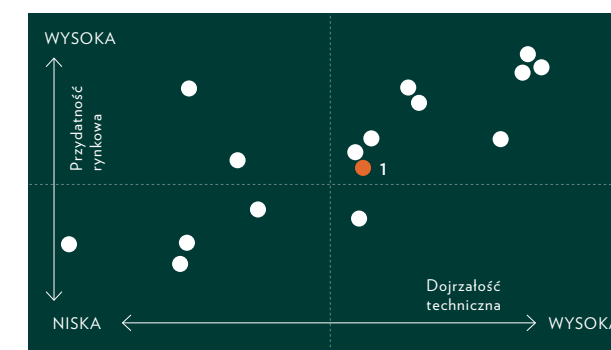


Rys. 2. Wyniki ankiety prowadzonej przez asmag.com 2021 r. – zainteresowanie usługami w chmurze dotyczące dozoru wizyjnego i kontroli dostępu

Wielu ekspertów uważa również, że technologia chmury hybrydowej może być bardziej popularna niż czyste rozwiązania oparte na chmurze. Wdrożenie chmury hybrydowej ma sens dla wielu klientów, ponieważ daje im to, co najlepsze z obu rozwiązań.

– Chmura hybrydowa zapewnia większą elastyczność i szybsze przywracanie systemu po awarii, ułatwia zarządzanie lokalizacjami zdalnymi na jednej platformie i jest prawdopodobnie najlepszym sposobem na przestrzeganie zasad przechowywania materiału wizyjnego – powiedział L. Villeneuve. – Oferuje doskonałą równowagę między wydajnością i zestawem funkcji systemów lokalnych a łatwością wdrażania rozwiązań w chmurze.

Ciekawy wynik badania uzyskał dozór wizyjny jako usługa (VSaaS), który został sklasyfikowany tylko nieznacznie powyżej średniego poziomu przydatności i dojrzałości (rys. 3) niż technologie związane ze sztuczną inteligencją (rys. 4).



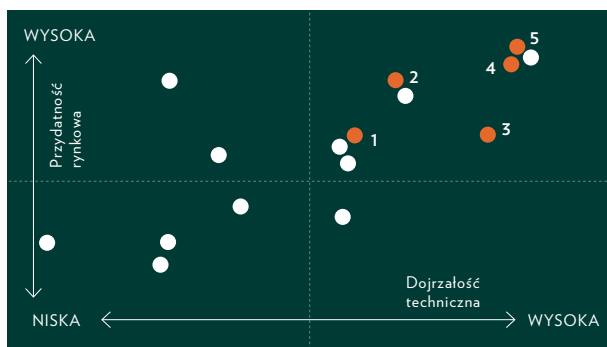
Rys. 3. Dojrzały i odpowiedni: 1 – VSaaS

4. WIĘCEJ AUTOMATYKI I ZASTOSOWAŃ ANALITYKI

Rok 2022 zapowiada się również obiecująco dla automatyzacji i sztucznej inteligencji. Teraz, gdy automatyczna analiza obrazów z kamer i inne większe możliwości działań automatycznych stają się coraz bardziej powszechne, AI może być głównym motorem innowacji w zakresie rozwiązań z obszaru zabezpieczeń technicznych.

– Oczekuje się, że AI będzie kluczowym elementem wsparcia systemów dozoru wizyjnego w nadchodzącym roku – ocenił Matt Tengwall, dyrektor generalny ds. oszustw i rozwiązań bezpieczeństwa w Verint. – Pomaga użytkownikom przechwytywać dane krytyczne pozwalające lepiej oszacować zagrożenia bezpieczeństwa czy zachowania klientów. Organizacje muszą przeanalizować AI i analitykę wideo, aby upewnić się, że ich strategia jest zgodna z celami biznesowymi.

Badanie trendów wykazało, że technologie AI związane z automatyczną analizą danych wizyjnych wspierające m.in. procesy sądowe, analizę zachowań, analizy biznesowe, wykrywanie obiektów i zajętości przestrzeni zostały uznane za odpowiednie i wystarczająco dojrzałe techniki do zastosowania przez rynki wertykalne (rys. 4).



Rys. 4. Technologie związane z analizą AI są uważane zarówno za dojrzałe, jak i odpowiednie: 1 – przepustowość kontrolowana przez sztuczną inteligencję, 2 – wykrywanie obiektów AI, 3 – analiza biznesowa oparta na sztucznej inteligencji, 4 – szybkie LPR (5) dochodzenia kryminalistyczne AI

W ostatnich latach wraz ze wzrostem możliwości technologicznych znacznie rozwinęła się analityka wizji do zastosowań security. Może ona teraz wesprzeć użytkowników końcowych w identyfikowaniu ich potrzeb: w rozbudowywaniu automatyki budynkowej, generowaniu wyników biznesowych czy poprawie bezpieczeństwa budynków. Według K. Angadi technologia przekroczyła granice realizacji jednej funkcji fizycznej kamery dozorowej, dowodząc zalet integrowania wielu funkcjonalności.

– W Honeywell koncentrujemy się na wykorzystaniu takich narzędzi, jak sztuczna inteligencja i uczenie maszynowe, aby stale ulepszać algorytmy analityki i gromadzenie danych – powiedziała K. Angadi. – Może to nie tylko umożliwić klientom tworzenie wysokiej jakości systemu zabezpieczeń, ale także wesprzeć w zarządzaniu ich danymi w sposób, który zapewni im osiągnięcie celów biznesowych. Odkąd kamery stają się coraz inteligentniejsze, zauważamy wzrost wdrażania zabezpieczeń. Klienci dostrzegają niższe koszty instalacji, a także szybszą analizę gromadzonych danych, co ostatecznie pomaga im lepiej przygotować się na incydenty bezpieczeństwa i reagować na nie.

F. Marti, zgadzając się z tym, dodaje, że wzrost liczby kamer w systemie i danych wizyjnych wymaga wstępnej analizy istotnych zdarzeń i informacji, aby dać operatorom możliwość określenia najbardziej odpowiedniej reakcji na zaistniałą sytuację: – Analityka wizyjna pomaga wyodrębnić najistotniejsze zdarzenia, na które powinni zwrócić uwagę operatorzy, i dostarcza dodatkowych informacji wspierających podejmowanie decyzji. Przykładowo w przypadku włamania na podstawie każdej z następujących analiz można dokonać oceny obserwowanej sceny pod kątem dalszych działań: czy wykryto broń, ile osób zostało wykrytych, czy wystąpiły inne podejrzane zachowania, rozpoznać model samochodu, określić jego prędkość itp. Dopasowując te inicjatywy do rzeczywistych wyników biznesowych i poważnie podchodząc do jakości danych, organizacje mają potencjał, aby zwiększyć zaangażowanie klientów.

5. WIĘKSZA DBAŁOŚĆ O CYBERBEZPIECZEŃSTWO

L. Villeneuve spodziewa się kolejnych zmian w obszarze cyberbezpieczeństwa w nadchodzącym roku. Sieciowe systemy zabezpieczeń są poddawane większej kontroli, więc będą musiały ewoluować, aby sprostać oczekiwaniom rynku i wyższemu standardowi w zakresie cyberbezpieczeństwa i poufności danych osobowych.

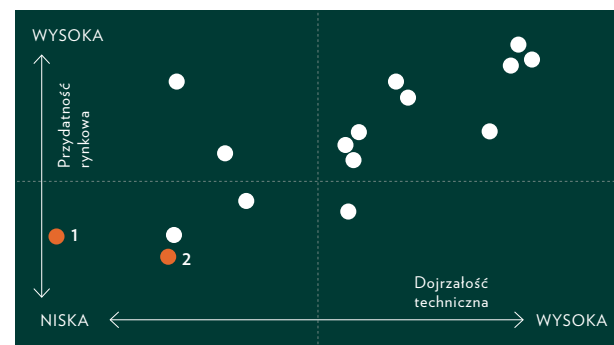
– Nasi klienci stawiają teraz bezpieczeństwo i prywatność osób na pierwszym miejscu, a posiadanie odpowiednich produktów jest niezbędne, aby budować zaufanie do ludzi, którzy coraz częściej korzystają z rozwiązań technologicznych – stwierdził L. Villeneuve.

Z tym zgadzają się inni eksperci. John Rezzonico, założyciel i dyrektor generalny Surveill, powiedział, że zapewnienie bezpieczeństwa cyfrowego nadal będzie priorytetem, szczególnie w świetle nagłośnionych ataków hakerskich, których organizacje doświadczyły w ciągu ostatnich 12 miesięcy.

– Dostawcy zabezpieczeń technicznych chcą mieć pewność, że stosują się do najlepszych praktyk w zakresie cyberbezpieczeństwa i oferują najwyższą ochronę swoim klientom końcowym – powiedział J. Rezzonico. – To wyraźna zmiana w podejściu do cyberzagrożeń. Instalując system dozoru wizyjnego, nie od razu myśli się o jego cyfrowym zabezpieczeniu.

Ataki hakerskie, złośliwe oprogramowanie często traktuje się odrębnie w oderwaniu od urządzeń systemów zabezpieczeń. A te dwie kwestie muszą być powiązane, ponieważ hakerzy posługują się coraz bardziej wyrafinowanymi metodami, by uzyskać dostęp do sieci, danych i zasobów. Coraz więcej fizycznych urządzeń zabezpieczających jest stale połączonych ze sobą za pośrednictwem sieci internetowej, zatem szyfrowanie komunikacji i testowanie luk w zabezpieczeniach są niezbędne do zapewnienia bezpiecznego przesyłu danych.

Technologia *blockchain* i aplikacje kontenerowe (*containerised app*) zainteresowały branżę ze względu na wiele możliwych funkcji, w tym ich potencjał poprawy bezpieczeństwa danych – zdecentralizowana infrastruktura może być pomocna w szyfrowaniu materiału wizyjnego i minimalizowaniu fałszowania danych. W ankiecie stwierdzono jednak, że oba te rozwiązania nie są dojrzałe technicznie, a i branża zabezpieczeń jeszcze nie jest na nie gotowa (rys. 5). Nie jest to zaskakujące, ich implementacja stanowi dziś duże wyzwanie. Brak wiedzy i trudności w opracowaniu kompleksowej strategii poprawnego wdrożenia bez zakłócania bieżącej działalności są wymieniane jako ograniczenia dodatkowe.



Rys. 5. Niedojrzałe technicznie i nieodpowiednie do wdrożeń: 1 – technologia *blockchain*, 2 – aplikacje kontenerowe

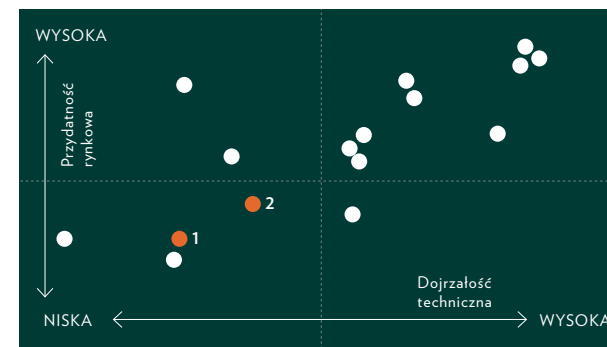
6. WIĘCEJ APLIKACJI MOBILNYCH

Ekspert branżowy spodziewają się w nadchodzącym roku znacznych ulepszeń aplikacji internetowych i mobilnych. Powinny one być w stanie prezentować tego samego typu bogate funkcjonalności wykraczające poza tradycyjne udostępnianie i odtwarzanie materiału wizyjnego.

– Niezależnie od tego, czy chodzi o interfejsy mapowe, czy pulpitowe, stają się one potężnymi narzędziami do reagowania na żywo i zadań dochodzeniowych, a użytkownicy będą mogli wykonywać tak wiele operacji, korzystając z telefonu lub zdalnie na laptopie, jak w pomieszczeniu centrum monitoringu – powiedział L. Villeneuve.

Niektóre z czołowych firm związanych z kontrolą dostępu oczekują, że popularne staną się również rozwiązania oparte na mobilnym uwierzytelnianiu. John Becker, wiceprezes ds. sprzedaży globalnej w firmie AMAG, zauważył, że pandemia uwypukliła potrzebę stosowania mobilnych poświadczeń tożsamości. Instalowanie czytników *bluetooth* i używanie telefonu komórkowego jako karty dostępu to naturalna konsekwencja postępu w odpowiedzi na konieczność ograniczania rozprzestrzeniania się COVID-19.

– Użytkownicy mogą samodzielnie skonfigurować swoje dane uwierzytelniające i nie muszą już fizycznie udawać się do biura – stwierdził J. Becker. – Nie ma potrzeby drukowania kart czy karty zastępczej, gdy pracownik zapomni identyfikatora. Można więc sporo zaoszczędzić.



Rys. 6. Niedojrzałe technicznie i nieodpowiednie do wdrożeń: 1 – Bezzatogowe platformy bezpieczeństwa, 2 – Radar i LiDAR

7. RADAR I LIDAR NIE SĄ JESZCZE GOTOWE NA 5G, ALE MAJĄ POTENCJAŁ

Chociaż ankieta wykazała, że Radar i LiDAR są najmniej przygotowane do obsługi 5G (rys. 6), K. Angadi sugeruje, że ze względu na wyjątkowe korzyści mogą być odpowiednie dla niektórych branż.

– LiDAR może być stosowany w systemach zabezpieczeń w szerokim zakresie, w tym w dozorcze obszarów zewnętrznych i wewnętrznych, strefach bezpieczeństwa publicznego, kontroli granic, wykrywania intruzów, kontroli dostępu i ochrony obwodowej – podkreśliła K. Angadi. – Dla Honeywell największym rynkiem zbytu tych detektorów są obiekty infrastruktury krytycznej, głównie centra danych, dostawcy i dystrybutorzy energii, wodociągi i usługi komunalne, elektrownie jądrowe oraz petrochemia.

R E K L A M A

Hanwha Techwin

WISeNET

1 KAMERA
16 MIEJSC

KAMERA AI WSKAZUJĄCA WOLNE
MIEJSCE PARKINGOWE

- Monitorowanie 16 miejsc 1 kamerą
- Brak serwera i łatwość konfigurowania
- Różne kolory diod LED
- Dołączanie innych urządzeń poprzez wejścia/wyjścia alarmowe i audio
- Wyświetlanie w trybie pojedynczym lub podzielonym

www.hanwha-security.eu





NA UKŁADY NIE MA RADY

KRYZYS W DOSTAWACH MIKROPROCESORÓW

Rok 2021 dla polskiej branży zabezpieczeń technicznych to czas ciągłej walki z wydłużającymi się terminami dostaw, wyzwań związanych z wprowadzaniem zamienników produktów w trakcie realizacji projektu i odbudowy lokalnych stoków magazynowych. Nagłe zmiany wywołane pandemią obnażyły wiele słabości światowej gospodarki i globalnych łańcuchów dostaw, które posypały się w najmniej spodziewanym momencie. Jedną z tych słabości okazały się twarde realia rynku produkcji układów scalonych oraz uzależnienie rynków od stopnia skomplikowania otaczających nas urządzeń i rosnącego na nie zapotrzebowania.

T E K S T
Jan T. Grusznic

a&s Polska

Półprzewodniki – produkty względnie proste składające się w głównej mierze z przetworzonego piasku (a właściwie krzemu, pierwiastka powszechnego na Ziemi, w dodatku o niezwykłych właściwościach), a jednocześnie produkowane w laboratoryjnych warunkach z użyciem technologii tak precyzyjnych, że kilka zbłądzonych cząsteczek kurzu może doprowadzić do zniszczenia milionów układów scalonych¹.

Półprzewodniki stały się wszechobecne w otaczającym nas świecie i są kluczowym komponentem każdej współczesnej techniki – od aut (w pojazdach z silnikiem spalinowym zainstalowane jest od 50 do 200 różnych chipów, a w autach hybrydowych i elektrycznych dochodzi do 3500²), komputerów, kamer, elementów systemów kontroli dostępu i sygnalizacji włamania, AGD po szczoteczki do zębów, sygnalizację świetlną, etykiety w sklepach czy żarówki. Układy scalone stanowią podstawę wszystkich tzw. inteligentnych urządzeń, z których korzystamy każdego dnia. Niespodziewanie szybkie odbicie gospodarek całego świata po pierwszych lockdownach, a także puste magazyny komponentów wynikające ze zmniejszenia produkcji i wyprzedaży na początku pandemii spowodowały, że ograniczona liczba fabryk potrafiących wyprodukować zaawansowane technologicznie układy mierzy się obecnie z ogromnym zapotrzebowaniem.

Zaburzone przez pandemię łańcuchy dostaw, które najpierw się załamały, później zaś nastąpił proces ich szybkiej odbudowy, wywołały chaos, który przełożył się na długie terminy oczekiwania i znaczącą podwyżkę cen (niekiedy nawet 10-krot-

ną). Na domiar złego koncentracja produkcji półprzewodników w Azji³ (rys. 1) nie pomaga w szybkim rozwiązaniu problemu.

Większość firm zabezpieczyła się przed najgorszym (np. BCD właściciel marki BCDVideo), natomiast mało kto był przygotowany na nagłą i gwałtowną poprawę koniunktury. Szacuje się, że obecna różnica między podażą a globalnym popytem na półprzewodniki wynosi nawet 20%. W efekcie koncerny motoryzacyjne są zmuszane wstrzymać produkcję aut, skrócić wymiar pracy i podejmować decyzje, które modele nie trafią na rynek. Martwią się również m.in. producenci elektronicznych systemów zabezpieczeń, którzy o miejsce w kolejce muszą konkurować m.in. z producentami komputerów i smartfonów płacących o wiele lepiej.

Popyt przerasta podaż i wszyscy stoją po ten sam towar w kolejce. W 2011 roku przyczyną tego stanu rzeczy było trzęsienie ziemi w Japonii, które odbiło się na światowym przemyśle elektronicznym, gdy doszło do uszkodzeń w wielu fabrykach i utraty zdolności produkcyjnej przez 53 zakłady (łącznie 130 linii produkcyjnych)⁴. Dlaczego zwiększenie produkcji, jak o to wnioskował u jednego z producentów Peter Altmaier, niemiecki minister gospodarki, nie jest takie łatwe⁵.

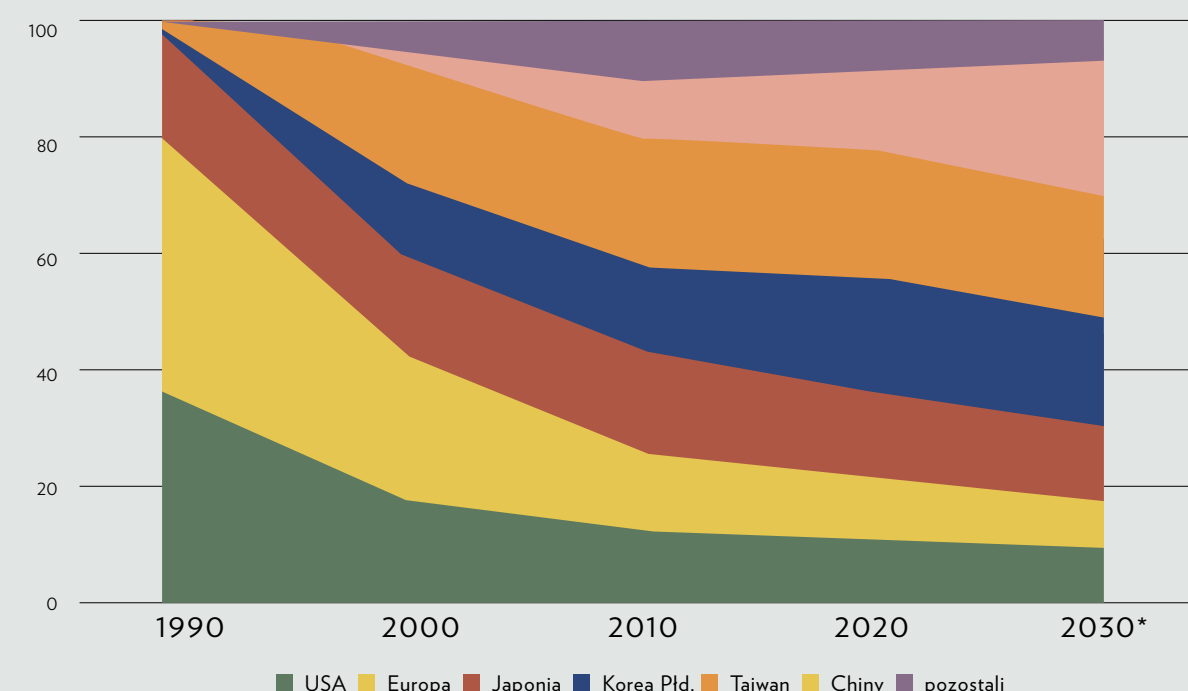
Żeby właściwie pokazać przyczynę obecnych kłopotów, należy zacząć od „wafli”, czyli gładkiej, okrągłej płytki wyciętej najczęściej z monokryształu krzemu. Jednym z najważniejszych kroków, kiedy krzemowe wafle zamieniają się w zdolne wykonywać miliardy operacji na sekundę mikroukłady (chipy),

³ Dane Boston Consulting Group i Semiconductor Industry Association pokazują, jak bardzo w ostatnich dekadach produkcja chipów oddaliła się od tradycyjnych ośrodków, w tym Japonii. W 1990 roku Japonia, Europa i Stany Zjednoczone dominowały w produkcji półprzewodników, ale wraz z wejściem na rynek Korei Południowej, Tajwanu i Chin kontynentalnych, te trzy pierwsze lokalizacje w 2020 r. odpowiadały za zaledwie około 35 proc. rynku. Trend spadkowy ma kontynuować do 2030 roku.

⁴ <https://elektronikab2b.pl/biznes/13078-kataklizm-przerwal-ciaglosc-lancucha-dostaw-polprzewodnikow/28/11/2021>

⁵ <https://www.reuters.com/article/taiwan-autos-chips-idUSL1N2JZ04I/25/11/2021>

Rys. 1. Wielkość światowej produkcji półprzewodników wg lokalizacji (w %)



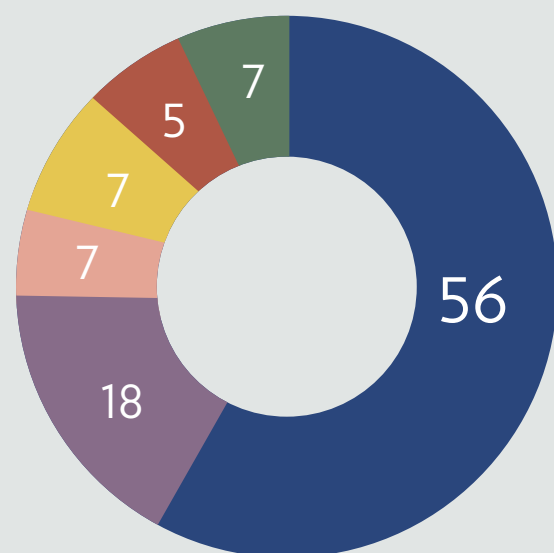
źródło: <https://www.statista.com/chart/25552/semiconductor-manufacturing-by-location/>

* predykcja

jest fotolitografia, czyli rzeźbienie światłem. Proces wymaga tak ogromnej precyzji (typowo 10 nm – dla przykładu włos ludzki ma ok. 400 µm, czyli 40 tys. razy więcej) i zaawansowania technologicznego, że maszyny potrzebne do wytwarzania tych najbardziej skomplikowanych układów produkuje tylko jedna firma na świecie, holenderskie ASML (*Advanced Semiconductor Materials International*). Natomiast garstka producentów mających do nich dostęp decyduje o tym, co i w jakich ilościach będzie produkowane⁶. TSMC (Tajwan) wraz z Samsungiem (Korea), UMC (Tajwan), Global Foundries (USA) i SMIC (Chiny) kontrolują 93% światowego rynku produkcji półprzewodników (rys. 2). Taką pozycję firmy te uzyskały głównie dzięki standaryzacji współczesnych chipów, co pozwoliło na całkowite lub częściowe zlecenie produkcji na zewnątrz.

Jednocześnie ich produkcja to biznes wymagający stalowych nerwów – zarobek jest uzależniony od dużej skali działalności, bardzo kosztownych inwestycji i czasu. Często połowa przychodów jest przeznaczana na rozbudowę linii produkcyj-

Rys. 2. Udział w rynku producentów półprzewodników w I kw. 2021 (w %)



■ TSMC ■ Samsung ■ UMC ■ Global Foundries
■ SMIC ■ inne

<https://www.trendforce.com/presscenter/news/20210224-10675.html>

**PIĘĆ FIRM KONTROLUJE 93% ŚWIATOWEGO
RYNKU PRODUKCJI PÓŁPRZEWODNIKÓW.
W NAJBLIŻSZYCH LATACH INWESTYCJE
W ODLEWNIE WYNIOSĄ PRZESZŁO
300 MLD DOL.**

⁶ <https://itwiz.pl/na-swiecie-brakuje-procesorow-dlaczego-powstala-luka-podazowa-na-ryнку-półprzewodników/> 28/11/2021

nych i dotrzymanie tempa rozwoju technologii (TSMC w ub. roku wydał na inwestycje 17 mld dol. i planuje w ciągu trzech lat przeznaczyć 100 mld dol. na zwiększenie mocy produkcyjnych, Samsung zaś zamierza wydać 116 mld dol. w ciągu dekady na nowe odlewnie)⁷ – wielu producentów nie wytrzymuje tego wyścigu.

Problemy wynikające z takiej sytuacji dostrzegli nie tylko liderzy korporacji, ale także przywódcy polityczni. Półprzewodniki, nazywane „ropą naftową XXI wieku”, to produkt, który już dzisiaj wpływa na globalny układ sił, a trwający kryzys zmusił światowe potęgi do szybkich i zdecydowanych działań. Jak zauważa prof. Włodzisław Duch⁸, obecnie trwający kryzys pokazał, że pierwszym odbiorcą ograniczonej liczby produktów są bogate kraje. W dobie kryzysu kraje słabe technologicznie są ostatnie w kolejce. Stąd wielomiliardowe plany wsparcia, mające uodpornić rodzime rynki i zapewnić krajom dostęp do tego strategicznego zasobu zostały w ostatnim czasie ogłoszone w Chinach, USA i Unii Europejskiej (której ambicją jest posiadanie 20% udziału w rynku do 2030 r.)⁹.

Liderzy 20 europejskich krajów (w tym Polska) sygnowali w grudniu 2020 r. deklarację „Europejskiej inicjatywy na rzecz procesorów i technologii półprzewodnikowych”. Jej celem jest zapewnienie niezależnego dostępu do różnych dóbr strategicznych oraz rozwoju tradycyjnych gałęzi przemysłu.

Korea Płd. jest stawiana za wzór zarządzania rodzimą gospodarką i odporności na globalne zawirowania, co stało się możliwe głównie ze względu na kontrolowanie wszystkich elementów łańcucha wartości¹⁰:

1. produkcji nieskomplikowanych elementów,
2. produkcji elementów zaawansowanych technologicznie,
3. wytwarzania produktów gotowych.

W efekcie urządzenia koncernów koreańskich są dostępne niemal od ręki. W obecnej sytuacji wygrywają te kraje, które kontrolują łańcuch wartości (od surowców po gotowe produkty), mają know-how, edukację na odpowiednim poziomie i innowacyjność – Koreańczycy na tym polu ewidentnie wygrywają¹¹.

Zdaniem ekspertów kryzys może jeszcze potrwać. Jeśli miałyby się skończyć przed świętami Bożego Narodzenia, to raczej w 2022 niż 2021 roku. Najwięksi producenci mikroprocesorów (TSMC oraz Samsung) rozpoczęli już inwestycje w rozwój mocy produkcyjnych, jednak ich efekty będą widoczne dopiero po pewnym czasie. Przy dużej sztywności podaży dalszy rozwój sytuacji będzie więc zależał przede wszystkim od kondycji globalnego popytu w najbliższych miesiącach. Jeśli pozostanie mocny, koniec kryzysu zaopatrzeniowego półprzewodników zobaczymy zapewne dopiero w 2023 roku¹². 📍

⁷ <https://forsal.pl/biznes/przemysl/artykuly/8137281,producenci-chipow-z-wiekszym-sladem-weglowym-niz-stare-przemysly.html> 27/11/2021

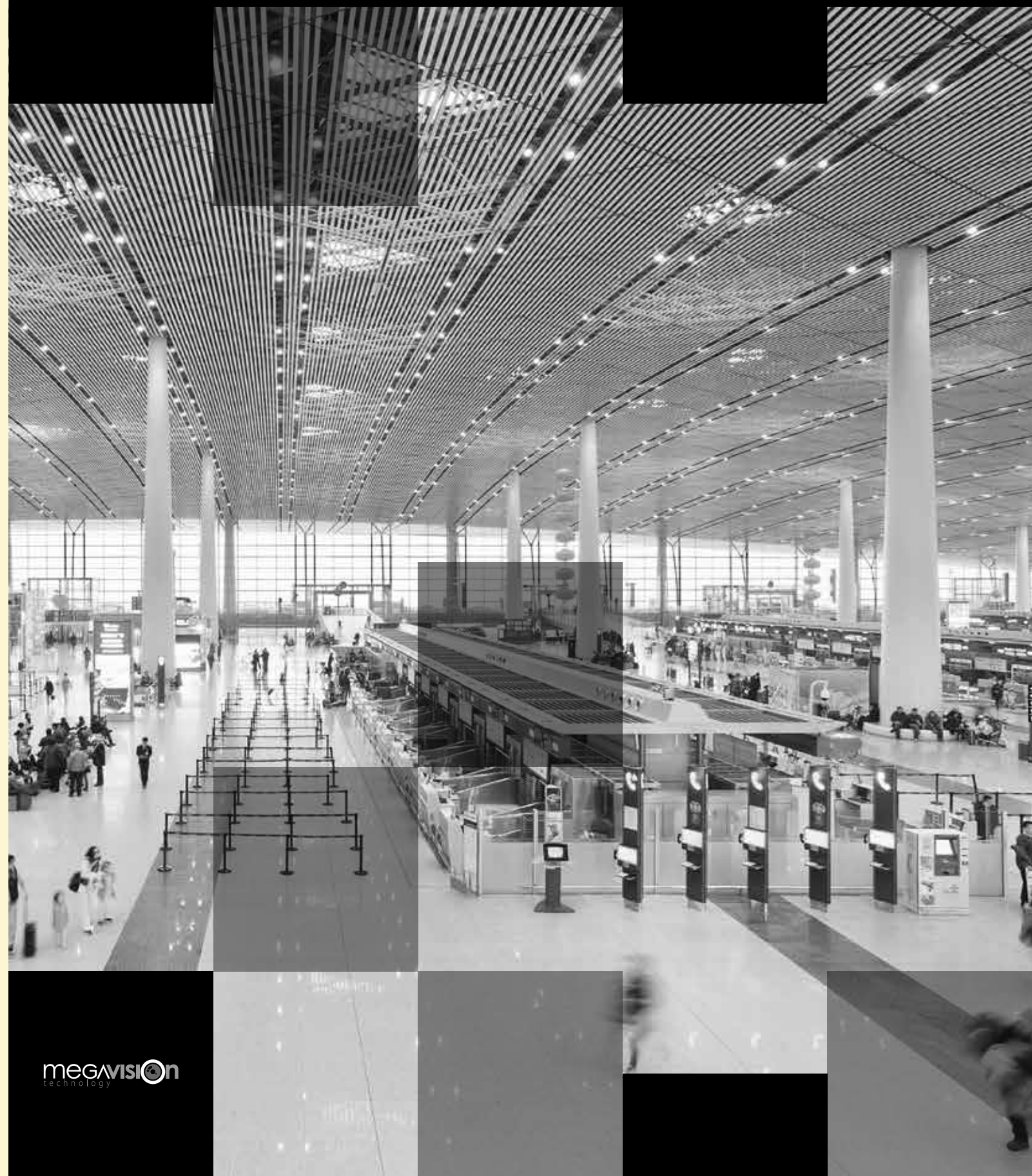
⁸ Polski naukowiec, profesor nauk fizycznych specjalizujący się w informatyce stosowanej, neuroinformatyce, sztucznej inteligencji, uczeniu maszynowym, kognitywistyce i neurokognitywnych technologiach; w latach 2014–2015 podsekretarz stanu w Ministerstwie Nauki i Szkolnictwa Wyższego

⁹ <https://www.extremetech.com/computing/320563-eu-wants-20-percent-of-semiconductor-manufacturing-by-2030> 27/11/2021

¹⁰ Według Michaela E. Portera to sekwencja działań podejmowanych przez firmę, aby opracować, wytworzyć, sprzedać i dostarczyć produkt, a następnie świadczyć usługi posprzedażowe.

¹¹ <https://raportostaniewiata.pl/w-powiekszeniu/swiat-cyfrowy/> podcast z 6 listopada 2021 z Jakubem Chabikiem

¹² <https://tvn24.pl/biznes/tech/kryzys-na-ryнку-półprzewodników-największy-od-dekad-5453518>, 28/11/2021



Rola inżyniera uruchomieniowego w procesie inwestycyjnym

Trudności, pułapki i szanse

Tym razem postanowiłem poruszyć umysły nieszablonowymi określeniami, niecodziennymi porównaniami czy też kontrowersyjnymi тезami. Zaczę od dość zaskakującej, przynajmniej na pierwszy rzut oka, ale dobrze przemyślanej i moim zdaniem trafnej definicji osoby inżyniera uruchomieniowego oraz tego, czym powinien się zajmować w procesie inwestycyjnym.



Michał Zalewski

Pomysł na sformułowanie takiej definicji pojawił się z potrzeby wypełnienia luki, nie spotkałem bowiem takowej informacji w polskiej inżynierskiej rzeczywistości. Kim zatem jest i czym zajmuje się inżynier uruchomieniowy? Moim zdaniem **inżynier uruchomieniowy to osoba, której zadaniem jest określenie, zaplanowanie, pomoc w przeprowadzeniu i udokumentowaniu zintegrowanego, wielobranżowego procesu uruchomienia obiektu i instalacji będących na jego wyposażeniu.**

To skomplikowane, więc rozłożmy definicję na czynniki pierwsze. Najpierw przedmiot, czyli proces uruchomienia. Tutaj zapewne wszystko jasne, trzeba wszyst-

ko uruchomić. Wielobranżowy to też oczywiste. Najczęściej uruchomienie dotyczy systemów wielu branż jednocześnie i wszystko trzeba robić w tym samym czasie. Skąd więc pomysł na określenie zintegrowany? Czy nie lepiej określić jednocześnie? Otóż nie, przywołam również moją definicję integracji z numeru 5/2020 „a&s Polska”: *Integracja niezależnych systemów to takie ich połączenie, dzięki któremu osiągamy dodatkowe funkcjonalności niedostępne dla systemów niezintegrowanych.*

W określeniu zintegrowany proces uruchomieniowy mamy ten sam powód użycia tego sformułowania. Każda branża (pakiet wentylacyjny, elektryczny, automatyki HVAC) dobrze wie, co i jak ma uruchomić. Ale z osobna, bez ścisłego współdziałania z innymi, albo nie jest w stanie tego zrobić, a już na pewno nie w odpowiednio krótkim czasie. Stąd świadome użycie słowa zintegrowany, bo w tym współdziałaniu jest ogromna wartość dodana, niedostępna przy jego braku. Przejdziemy do zadań inżyniera uruchomieniowego z przytoczonej definicji.

OKREŚLENIE PROCESU URUCHOMIENIOWEGO

Trzeba sporządzić pełną listę urządzeń, systemów, elementów budynku, które muszą być uruchomione dla osiągnięcia zakładanej funkcjonalności obiektu. Lista ta musi uwzględniać również podsystemy i zbiorcze elementy poszczególnych systemów (poszczególne szafy automatyki w systemie BMS, centrale, podcentrale i pętle w systemie SSP, maszynownie, zaworownie, sekcje i podsekcje instalacji tryskaczowej itp.). Przecież to wszystko jest w projekcie, więc po co? Przede wszystkim po to, by je zidentyfikować i określić w jednym dokumencie, który nazywam planem uruchomień. Przygotowanie takiego planu poprzedza analiza projektów wykonawczych poszczególnych branż, opisów projektu budowlanego, architektonicznego, warunków ochrony ppoż., scenariuszy pożarowych, listy we/wy systemu SSP, opisów algorytmów pracy poszczególnych instalacji itp.

Z doświadczenia wiem, że zawsze w projekcie taka analiza wskaże tematy uruchomieniowe, których nikt wcześniej nie zauważył, np. centralka pogodowa w systemie sterowania oddymianiem grawitacyjnym dla bardzo skomplikowanego geometrycznego dachu, wspomniana w projekcie w opisie architektury jednym zdaniem: podział na odpowiednie grupy poszczególnych sekcji okien oddymiających będzie zależał od kierunku wiatru. I nic więcej nie znajdziemy w całym projekcie.

ZAPLANOWANIE PROCESU URUCHOMIENIOWEGO

Gotowy plan uruchomień najpierw przekształcamy w harmonogram poprzez ustalenie kolejności i następstwa pracy uruchomieniowej na poszczególnych systemach, elementach oraz czas trwania poszczególnych zadań. Drugim zadaniem jest omówienie ze wszystkimi uczestnikami zintegrowanego procesu uruchomieniowego poszczególnych zadań im przynależnych oraz określenie i uzgodnienie zasad kolejności pracy. Nie da się uruchamiać tych systemów po kolei, gdyż nie ma na to odpowiednio dużo czasu, trzeba to umiejętnie robić równolegle. Zaczynamy od uruchomienia pętli modułowych SSP, automatyki wentylacji oraz układu sterowania klapami oddymiającymi i bytowymi, koniecznie równolegle. Następnie przerywamy uruchomienia SSP, przeprowadzamy testy punktowe współdziałania interfejsów we/wy, dość krótkie, jeżeli wcześniej automatyka wentylacji była prawidłowo uruchomiona jako samodzielna, a wszystkie klapy zostały przetestowane elektromechanicznie. Następnie punktowo z SSP sprawdzamy po kolei każde z urządzeń.

To przykład dla zilustrowania procesu, natomiast wszystkie te i podobne aspekty trzeba szczegółowo omówić z inżynierami odpowiedzialnymi za poszczególne systemy i uzgodnić zintegrowanie działania. Słowo „uzgodnić” jest tutaj kluczowe. Do swojego planu trzeba przekonać możliwie największą liczbę osób, inaczej będą próby działania wg własnych pomysłów lub potrzeb, bez zwracania uwagi na główny cel lub priorytety.

I tutaj pierwsza pułapka: podobnie jak w integracji systemów, tak i w integracji uruchomień ważna jest spójność komunikacji. Przy próbie „poukładania” zespołu inżynierów zawsze dochodzi do spięć i konfliktów wynikających najczęściej wyłącznie z powodu braku prawidłowej komunikacji. To zadanie dla inżyniera uruchomieniowego, by połączyć czasem sprzeczne plany i interesy we wspólny zintegrowany cel.

POMOC W PRZEPROWADZENIU URUCHOMIEŃ

Celowo używam słowa „pomoc”. Zdarzyło mi się kilka razy, że moja propozycja współpracy jako inżyniera uruchomieniowego była źle zrozumiana. Wykonawca SSP stracił pracownika odpowiedzialnego za uruchomienie systemu (opracowanie matrycy sterowań i programowanie). Poproszono mnie o pomoc, oczekując, że zaprogramuję SSP. A to nie ta funkcja i nie te kompetencje. Owszem, inżynier uruchomieniowy musi znać zasady programowania systemów, by np. wspomóc programistę w doborze odpowiedniego planu adresacji, ale nie może koncentrować się tylko na programowaniu.

Podobnie dla wentylacji: inżynier uruchomieniowy nie mierzy wydajności wentylacji, tylko tak zaplanuje wcześniejsze działania, by umożliwić jej przeprowadzenie. W tym samym czasie nie można prowadzić uruchomień SSP (klapy odcinające wentylacji będą zamykały się przy każdym teście), nie można testować Systemu Zasilania Rezerwowego (SZR), Przeciwpowarowego Wyłącznika Prądu (PWP), agregatu, nie mówiąc o pracach pyłących. Rolą inżyniera uruchomieniowego powinno być trochę arbitralne podzielenie czasu na uruchomienia poszczególnych pakietów, by nie powodowały kolizji lub konieczności powtarzania części prac.

Ktoś słusznie zauważył: przecież to już zostało zaplanowane. Racja, ale każdy projekt jest uni-

katowy, napotyka się nieoczekiwane problemy i niezbędna jest korekta planów, trzeba znajdować nowe rozwiązania dla nieoczekiwanych przeszkód lub problemów.

UDOKUMENTOWANIE URUCHOMIEŃ

Nie jest to jedynie podpisanie protokołów końcowych, że wszystko działa. Ważne jest udokumentowanie problemów i usterek stwierdzanych podczas poszczególnych etapów uruchomień, a także opis podjętych działań naprawczych. Jest to ważne, ponieważ może mieć wpływ na prawidłową eksploatację budynku. Coraz więcej inwestorów nabiera świadomości, że taka wiedza jest cenna i w tych procesach wymaga aktywnego uczestnictwa nadzoru inwestorskiego. Ostatnio obserwuję również podobne działania generalnych wykonawców, gdyż oczekiwania wydłużania czasu gwarancji w budynkach i zapewnienia prowadzenia czynności serwisowych (nie mylić z serwisem eksploatacyjnym) przez okres gwarancji wymuszają przygotowania do sprawnego procesu usuwania usterek.

Brak informacji z uruchomień może powodować konieczność ponownego przeprowadzania badań, testów itp., bo ich wyniki mogą być pomocne w szukaniu przyczyn awarii. Co ważne, ten fakt może rzutować na bezpieczeństwo budynku lub osób w nim przebywających. Przykłady: inaczej potraktujemy awarię zaciętej klapy oddymiającej, jeżeli to jest jej pierwsze zacięcie, wezwiemy serwis do naprawy czy kontroli, inaczej zaś, gdy w dokumentach uruchomieniowych będzie wskazane, że dana klapa już na początku wykazywała problemy. Inaczej podejmiemy do szukania przyczyny zakłóceń magistrali komunikacyjnej, jeżeli będziemy mieli pewność, że na początku działała poprawnie, a inaczej, jeśli w trakcie testów zostały już odnotowane problemy, np. powtarzające się przy określonych testach strefy dymowej. Dlatego warto dokumentować pisemnie wyniki testów i sprawdzeń, ta wiedza może być pomocna. I argument najważniejszy: warto posiadać kopie takich dokumentów w przypadku sporów, poważnych awarii oraz (odpukać) tragicznych zdarzeń na terenie obiektu.

Dokumentowanie uruchomień może być odbierane jako niepotrzebna „papierologia”, ale jeżeli potrafimy wspomóc proces poprzez sporządzenie wzorów list kontrolnych i czynności, mając gotowe do wypełnienia formularze testów, zyskamy większe zrozumienie i aprobatę. Na tym właśnie polega oferowana przez inżyniera uruchomieniowego pomoc w uruchomieniach – nie można dać się wciągać w bezpośrednie uruchomienia, to nie twoja rola, zaplanuj szczegółowe plany testów i przygotuj gotowe formularze. Co ważne, „spersonalizowane”, czyli przystosowane do konkretnego obiektu, konkretnych systemów i rozwiązań. Nie będzie akceptacji twoich pomysłów, jeżeli check lista uruchomieniowa będzie zawierała pozycje, w które należy wpisywać wynik „Nie dotyczy”.

Inżynier uruchomieniowy nie powinien głęboko angażować się w bezpośrednie uruchomienia poszczególnych elementów. Jeżeli jednak posiadasz wiedzę szczegółową, to dziel się nią z innymi. Pokazuj, jak można coś zaprogramować szybciej, lub pomagaj w wyszukiwaniu sposobów kontynuowania testów po napotkaniu problemów. Jeżeli nie dojechała połowa sygnalizatorów akustycznych, nie przerywaj testów współdziałania, można zainstalować po jednym na każdym końcu linii, w najgorszym wypadku w trakcie testów sprawdź multimetrem stan wyjść. Nie przerywaj testów, gdy linki bramy pożarowej zerwały się przy pierwszym uruchomieniu – trzymacz bramy można przetestować, przykładając do niego śrubokręt (konieczne nie ferromagnetyczny). Ważne, by było to odnotowane w protokołach. Algorytm zostaną przetestowane, a potem, po naprawie lub uzupełnieniu braków, wystarczy jeden test, by wiedzieć, że wszystko działa.



Przy planowaniu uruchomień trzeba pamiętać, że harmonogram to nie cyrograf, można i należy nad nim pracować i korygować, by dopasować go w fazie uruchomień. A jeżeli uda się dotrzymać daty końcowej, nikt nie będzie miał pretensji o małe korekty w trakcie.

Wróćmy do określenia procesu uruchomieniowego. Zdarzało mi się pominąć w tej fazie jakiś fakt lub oczywiste wątpliwości. Przykłady: nieprecyzyjne sformułowania scenariusza pożarowego, brak algorytmu pracy (np. automatyki chłodu lub wentylacji) i deklaracja, że programista wgra gotowy program, okazało się natomiast, że kaskada pracy układu wież nie uwzględniała rotacji, tylko załączanie zawsze wg zapotrzebowania tej samej kolejności. Żywotność układu dramatycznie spadła, bo pierwsza wieża wyeksploatowała się już po roku. Projektant myślał, że to sprawa oczywista, i nie napisał, a programista zaprogramował to, co otrzymał w wytycznych. Każde zbagatelizowanie identyfikacji lub nieprecyzyjność zapisów obracało się przeciwko jakości lub, co gorsza, było powodem problemów odbiorowych. Jeżeli więc coś zauważysz i masz wątpliwości, walcz uparcie o wyjaśnienie. Na papierze to tylko trochę więcej pracy projektanta, podczas uruchomień zaś to czas stracony na przeprogramowywanie i ponowne testy.

Nie każdy dostrzega walory i korzyści z zaproszenia inżyniera uruchomieniowego do pomocy. Moje doświadczenia są jednak takie, że coraz częściej udaje się zachęcić do współpracy przy projekcie. W przypadku dużych i skomplikowanych obiektów łatwiej przekonać do tego pomysłu, na łatwych jest mniej potrzeb. Jednak zawsze jest wiele problemów i trzeba być gotowym na duży wysiłek, pot i łzy, ale warto, bo satysfakcja jest ogromna.

Odważnych i z odpowiednim doświadczeniem zapraszam do zajęcia się tematem i promowania poprzez swoje oferty innowacyjnej pozycji w trakcie projektów. Mniej doświadczonych zapraszam do kontaktu, zadawania pytań, dzielenia się wątpliwościami. Wszystkich gorąco zachęcam do dyskusji. ☺

MICHAŁ ZALEWSKI

Absolwent Politechniki Gdańskiej i studiów podyplomowych Zarządzania Projektami Politechniki Warszawskiej. W branży od 24 lat, od 12 lat niezależny konsultant, inżynier uruchomieniowy.



ARGUS

rodzina systemów integrujących klasy PSIM do zarządzania bezpieczeństwem obiektów

✖ ARGUS WEB

✖ ARGUS RV

✖ ARGUS RV-C

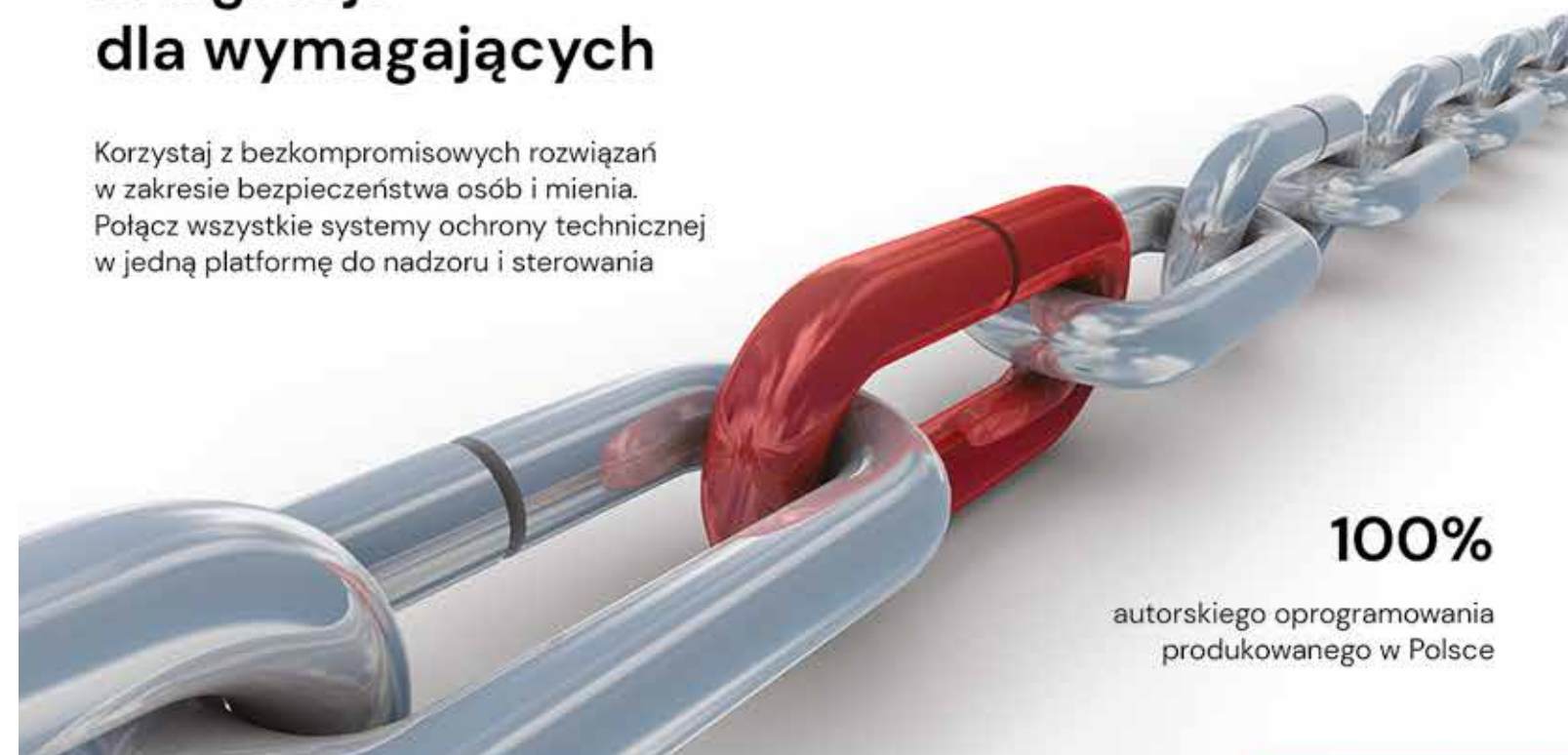
bezpieczeństwo
obiektów w przeglądarce
internetowej

wysokowydajny
system integrujący

sprzętowo-programowa
platforma z certyfikacją
CNBOP-PIB

Integracje dla wymagających

Korzystaj z bezkompromisowych rozwiązań w zakresie bezpieczeństwa osób i mienia. Połącz wszystkie systemy ochrony technicznej w jedną platformę do nadzoru i sterowania



100%

autorskiego oprogramowania
produkowanego w Polsce



Telbud S.A.
ul. Krauthofera 23
60-203 Poznań

f in



+48 61 866 88 48



www.telbud.pl



telbud@telbud.pl

1987
rok założenia



Listopadowe nowości SATEL

Jesienią br. oferta urządzeń i akcesoriów marki SATEL przeznaczonych do systemów sygnalizacji włamania i napadu oraz automatyki budynkowej została rozszerzona o kilkanaście nowych pozycji.

UNIERSALNY ETHERNETOWY MODUŁ MONITORUJĄCY

ETHM-A umożliwia przesyłanie informacji za pośrednictwem sieci Ethernet, pracując zarówno autonomicznie, jak i jako element systemu alarmowego czy automatyki. Ośmiem wejść modułu można wykorzystać do pracy z czujnikami analogowymi lub urządzeniami mającymi wyjścia NO lub NC. Do magistrali cyfrowych czujników 1-Wire można podłączyć do 8 detektorów. Dzięki temu moduł może gromadzić i przysyłać w ramach IoT różnego typu dane, np. aktualną temperaturę, stopień wilgotności i inne. ETHM-A współpracuje z dowolną centralą alarmową (podłącza się go do jej dialera telefonicznego lub odpowiednio skonfigurowanych wyjść), przekazując do stacji monitorującej zdarzenia, które miały miejsce w systemie alarmowym (m.in. załączenie czuwania, alarm).

ETHM-A umożliwia powiadamianie wybranych użytkowników o określonych zdarzeniach za pomocą komunikatów PUSH na urządzenia mobilne z zainstalowaną aplikacją GX CONTROL oraz poprzez wiadomości e-mail. Moduł ma cztery wyjścia typu OC, których stan zmienia się wraz z naruszeniem wejść. Wyjściami można też sterować zdalnie z ww. aplikacji mobilnej, komputera z programem GX Soft lub w ramach Internetu rzeczy.

INTELIWENTNA WTYCZKA

ASW-200 przeznaczona do współpracy z dwukierunkowym systemem ABAX 2 służy do włączania/wyłączania urządzeń elektrycznych o mocy do 2300 W. Wyposażona jest w LED Ring, którego kolor świecenia może m.in. zmieniać się



wraz ze zmianami mocy podłączonego odbiornika – od niebieskiego, przez zielony, aż do czerwonego. Inteligentna wtyczka dostępna jest w dwóch wariantach: z gniazdem sieciowym typu E (EURO) i F (SCHUKO).

BEZPRZEWODOWA CZUJKA TLENKU WĘGLA

ACMD-200 to kolejne urządzenie systemu ABAX 2, które może pracować także w trybie autonomicznym. Czujka ta nadzoruje stężenie tlenku węgla (czadu) w chronionym pomieszczeniu. Gdy przekroczy ono niebezpieczny poziom, zgłoszony zostaje alarm.

PRZYCISKI NAPADOWE

Trzy modele przycisków napadowych: przewodowy PB-10 oraz bezprzewodowe APB-200 (system ABAX 2 – pasmo częstotliwości 868 MHz) i MPB-300 (system MICRA – 433 MHz), oprócz wzywania pomocy czy wyzwalania alarmu napadowego, mogą być używane do sterowania pracą różnych urządzeń, np. systemu automatyki lub kontroli dostępu.

KURTYNY WEWNĘTRZNE

Czujki kurtynowe CD-2 (wersja przewodowa) i ACD-220 (beziprzewodowa – ABAX 2) są wyposażone w czujnik PIR i przeznaczone do montażu wewnątrz pomieszczeń. Ich obudowy charakteryzują się kompaktowymi wymiarami i wyglądem nawiązującym do uniwersalnych czujek XD-2 i AXD-220. Dostępne są w trzech wersjach: białej, brązowej i ciemnoszarej.

HERMETYCZNA OBUDOWA CZUJEK

Nawiązując do czujek uniwersalnych, należy wspomnieć o obudowie OPX-1 przeznaczonej właśnie do tych urządzeń. Jest wykonana z wytrzymałego poliwęglanu i ma klasę szczelności IP65 – umieszczone w niej czujki mogą być montowane na zewnątrz budynków. Gdy wymagana jest współpraca z magnesem, należy sięgnąć po OPXM-1 – magnes zamknięty w szczelnej obudowie. Dostępne są w trzech kolorach: białym, szarym i czarnym.

RETRANSMITER SYGNAŁÓW RADIOWYCH ABAX 2

ARU-200 umożliwia zwiększenie zasięgu komunikacji radiowej systemu ABAX 2. Odbiera transmisje od urządzeń bezprzewodowych (których może obsłużyć nawet 46) i przekazuje je dalej. Więcej informacji można znaleźć na stronie www.satel.pl



Satel
MADE TO PROTECT



INT-TSH2



INT-TSG2



INT-TSH2 i INT-TSG2 NOWA JAKOŚĆ W STEROWANIU systemami alarmowymi i automatyki budynkowej



Zeskanuj kod QR telefonem
i przejdź do serwisu **YouTube**

ReX 2

Weryfikacja fotograficzna przez stal i beton

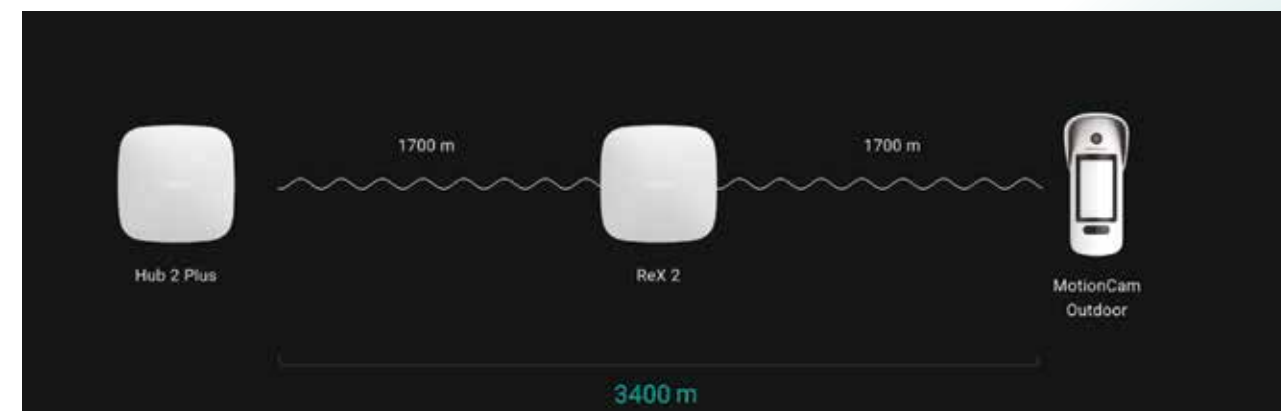
ReX 2 to nowa generacja inteligentnych podwajaczy zasięgu firmy Ajax z obsługą weryfikacji fotograficznej. Dzięki ReX 2 czujki MotionCam i MotionCam Outdoor można zainstalować dwa razy dalej od huba, a zapowiedziana duża aktualizacja oprogramowania OS Malevich pozwoli na ich instalację za betonowymi ścianami i metalowymi osłonami.



ZWIĘKSZONY ZASIĘG KOMUNIKACJI RADIOWEJ

ReX 2 zapewnia dwukierunkową komunikację za pośrednictwem bezpiecznych protokołów Jeweller i Wings w odległości do 3400 m od huba. System złożony z pięciu podwajaczy zasięgu może objąć teren o powierzchni 35 km². Jest to rozwiązanie przydatne w magazynach, kompleksach przemysłowych i innych dużych zakładach.

Dzięki zbliżającej się aktualizacji oprogramowania OS Malevich podwajacz zasięgu ReX 2 będzie w stanie łączyć się z hubem drogą radiową, a także poprzez sieć Ethernet. Dzięki temu będzie można chronić wielopiętrowe budynki z podziemnymi parkingami i dzielonymi metalowymi magazynami bez osłabienia lub odbicia sygnału radiowego. ReX 2 będzie komunikować się z hubem poprzez router. System Ajax nie ogranicza potencjalnego zasięgu przewodowego połączenia Ethernet, ale długie segmenty będą wymagały zastosowania wzmacniaczy lub łączy światłowodowych z konwerterami.



Połączenie Ethernet umożliwi korzystanie z podwajacza zasięgu jak z punktu dostępu dla bezprzewodowych czujek w piwnicy, na innych piętrach lub w pobliskich budynkach – w miejscach, gdzie zasięg radiowy jest niedostępny lub niestabilny. Zdarzenia i alarmy nawet w przypadku najbardziej złożonych obiektów będą dostarczane natychmiast. Pierwszy obraz z weryfikacji fotograficznej wyświetli się w stacji monitorowania i aplikacji użytkownika już w 10 sekund po uruchomieniu alarmu.

WZMACNIANIE SYSTEMU ALARMOWEGO

ReX 2 to coś więcej niż zwykły podwajacz zasięgu. Łączy urządzenia w autonomiczne grupy i zarządza ich komunikacją, umożliwiając połączenie do 199 urządzeń (w zależności od modelu huba). Jednocześnie nie ma to wpływu na stabilność łączności radiowej i prędkość dostarczania zdarzeń. Jeśli z jakiegoś powodu nie ma łączności z hubem, a czujki zarejestrują włamanie, ReX 2 odbierze sygnał alarmowy i włączy syrenę, aby zwrócić uwagę na zdarzenie.

FOTOGRAFICZNA WERYFIKACJA ALARMÓW

Nowy podwajacz zasięgu współpracuje z czujkami ruchu MotionCam i MotionCam Outdoor. Czujki wykonują serię zdjęć po wykryciu ruchu, umożliwiając ocenę sytuacji na miejscu. Alarm jest dostarczany w czasie 0,3 sekundy, a pierwsze zdjęcie dociera do stacji monitorowania i aplikacji użytkownika w 13 sekund za pośrednictwem protokołu Wings i w 10 sekund przez Ethernet. Zdjęcia na każdym etapie transmisji chroni szyfrowanie. Przechowywane na serwerze Ajax Cloud nie są przetwarzane ani analizowane.

Fotograficzna weryfikacja alarmów jest widoczna tylko dla użytkowników, którzy mają dostęp do zdarzeń huba, jak również dla pracowników agencji ochrony, jeśli system alarmowy jest podłączony do stacji monitorowania.

WIELOPOZIOMOWA OCHRONA PRZED SABOTAŻEM

ReX 2 pracuje z systemem OS Malevich, który jest chroniony przed wirusami i cyberatakami. Podwajacz zasięgu zgłasza zakłócenia kanałów radiowych, zagłuszanie, utratę łączności Ethernet, a także wykrywa próby demontażu obudowy. W przypadku awarii zasilania zapasowa bateria umożliwia autonomiczną pracę nawet przez 38 godzin. Urządzenie spełnia wymagania klasy 2. europejskiej normy EN 50131 i jest w stanie odpierać ataki nawet wyszkolonych intruzów.

BEZPROBLEMOWA INSTALACJA I MINIMALNA KONSERWACJA

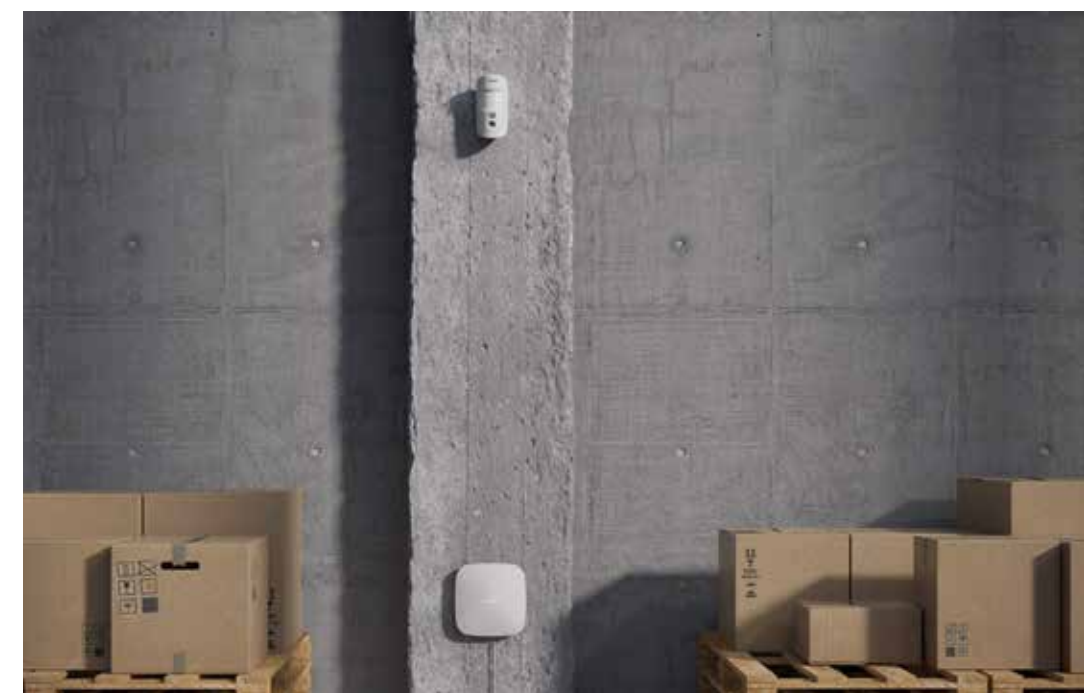
Dodanie podwajacza zasięgu ReX 2 do systemu wymaga jedynie zeskanowania kodu QR w aplikacji Ajax. W aplikacji są także dostępne testy tłumienia i mocy sygnału radiowego, co ułatwia znalezienie najlepszego miejsca do instalacji.



Adresowanie każdego urządzenia umożliwia monitorowanie stanu danego ReX 2 w czasie rzeczywistym z użyciem aplikacji mobilnej Ajax i aplikacji PRO Desktop. Ustawienia można zmieniać zdalnie bez konieczności wizyty na miejscu.

AJAX SYSTEMS POLAND

Fryderyka Chopina 41/2
20-023 Lublin
<https://ajax.systems/pl/>



Czy powstałe przed laty budynki biurowe

mogą skutecznie walczyć o nowego najemcę?

Zbliża się koniec roku 2021, mamy już za sobą kilka fal COVID-19 i pewnie kilka jest jeszcze przed nami. Ta globalna sytuacja dotknęła wszystkich aspektów naszego życia. W szczególności nie oszczędziła branży nieruchomości, o czym świadczą puste przestrzenie biurowe.

Błażej Ożga

Ten rok pokazał też, że inwestorzy mimo wszystko ruszyli z nowymi inwestycjami. *Home office*, stając się dominującym standardem pracy, wymusił na inwestorach zmianę założeń działalności w obiektach biurowych. Z powierzchni zastawionych setkami biur przeksztala się je w miejsca, które sprzyjają pracy zarówno indywidualnej, jak i zespołowej. Jednak muszą być one bezpieczne pod względem zagrożeń epidemiologicznych, fizycznych i cyfrowych.

Biurowce, które są teraz przeprojektowywane, aby sprostać nowym potrzebom, zostaną już niedługo oddane do użytku. Nasuwa się natomiast pytanie: co z tymi, które zostały oddane do użytku kilka, kilkanaście lat temu. W jaki sposób mogłyby one konkurować z nowymi inwestycjami? Okazuje się, że w większości przypadków wystarczy zastanowić się, co należałoby zmodernizować, aby starsze nieruchomości stały się na nowo atrakcyjne dla najmu. Decyzję o unowocześnieniu lub wymianie poszczególnych podsystemów należałoby oprzeć na analizie celów. A niewątpliwie jednym z ważniejszych jest sprawienie, aby budynek był bardziej przyjazny i bezpieczny.

Kluczowym elementem mającym na to bezpośredni wpływ jest system kontroli dostępu. Po pierwsze stanowi on fizyczną barierę dla intruzów, po drugie ułatwia sterowanie przepływem osób, po trzecie jest wizytówką danej nieruchomości, po czwarte może oferować coś więcej niż tylko samą kontrolę dostępu, mianowicie otwartość na integrację z innymi rozwiązaniami. Wybór odpowiedniego rozwiązania powinien być poprzedzony szczegółową analizą aktualnej sytuacji. Wprowadzenie nowego systemu kontroli dostępu nie musi zawsze wiązać się z całkowitą wymianą istniejącego rozwiązania. Niekiedy wystarczy integracja istniejących systemów, oprogramowania i urządzeń w celu maksymalnego wykorzystania danej inwestycji. Należy przeprowadzić audyt aktualnego systemu

kontroli dostępu i sporządzić pełną listę urządzeń, serwerów i elementów wyposażenia sieci, które są wykorzystywane przez ten system, jednocześnie pamiętając o konieczności aktualizacji funkcji oprogramowania, które ma pozostać w modernizowanym rozwiązaniu. Może się też okazać, że wymiana okablowania, zasilaczy, a w niektórych przypadkach kontrolerów czy czytników kart nie musi być konieczna. Jeżeli po analizie dojdziemy do wniosku, iż system spełnia wymagane funkcjonalności, możemy ogłosić sukces, co jednak rzadko ma miejsce, zwłaszcza że najczęściej nie był on modernizowany od momentu oddania budynku do użytkowania.

Następnym krokiem jest przygotowanie planu i harmonogramu wymiany. Skróci to czas, kiedy poszczególne przejścia KD będą wyłączone z działania. W proces ten powinny być zaangażowane wszystkie zainteresowane strony, m.in. najemcy również powinni być o tym poinformowani, aby uniknąć nieporozumień podczas prowadzonych prac.

Kolejnym krokiem jest instalacja nowego serwera kontroli dostępu. To fundament nowego systemu. Wykonanie tego kroku umożliwi wcześniejsze przeszkolenie zaangażowanych stron, co z kolei przełoży się na płynniejszą migrację. Następnie należy wykonać import danych ze starego systemu kontroli dostępu do nowego. Skróci to czas przejścia, ponieważ często wymieniany system zawiera dane, które z powodzeniem mogą znaleźć się w nowym.

Kolejnym etapem jest wykonanie niezbędnych integracji (jeżeli są konieczne) umożliwiających spełnienie określonych wcześniej celów. Takimi pracami mogą zostać objęte połączenia z systemem windowym, systemem parkingowym, mobilnymi kartami czy też z kluczowym elementem każdego nowoczesnego budynku biurowego – systemem zarządzania gośćmi (*Visitor Management System*). Teraz można rozpocząć montaż nowych elementów z jednoczesnym usuwaniem starych komponentów. To również ważny etap, ponieważ usunięcie starych urządzeń zapobiega bałaganowi i ułatwia kontrolę nad sytuacją.



ODDANIE NOWEGO SYSTEMU DO EKSPLOATACJI JEST KOLEJNYM ETAPEM. OBEJMUJE ON TAKIE ELEMENTY, JAK:

- przekazanie dokumentacji, w tym niezbędnych rysunków i schematów,
- przeszkolenie użytkowników i administratorów,
- przeprowadzenie testów funkcjonalnych.

W całym procesie modernizacji systemu KD nie należy zapominać o serwisie nowego rozwiązania i jego cyklicznej konserwacji. Pamiętajmy, że wszystko się starzeje oraz, co ważniejsze, podlega aktualizacjom. W szczególności oprogramowanie, które już teraz jest podstawowym elementem każdego systemu. Dlatego należy wybrać takie rozwiązanie, które zapewni długoletnie wsparcie oraz dostępne aktualizacje. Spełniając cele stawiane modernizowanym budynkom biurowym, system kontroli dostępu AEOS może być z powodzeniem wykorzystywany przez naszych klientów w procesach migracyjnych. Skalowalność i otwartość na integrację to zalety, które wielokrotnie potwierdziły jego przydatność w zmodernizowanych systemach.

PRZYKŁADOWE ROZWIĄZANIE W ZAKRESIE MODERNIZACJI SYSTEMU KONTROLI DOSTĘPU MOŻE OBEJMOWAĆ:

- wymianę czytników RFID na takie, które umożliwiają użycie kart mobilnych (interfejs BLE, NFC),
- dodanie czytników kodów QR – umożliwienie czytania zaproszeń wysyłanych e-mailem do zaproszonych osób,
- integrację z systemem windowym,
- integrację z dedykowaną aplikacją budynkową,
- integrację z systemem zarządzania salami konferencyjnymi,
- obsługę parkingu z wykorzystaniem czytnika tablic rejestracyjnych,
- włączenie funkcji liczenia osób i pojazdów.

Jeszcze raz chciałbym podkreślić, że w całym tym procesie najważniejsze są wygoda użytkowania i bezpieczeństwo nowego rozwiązania. 

NEDAP SECURITY MANAGEMENT

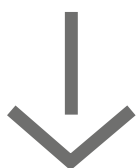
al. Niepodległości 18
02-653 Warszawa
www.nedapsecurity.com/pl/





Nowoczesny system kontroli dostępu

Zaproponuj swoim klientom coś wyjątkowego. WaveKey to technologia najszybszego mobilnego dostępu na rynku, która wyróżnia się za sprawą najwyższej niezawodności w swojej klasie oraz doskonałego poziomu bezpieczeństwa. Zobacz, jak nam się to udało.



NAJWYŻSZA NIEZAWODNOŚĆ W SWOJEJ KLASIE

Sześć miesięcy intensywnych testów w biurówcu pełnym zapracowanych osób pozwoliło osiągnąć to, na czym nam zależało. Przetestowaliśmy otwieranie drzwi ponad 15 000 razy, korzystając ze 100 rozmaitych modeli telefonów 20 marek. WaveKey to marka, której naprawdę można zaufać.

NAJSZYBSI NA RYNKU

WaveKey otwiera drzwi w 0,3 sekundy, dzięki czemu z powodzeniem sprawdzi się nawet w biurówcach, gdzie czas jest na wagę złota. Tajemnica tkwi w wyjątkowym systemie preautoryzacji do 8 numerów telefonów komórkowych w zasięgu czytnika.

ROZWIĄZANIE PROBLEMU NIEPOŻĄDANEGO OTWIERANIA DRZWI

Dzięki adaptacyjnym algorytmom i analizie sygnału RSSi czytnik wie, czy użytkownik zbliża się do niego, czy też oddala. Telefon znajdujący się w zasięgu, lecz leżący nieruchomo nigdy nie spowoduje otwarcia drzwi.

NAJWYŻSZY POZIOM BEZPIECZEŃSTWA

Nasz bezpieczny algorytm kompleksowo chroni komunikację za pośrednictwem systemu Bluetooth. Wykorzy-

staliśmy klucze szyfrowania AES-128 i RSA-1024. W zasadzie uniemożliwia to przechwycenie i niewłaściwe wykorzystywanie mobilnych danych uwierzytelniających.

BEZPROBLEMOWE PRZEKAZYWANIE DANYCH

Za sprawą zaledwie kilku kliknięć w interfejsie sieciowym administrator generuje dane uwierzytelniające telefonu komórkowego i przesyła je zdalnie do użytkowników. Nie trzeba spotykać się z użytkownikami, aby przekazać im te dane, ani generować kosztów na infrastrukturę do fizycznej dystrybucji.

BRAK OPŁAT ZA DANE UWIERZYTELNIAJĄCE

Dzięki nam użytkownik nie musi ponosić niepotrzebnych kosztów. Dane uwierzytelniające telefonów komórkowych do kontroli dostępu są zawsze tańsze niż karty RFID. My oferujemy je bezpłatnie. Zupełnie tak samo, jak naszą aplikację 2N® Mobile Key.

WYBIERAJ SPOŚRÓD CZTERECH TRYBÓW

To ty decydujesz, które tryby są dostępne w czytnikach, dzięki czemu użytkownicy mogą wybrać odpowiedni sposób dostępu.

- Tryb dotykowy to gwarancja pełnej wygody. Użytkownicy muszą tylko dotknąć czytnik dłonią albo łokciem, bez konieczności wyjmowania telefonu.
- Bezkontaktowy dostęp w trybie aplikacji to gwarancja jeszcze większego bezpieczeństwa. Użytkownicy muszą dezaktywować ewentualny ekran blokady i otworzyć drzwi za pomocą wirtualnego przycisku w aplikacji. To także doskonały sposób na otwieranie bramy parkingowej z poziomu samochodu.
- Tryb ruchu jest całkowicie bezkontaktowy. Wystarczy podejść do wideodomofonu z telefonem w kieszeni lub pomachać dłonią przed kamerą, a drzwi się otworzą.
- Ostatnia opcja to tryb karty. Telefon działa jak karta, a użytkownik musi umieścić go blisko czytnika. Przypomina to popularną technologię NFC, ale w przypadku WaveKey ta opcja jest dostępna na telefonach z systemami Android oraz iOS.

CO JEST POTRZEBNE, ABY SKORZYSTAĆ Z NASZEGO ROZWIĄZANIA W ZAKRESIE MOBILNEGO DOSTĘPU?

Użytkownicy muszą zainstalować w swoim telefonie aplikację 2N® Mobile Key. Jest dostępna bez opłat na telefony z systemami iOS oraz Android. Rozwiązanie obejmuje także nasze czytniki kontroli dostępu z łącznością Bluetooth. Takie rozwiązanie jest dostępne w przypadku wybranych produktów z rodziny 2N Access Unit 2.0, 2N Access Unit M oraz wideodomofonów 2N® IP Style i 2N® IP Verso z modulem Bluetooth. Proste i szybkie zarządzanie inteligentnym systemem kontroli dostępu i mobilnymi danymi jest możliwe za pomocą oprogramowania 2N® Access Commander. ☑



**Polskie profesjonalne
zintegrowane rozwiązania
VMS
Ponad 200 000 instalacji
na całym świecie
Jesteśmy z Wami od
2003 roku**

Z naszych rozwiązań korzysta



Wiodący przetwórcza technicznych tworzyw sztucznych,
kluczowy dostawca dla branży motoryzacyjnej,
elektronicznej, kosmetycznej
oraz czołowy europejski producent
profesjonalnego sprzętu ręcznego
do utrzymywania czystości

www.alnetsystems.com

Automatyczny skarbiec SafeStore Auto

– czyli skrytki
depozytowe jak
z bankomatu



Zacznijmy od wykonania prostego ćwiczenia: prosimy zamknąć oczy i wyobrazić sobie, że korzystamy ze skrytki depozytowej. Zazwyczaj taka wizja przybiera poniższą formę:

Wchodzimy do budynku, a miły pracownik prowadzi nas korytarzami, na których końcu widzimy piękne otwarte drzwi skarbcza. Przechodzimy przez nie, podziwiając ich grubość, i znajdujemy się w pomieszczeniu w całości wypełnionym małymi drzwiczkami do skrytek depozytowych.

STOP!

Co powinno nas, jako właścicieli depozytów ukrytych za tymi drzwiczkami, zaniepokoić w powyższym opisie?

Uzasadniony powód do niepokoju to „otwarte drzwi” i „znajdujemy się w środku”. Co to bowiem oznacza w praktyce? W zależności od liczby skrytek codziennie dziesiątki, a może i setki różnych osób wchodzi do skarbcza, a te piękne, grube drzwi są przeważnie cały czas otwarte. Ale czy na pewno trzeba wchodzić do skarbcza, aby skorzystać ze swojej skrytki depozytowej?

SKARBIEC ZA ZAMKNIĘTYMI DRZWIAMI

Okazuje się, że istnieje alternatywny, znacznie bezpieczniejszy system korzystania z usług depozytowych, który już dziś znajduje się w naszym zasięgu. Oferowane przez koncern Gunnebo automatyczne skarbcze depozytowe SafeStore Auto (SSA), którym poświęcony jest ten artykuł, budują rzeczywiście odpowiadają naszemu wyobrażeniu: są tu piękne grube drzwi – z tym, że te drzwi pozostają cały czas zamknięte! **Klienci nigdy nie wchodzą do skarbcza!**

Co więcej, personel placówki nie ma możliwości otwierania drzwi skarbcza. Również i sam jego właściciel, w celu zwiększenia poczucia własnego bezpieczeństwa, często rezygnuje z możliwości samodzielnego otwierania drzwi skarbcowych. W takim wypadku zainstalowane na nich zamki elektroniczne są kontrolowane przez zewnętrzną firmę ochroniarską i tylko spełnienie uzgodnionych wcześniej procedur, takich jak przyjazd grupy interwencyjnej, pozwoli otworzyć drzwi. Jest to tzw. otwarcie komisyjne wymagające współpracy dwóch niezależnych podmiotów.

Jedynym mieszkańcem skarbcza jest robot, który wydaje skrytki do podajnika umieszczonego na ścianie lub w suficie skarbcza.

SKRYTKI DEPOZYTOWE JAK Z BANKOMATU

Z punktu widzenia klienta korzystanie ze skrytki depozytowej przypomina dokonywanie wypłat z powszechnie znanego bankomatu: tak jak bankomat wydaje banknoty poprzez szczelinę w obudowie, tak i nasz automat skarbcowy, dostarczając skrytkę do podajnika, umożliwia klientowi swobodny dostęp do jej wnętrza.

Ulepszeniem w porównaniu z funkcjonalnością znaną z bankomatu jest dodanie czytnika linii papilarnych / cech biometrycznych. Klient ma zatem

możliwość wyboru jednej z trzech form identyfikacji na terminalu: karta + PIN + biometryka, karta + PIN lub karta + biometryka. Ponadto każda skrytka ma własny zamek kluczowy, a klient jest posiadaczem obu kluczy do swojej skrytki.

POKÓJ Z PODAJNIKIEM SKRYTEK

Chyba każdemu towarzyszy uczucie pewnego dyskomfortu, gdy korzysta z bankomatu na chodniku przy ruchliwej ulicy. Naszym głównym celem w konstrukcji automatu skarbcowego SafeStore Auto było zapewnienie poczucia pełnego bezpieczeństwa klientom korzystającym ze swoich skrytek, dlatego zawsze przy naszym skarbcu znajduje się tzw. pokój bezpieczeństwa – pomieszczenie, w którym umieszcza się podajnik skrytek depozytowych. Przy drzwiach do tego pomieszczenia montuje się czytnik kontroli dostępu. Klient dopiero po uzyskaniu autoryzacji może wejść do środka. W sytuacji, gdy system jest w użyciu (inny klient korzysta właśnie ze swojej skrytki), system operacyjny skarbcza zarządzający wspomnianym czytnikiem odmówi wejścia, informując: „System w użyciu”.

GWARANCJA BEZPIECZEŃSTWA

Motto szwedzkiego koncernu Gunnebo, widoczne w logo, głosi *For a safer world – Działamy na rzecz bezpiecznego świata*. Produkowany w Niemczech automatyczny skarbiec depozytowy SafeStore Auto to pod tym względem nasze szczytowe osiągnięcie. SSA posiada bowiem certyfikaty antywłamaniowe w klasach od VII do X. Ponadto przyznano mu certyfikat EX potwierdzający odporność antywybuchową. Te atesty są wydawane przez niemieckie jednostki certyfikacyjne VdS lub ECB•S. Co najważniejsze: certyfikatem objęte jest całe prezentowane urządzenie, a nie tylko drzwi lub panele ściennne. Jest to możliwe dzięki specjalnej konstrukcji, w której podajnik skrytek stanowi integralną część skarbcza. Ciekawostką jest fakt, iż pod pięknym wykończeniem podajnika (blat z materiału typu Corian) kryje się betonowa konstrukcja, a sam podajnik waży ok. 800 kg.

SAMOKONTROLA I SAMOREJESTRACJA

System operacyjny skarbcza SafeControl zapisuje każde zdarzenie związane z pracą robota i weryfikacją dostępu na terminalu. Zapis ten jest przechowywany w szyfrowanej bazie danych na serwerze znajdującym się wewnątrz skarbcza. Modyfikacja zapisów jest wykluczona, a klient może w dowolnym momencie poprosić o wydruk historii zdarzeń dla swojej skrytki. Ponadto system SafeControl cały czas monitoruje działanie skarbcza, a wszelkie nieprawidłowości są zapisywane w systemie w postaci kilku kategorii alarmów.

WERSJE MOBILNA I STACJONARNA

Najpopularniejszymi wersjami skarbcza typu SSA są wersje MIDI i MAXI.

Modele MIDI to skarbcze w całości wyprodukowane w fabryce w Niemczech. Gotowe urządzenia typu plug and play są przywożone na miejsce i instalowane w pomieszczeniu docelowym. Jako że wysokość skarbcza wynosi zaledwie 192 cm, a jego szerokość 170 cm, instalacja jest znacznie ułatwiona – choć należy pamiętać o masie skarbcza, która może dochodzić do 11 000 kg. Pojemność wersji MIDI to maks. 430 skrytek przy długości skarbcza wynoszącej 392 cm.



Druga powszechnie stosowana wersja to SSA MAXI. Ten skarbiec jest dostarczany w częściach i składany w lokalizacji docelowej. Pojemności w tej wersji mogą sięgać kilku tysięcy skrytek.

NISZA RYNKOWA, CZYLI IDEALNY MOMENT NA INWESTYCJĘ

Widoczny w całej Europie trend zamykania kolejnych placówek bankowych sprawił, iż w ostatnich latach rosnącą grupą oferującą usługi dostępu do automatycznych skrytek depozytowych stali się inwestorzy z sektora prywatnego. Zaskakująco krótki czas zwrotu z inwestycji, niewielka potrzebna przestrzeń, bezpieczeństwo całego projektu oraz możliwość oferowania unikalnej całodobowej usługi dostępu do skrytek w trybie 24/7 przyczyniają się do rosnącej popularności tej formy inwestycji.

20 LAT I 1600 SKARBCÓW

I najważniejsze na koniec: opisany skarbiec to nie nowość! Takie skarbcze produkujemy już od blisko 20 lat, a liczba dostarczonych skarbców przekracza 1600 sztuk. Większość z nich jest zainstalowana w kraju ich produkcji, czyli w niemieckich bankach. Obecnie oferowana wersja oprogramowania i robotyki charakteryzuje się bardzo wysoką stabilnością pracy, co jest efektem doświadczeń nabytych przez wspomniany czas i na podstawie ogromnej liczby działających już urządzeń typu SSA. Dzięki temu i w Polsce możemy z dumą prezentować flagowy produkt koncernu Gunnebo, jakim jest automatyczny skarbiec ze skrytkami depozytowymi z linii SafeStore Auto. Zapraszamy do wyszukania w serwisie YouTube hasła "SafeStore Auto PL" i obejrzenia polskojęzycznej animacji prezentującej działanie systemu. Istniejąca od blisko 30 lat firma Gunnebo Polska zlokalizowana w Kaliszu zapewnia pełne wsparcie udokumentowane dziesiątkami instalacji systemów SSA w Polsce i za granicą. ☺

GUNNEBO POLSKA

ul. Chopina 20-22, 62-800 Kalisz
Tomasz.Derbich@Gunnebo.com
www.GunneboSafeStorage.com/pl-PL/





Kamery nasobne w służbie

W przestrzeni publicznej można znaleźć doniesienia o niewłaściwie realizowanych interwencjach, nieuprawnionym stosowaniu przymusu, w tym środków przymusu bezpośredniego. Jednocześnie funkcjonariusze służb mundurowych czy pracownicy ochrony podczas pełnienia obowiązków nierzadko spotykają się z wrogością, atakami fizycznymi, naruszeniami nietykalności i innymi agresywnymi zachowaniami. Często po interwencji zarzuca się im niewłaściwe postępowanie.



Rafał Batkowski

Pomocna w takiej sytuacji okazuje się kamera nasobna (*body camera, body worn camera, weareble camera*). Zarejestrowany przez nią materiał może stanowić dowód w sprawie, zwiększa poczucie bezpieczeństwa funkcjonariuszy, pełni też funkcję prewencyjną – wpływa na deeskalację konfliktu i ogranicza zachowania przemocowe. Istotny jest również społeczny aspekt zastosowania takich urządzeń, tj. zapobieganie nadużyciom ze strony funkcjonariuszy, a w przypadku wyjaśnienia skarg obywateli – szybki i łatwy proces weryfikacji okoliczności zdarzenia.

WŁAŚCIWOŚCI

Wiele informacji technicznych dot. kamer nasobnych producenci podają w kartach katalogowych. W szczególności są to dane dotyczące

zapisu obrazu i dźwięku. Od nowych urządzeń powinniśmy oczekiwać nagrywania w jakości full HD i czasu zapisu od 30 do ponad 70 godz. w zależności od rozdzielczości, a także obiektywu szerokokątnego (ponad 140°) i podświetlenia IR niezbędnego do pracy w porze nocnej. Ważną funkcją jest nagrywanie w odpowiednich interwałach czasowych i nadpisywanie materiału. Po aktywacji urządzenia włącza się tryb nagrywania ciągłego (z fonią lub bez niej), a system automatycznie dodaje zbuforowany obraz sprzed interwencji, np. 2-minutowy.

Istotne jest to, jak długo kamera nasobna może pracować. Dziś producenci oferują urządzenia, które w trybie ciągłym działają nawet ponad 12 godzin. Jest to czas wystarczający, tym bardziej że kamera w trybie wykorzystywanym czy to w pracy służb porządku publicznego, czy też pracowników ochrony służy głównie do nagrywania działań interwencyjnych, a nie przekazywania/nagrywania obrazu z całej służby. Producenci umożliwiają też transmisję obrazu na żywo dzięki karcie SIM i transmisję przez sieci komórkowe. Jest to o tyle istotne, że w przypadku poważnej interwencji dowodzący działaniami mogą tę sytuację monitorować, wydawać dyspozycje i podejmować trafne decyzje służące np. przywróceniu ładu i porządku, zatrzymaniu niebezpiecznego przestępcy itp.

Mówiąc o praktycznych aspektach kamer nasobnych, na które warto zwrócić uwagę, bardzo przydatnymi cechami będą szybkość ładowania, prostota w posługiwaniu się urządzeniem i brak możliwości ingerencji pracownika w nagrany materiał, co daje gwarancję rzetelnego przekazu, który można wykorzystać w toku czynności procesowych lub wyjaśniania wątpliwych działań przez przełożonych funkcjonariuszy lub pracowników ochrony. Dla każdego użytkownika kluczowa jest także odporność na uszkodzenia mechaniczne, czynniki środowiskowe, warunki atmosferyczne – najnowsze modele kamer mogą pracować w każdym środowisku właściwym dla obowiązków policjantów lub pracowników ochrony.

Istotny jest oczywiście moment, w którym kamera rozpoczyna nagrywanie. Pracownik/funkcjonariusz może ją uruchamiać poprzez wciśnięcie odpowiedniego przycisku. Aby urządzenie zadziałało niezawodnie, producenci oferują też możliwość automatycznego włączania nagrywania, np. w reakcji na odgłos wystrzału czy niebieskie światła uprzywilejowania. Samoistne aktywowanie trybu interwencji (nagrywania) jest kolejnym ułatwieniem dla użytkowników i wspiera profesjonalne wykonywanie ich zadań. Systemowe rozwiązanie w tym zakresie obejmuje także sensory umieszczone np. w kaburze z bronią lub paralizatorem elektrycznym.

Dla funkcjonariuszy korzystających z kamer i organizujących ich służbę znaczenie ma także sprawne i szybkie zgry-

wanie materiału. Jeżeli nie stosujemy rozwiązań opartych na danych w chmurze, warto sięgać po modułowe systemy dokujące ładujące baterię kamery i jednocześnie zgrywające materiał, znakujące konkretne pliki danych, przygotowując je do szybkiego wyszukiwania i analizy, określając stosowne kryteria wyszukiwania (miejscę, czas, funkcjonariusz/pracownik itp.). Wiodący producenci proponują także aplikacje do zarządzania cyfrowym materiałem dowodowym, w tym pochodzącym z innych źródeł.

ZASTOSOWANIA

Kamery nasobne najczęściej i w największej liczbie stosują służby porządku publicznego – policja, straż miejska. Trzeba jednak zwrócić uwagę na ich wykorzystanie przez pracowników ochrony. Miałem okazję, odpowiadając za bezpieczeństwo portu lotniczego w Warszawie, wdrażać kamery nasobne do użytkowania przez pracowników Straży Ochrony Lotniska (SOL – wewnętrzna służba ochrony operująca w obiekcie infrastruktury krytycznej). Nie wszyscy wiedzą, że kilka lat temu SOL jako pierwsza tego rodzaju formacja zastosowała kamery nasobne. Wcześniej urządzenie testowały policja i straż miejska, tam nastąpił proces wdrożenia. Wyposażono funkcjonariuszy w kamery zgodnie z obowiązującym porządkiem prawnym. Niewiele wyobrażało sobie, że pracownik ochrony również może takich urządzeń używać.

Chciałbym zwrócić uwagę na stanowisko Ministerstwa Spraw Wewnętrznych i Administracji wskazujące na brak powodów, dla których w świetle zapisów ustawy o ochronie osób i mienia pracownicy ochrony nie mogliby wykorzystywać w trakcie realizacji zadań „minikamer rejestrujących obraz i dźwięk”.

Taka konstatacja jest bardzo ważna dla wszystkich, którzy zarządzają obiektami podlegającymi obowiązkowej ochronie i innymi terenami chronionymi. Muszą spełnić wszystkie obowiązki informacyjne oraz cele przetwarzania pozyskanych danych w kontekście RODO. Należy też pamiętać, aby w regulaminie pracy i innych stosownych procedurach opisać dokładnie, jak postępować z kamerą, jakie są obowiązki pracownika, co robić z danymi, czemu mają służyć w procesie nadzoru nad pracownikiem ochrony.

Dlaczego to jest tak ważne? Wydaje się, że z punktu widzenia pracownika – który bywa oskarżany o niewłaściwe działania, że postępuje w sposób niezgodny z prawem – przekazanie kamery do jego użytkowania będzie wyrazem troski o jego bezpieczeństwo prawne, a także o profesjonalizm działania. Dbamy o jakość wykony-





wanych obowiązków (przeciwdziałamy naruszeniom prawa i procedur przez pracownika), lepiej nadzorujemy ich pracę. Wskazując jasno, że nagrywamy podejmowane czynności, możemy też ograniczać sytuacje konfliktowe i minimalizować agresywne, przemocowe zachowania, z którymi ma do czynienia interweniujący pracownik. Osoba, wobec której podejmowana jest interwencja, również widzi, że jej zachowania są monitorowane. Pamiętajmy, że większość ludzi w sytuacji problemowej, kryzysowej czy konfliktowej natychmiast sięga po urządzenie mobilne/telefon i nagrywa jej przebieg – warto mieć „swoją” obiektywny materiał.

W przypadku funkcjonariuszy służb państwowych te zadania są bardzo podobne. Skoncentruję się na policjantach – ich służba jest kluczowa dla bezpieczeństwa każdej społeczności lokalnej. Od policjantów oczekuje się poświęcenia i zaangażowania, działania w granicach prawa i na podstawie prawa, empatii i etycznych postaw oraz poszanowania praw człowieka – po prostu profesjonalnego działania. Zestawmy to z ogromną liczbą interwencji ok. 5,7 mln rocznie. Gros dotyczy interwencji w miejscach publicznych, które wymagają szczególnej uwagi, ostrożności i byłoby dobrze precyzyjnie je monitorować. Właśnie dlatego stosuje się kamery, aby zapewnić praworządność – bezstronne działanie zgodne z prawem i procedurami, a w sytuacji kiedy obywatel ma wątpliwości, by mieć szansę przejrzenia toku tej interwencji i oceny, czy sposób działania policjanta był adekwatny, czy nie naruszył prawa, a więc był właściwy w określonej sytuacji.

Ale jest też drugi, nie mniej istotny aspekt. Przełożony, dowódca ma dbać o to, żeby policjant czuł się bezpiecznie i pewnie podejmował decyzje o rozpoczęciu interwencji, żeby wiedział, co ma robić, by działać profesjonalnie. Pomijając kwestie wyszkolenia, wyposażenia i przygotowania do służby, to właśnie kamera nasobna może stanowić wsparcie, kiedy pojawiają się wątpliwości, gdy zarzuca się policjantom przekroczenie uprawnień czy niedopełnienie obowiązków itp. Powszechne zastosowanie kamer nasobnych nie tylko przez policjantów, ale także przez Straż Graniczną, Służbę Więzienną, Straż Miejską, uzbrojone formacje ochronne (SUFO) mogłoby zmienić obraz prowadzonych interwencji w Polsce, wpływając pozytywnie na każdą ze stron i obniżając gotowość do konfrontowania się, zwłaszcza z użyciem przemocy.



Patrząc na to w ten sposób, kamera może być istotnym wsparciem dla działań policyjnych. Nie należy się bać tych urządzeń, trzeba – i to jest także moje doświadczenie dotyczące służby – tłumaczyć pracownikom, również policjantom, że to nie jest działanie przeciwko nim, to nie jest próba nadmiernego kontrolowania ich działania. Zastosowanie kamer nasobnych ma głęboki sens ochrony prawnej i wpływa na profesjonalizm, którego oczekujemy czy to od policjanta, czy pracownika ochrony.

Niektórzy producenci oferują hybrydową możliwość stosowania kamer na mundurze lub w odpowiednich panelach mocujących w pojazdach. Doświadczenia policyjne wielu państw potwierdzają potrzebę monitorowania przestrzeni wokół pojazdu, kiedy interwencja jest podejmowana, lub wnętrza w sytuacji przewożenia zatrzymanego. To kolejne ważne rozwiązanie. Miałem przyjemność kilka lat temu inicjować pilotaż w Wielkopolsce w zakresie wdrażania kamer w pojazdach policyjnych przeznaczonych m.in. dla komórek patroloво- interwencyjnych i ruchu drogowego.

Był to znaczący i potrzebny projekt, którego uzasadnienie jest podobne, jak w przypadku kamer nasobnych. Obraz z kamery pojazdu często pozwala wyjaśnić przyczyny takiego zdarzenia i ocenić, czy policjant działał w sposób właściwy. Integracja z kamerami nasobnymi może wzbogacić ocenę zdarzenia. Pojazdy patrolujące tereny chronione również powinny posiadać takie urządzenia.

INTERWENCJE

Niektóre interwencje nie kończą się szczęśliwie. Znamy takie przypadki, chociażby wydarzenia z bieżącego roku odnotowane w województwie dolnośląskim zakończone śmiercią osób poddanych interwencjom: Lubin – 6 sierpnia; Wrocław – 2 sierpnia; Wrocław – 30 lipca. Opis zdarzeń wskazuje na agresywne zachowanie mężczyzn wobec policjantów oraz intoksykację środkami zmieniającymi świadomość. Nie wszystkie okoliczności zdarzeń są jasne.

Wątpliwości dotyczyły także wielu interwencji realizowanych w miejscach publicznych wobec osób protestujących, manifestujących swoje poglądy. Rozważania w tym zakresie należy prowadzić, nie zapominając o empatii, współczuciu wobec rodzin osób, które straciły życie, lub tych, które odniosły obrażenia. Jednocześnie odnosząc się do sposobu postępowania policjantów, pamiętajmy o ich ofierze i wielu tragicznych zdarzeniach, atakach, które ich dotyczą – ponad 150 policjantów poległo na służbie od czasu powstania policji w roku 1990.

Czy stosowanie kamer jest pomocne? Jak wyglądałby w pełni monito-



rowany przebieg każdej poważnej interwencji? Dzisiaj jeszcze nie da się precyzyjnie odpowiedzieć na tak postawione pytania, gdy odnosimy się do tegorocznych wydarzeń, ale powszechne wykorzystanie kamer nasobnych, szkolenia w tym zakresie oraz uświadamianie obywateli o sposobie działania policji i rejestrowaniu podejmowanych czynności na pewno wpłyną na mniejszą liczbę ofiar, redukcję naruszeń oraz generalną poprawę jakości służby i jej efektów. Integracja danych monitorujących pozwoli profesjonalnie zarządzać bezpieczeństwem w przestrzeni publicznej, przeciwdziałać nadużyciom i troszczyć się o bezpieczeństwo mieszkańców RP.

Pisząc krótko o osobistych urządzeniach rejestrujących, trudno szerzej komentować problemy interwencyjne identyfikowane w ostatnich latach w Polsce. Trzeba jednak pamiętać o kluczowej roli procesu szkolenia policjantów oraz często zaniedbywanego doskonalenia zawodowego w zakresie taktyki i technik interwencji podejmowanych lokalnie, w jednostkach policji. Czy skorzystano z wniosków po poprzednich tragicznych wydarzeniach związanych ze służbą, czy zrealizowano polecenia dotyczące nadzoru i organizacji służby? Jak oceniono stosowanie kamer nasobnych w toku interwencji? Na te pytania warto znać odpowiedzi, próbując optymalizować procesy podejmowania działań przez uprawnione podmioty wobec obywateli. Zgodnie z powszechnym przekonaniem kamery nasobne pozytywnie wpływają na bezpośrednie wykonywanie tak określonych czynności.

PRZYSZŁOŚĆ KAMER NASOBNYCH

Przewiduję, że wszyscy działający w przestrzeni publicznej i podejmujący interwencje wobec obywateli będą wyposażeni w nadajniki komunikacyjne zintegrowane z innymi urządzeniami, którymi operuje funkcjonariusz lub pracownik ochrony. W trybie przekazywania materiału w czasie rzeczywistym – strumieniowania sygnału wizyjnego i dźwiękowego do stanowiska kierowania kamera nasobna pozwoli na profesjonalne, trafne zarządzanie wybranymi elementami interwencji, akcji lub operacji służących bezpieczeństwu. Funkcjonalności oparte na zdalnym włączaniu urządzenia lub dostępie do strumienia wizyjnego mogą być istotne w sytu-

acjach awaryjnych, np. braku kontaktu z pracownikiem.

Przyszłością, w wielu aspektach naszego życia, będą także usługi chmurowe. Gromadzenie materiału z interwencji w chmurze znacznie ułatwi jego przetwarzanie, a wskazane możliwości dostępu do obrazu z kamery na odległość wpłyną na optymalizację zarządzania urządzeniami i działaniami policyjnymi.

Analiza danych zostanie wsparta w znacznie szerszym zakresie niż dotychczas sztuczną inteligencją (AI), co będzie skutkowało m.in. automatyzacją procesów przetwarzania informacji. Pozwoli to zredukować czas zaangażowania pracowników do czynności analitycznych i nadzorczych. Wykorzystanie AI wpłynie na jakość prezentowanych danych, pozwoli generować precyzyjne raporty.

Zastosowanie technologii *deep learning* i połączenie na potrzeby analizy danych z wielu sensorów, źródeł danych – rzeczywista integracja danych – w przyszłości umożliwi predykcję zdarzeń, zachowań osób poddanych interwencji. Przyszłość to także profilowanie sprawców i ich zachowań w czasie rzeczywistym, a wykorzystanie w tym zakresie nasobnych urządzeń komunikacyjnych wydaje się pożądane i interesujące. Nie wolno oczywiście zapominać o ochronie danych osobowych i trosce o prawa podstawowe każdego z nas.

Omawiane rozwiązania i perspektywa szerokiego stosowania kamer nasobnych wymagają działań świadomościowych, edukacyjnych w społeczeństwie oraz w odniesieniu do funkcjonariuszy i pracowników, którzy obawiają się nowych rozwiązań technologicznych, nie chcą być stale monitorowani, nadzorowani poprzez zdalne systemy audio-wideo.

Poszukanie właściwych, akceptowanych przez wszystkie strony procedur jest niezbędne. Kamery nasobne to w rzeczywistości troska o bezpieczeństwo prawne policjantów i innych funkcjonariuszy oraz pracowników ochrony, szansa na obniżenie poziomu emocji, agresji podczas interwencji i gwarancja dla obywateli w zakresie możliwości weryfikacji sposobu prowadzenia czynności na miejscu zdarzenia. ☉

DR RAFAŁ BATKOWSKI

Inspektor Policji w stanie spoczynku – w okresie służby m.in. naczelnik Zarządu Operacji Antyterrorystycznych w Komendzie Głównej Policji (KGP), mazowiecki komendant wojewódzkiej policji, wielkopolski komendant wojewódzki policji oraz szef Krajowego Biura Interpolu i Członek Zarządu Europolu. Obecnie ekspert Agencji UE ds. szkolenia Policji – CEPOL. Właściciel firmy RBS (Rafał Batkowski Strategie) i doradca na potrzeby innych podmiotów oraz międzynarodowych projektów.





www.axis.com/pl

Wszechstronne kamery od Axis

KAMERY NASOBNE AXIS ZAPEWNIĄĄ OSTRY OBRAZ W KAŻDYCH OKOLICZNOŚCIACH I DŹWIĘK Z SAMEGO CENTRUM AKCJI. SĄ LEKKIE, WYTRZYMAŁE, WODOODPORNE I ŁATWE W UŻYCIU. KAMERY WŁĄCZA SIĘ NA DOTYK. BUFORUJĄ ONE OBRAZ DO 90 SEKUND PRZED WŁĄCZENIEM REJESTRACJI. TRYB STEALTH UMOŻLIWIA NAGRYWANIE Z UKRYCIA. KAMERY NIE DA SIĘ WŁĄCZYĆ PRZYPADKOWO.



↓ Wytrzymały akumulator, ładowanie przez USB i szybkie pobieranie materiałów sprawiają, że kamery są natychmiast gotowe do pracy, a ich zdejmowanie trwa chwilę. Dodatkowo, miniaturowe i lekkie moduły optyczne mocuje się bezpośrednio do hełmów za pomocą standardowych mocowań Picatinny, dzięki czemu można rejestrować obraz wygodnie i dyskretnie. Kamery nasobne Axis są zgodne z systemem Axis VMS lub innymi

systemami VMS lub EMS do zarządzania materiałem wizyjnym. Kamery mają technologię Axis Zipstream, dzięki czemu można przechowywać zarejestrowany, dowolnie duży materiał wizyjny bez utraty jakości obrazu – lokalnie lub w chmurze. Dostępna jest aplikacja na telefony komórkowe do przeglądania i oznaczania materiałów. Dowody można łatwo wyszukać i zapisać. Kamery nasobne Axis spełniają normy FBI dotyczące cyberbez-

pieczeństwa dzięki kompleksowemu szyfrowaniu. Otwarte standardy i niedrogie stacje dokujące z oddzielnym kontrolerem systemu sprawiają, że są one wszechstronne, łatwe w użyciu i ekonomiczne w skalowaniu – można łatwo dodawać urządzenia i funkcjonalności. Otwarty standard umożliwia współpracę z dowolnym oprogramowaniem do zarządzania materiałem wizyjnym odpowiadającym indywidualnym potrzebom.

Kamery nasobne Axis odznaczają się najwyższą jakością i wytrzymałością na uderzenia. Dbłość o zachowanie jakości jest dla nas kluczowe, zapewniamy jakość podczas każdego kolejnego procesu: od produkcji, przez konfigurację, aż do testów. Na etapie projektowania każdy detal i element jest szczegółowo sprawdzany pod kątem spełnienia najwyższych standardów. Testujemy nasze produkty zarówno na żywo, jak i podczas rygorystycznych symulacji.

www.rtc.com.pl

Zobacz wszystko, nie przegap niczego

HYTERA OD PONAD TRZECH LAT Z SUKCESEM ROZWIJA CAŁY ZA-AWANSOWANY EKOSYSTEM SWOICH KAMER NASOB- NYCH – SAME URZĄDZENIA ORAZ AKCESORIA I OPRO-GRAMOWANIE. OBECNIE W OFERCIE SĄ TRZY MO-DELE: VM580D, VM750D I VM78. KOLEJNE PREMIERĘ BĘDĄ MIAŁY W I KW. 2022 R.



↓ Ich wspólne cechy to: obsługa transmisji danych i streamingu wideo z wykorzystaniem sieci WLAN lub 3G/4G, system operacyjny Android, możliwość pracy jako mikrofonogłosnik z radiotelefonami i terminalami Hytera (np. DMR, TETRA czy LTE) oraz współpraca z platformą PoC (PTT over Cellular) HyTalk – dostęp do łączności dyspozytorskiej z PTT. Wszystkie kamery firmy Hytera wspierają standard kompresji H.265 zapewniający prawie 2-krotnie lepszą kompresję danych w porównaniu z H.264, przy zachowaniu tej

samej jakości materiału. Wspierają też szyfrowanie danych oparte na AES256. Wszystkie też są odporne na pył i wodę (IP68). Zgodność z rygorystycznymi normami US Army MIL-STD-810G gwarantuje wysoką odporność na upadki, drgania i wibracje.

VM580D to podstawowy model kamery (grubość 20 mm, masa 172 g) z dotykowym wyświetlaczem LCD o przekątnej 2". Wymienny akumulator zapewnia ponad 8 godzin pracy. Kamera jest wyposażona w dodatkowy akumulator podtrzymujący funkcję nagrywania podczas wymiany akumulatora.

VM750D to najnowszy model kamery. O wiele większy ekran dotykowy LCD –

2.8" ułatwia korzystanie z funkcji i opcjonalnych aplikacji. Obsługuje technologię NFC (m.in. do identyfikacji użytkownika). Kamerę ma też funkcję stabilizacji obrazu.

VM780 – topowy model z obiektywem obracającym w pionie o 216° umożliwia uzyskanie optymalnego kąta widzenia. Wbudowany promiennik IR oraz dioda LED o mocy 1 W pozwalają na pracę o zmroku, a nawet w nocy.

Hytera oferuje oprogramowanie do zarządzania flotą kamer nasobnych oraz katalogowania, archiwizowania i zarządzania zebranym materiałem.

RTcom, autoryzowany dystrybutor firmy Hytera, oferuje bezpłatną możliwość testowania wymienionych urządzeń. Skontaktuj się z nami, wysyłając e-mail na adres: biuro@rtc.com.pl



ZAPOBIEGAJ AWARIOM INFRASTRUKTURY ZANIM WYSTĄPIĄ

Zabezpiecz swoją infrastrukturę aż przed 37 zagrożeniami fizycznymi, używając jednego urządzenia MultiSensor®. Właśnie to sprawia, że Kentix jest tak genialnie łatwy i wszechstronny w użyciu.

MultiSensor® wykrywa m.in.:

- WILGOTNOŚĆ
- JAKOŚĆ POWIETRZA
- TEMPERATURA
- TLENEK WĘGLA
- CIŚNIENIE
- KONTROLA URZĄDZEŃ
- WŁAMANIA
- WIBRACJE

KENTIX
Innovative Security



Niekomandos w centrum handlowym

Steward wsparty technologią robi różnicę

Centra handlowe, zwane galeriami handlowymi, to jedno z ulubionych miejsc spędzania czasu. Można by rzec, że ze swojej natury są bardzo „demokratyczne”. Powiew dobrobytu i elegancji, atmosfera zbytku i nierzadko piękna jest dostępna na wyciągnięcie ręki. Centra handlowe to fenomen społeczny, gratka dla socjologów. Te wielkie, np. warszawska Arkadia, łódzka Manufaktura czy poznańska Poshania, na mapie miast stanowią jeden z kluczowych punktów orientacyjnych.



Jacek Tyburek

Dla profesjonalistów zajmujących się bezpieczeństwem centra handlowe są zarówno wyzwaniem, źródłem dochodu, jak i wielkim ryzykiem. Większość z nas ma jeszcze ciągle przed oczami obrazy z ataku nożownika w warszawskiej Arkadii. Brak reakcji służb ochrony pokazany w materiale z kamery telefonu był szokujący. Pracownicy ochrony, wyglądający na zaawansowanych wiekiem, niesprawiający wrażenia sprawnych fizycznie czy zdeterminowanych, wykazali się całkowitą biernością. Nagrany materiał trwa ponad 2 minuty. Widzimy człowieka atakującego dwóch innych mężczyzn za pomocą prawdopodobnie noża oraz kopnięć i ciosów pięściami. Ochrona odsuwa się na bezpieczną dla siebie odległość. Po całym zdarzeniu napastnik wraz z młodą kobietą, która mu asystowała, odchodzi z miejsca zdarzenia. Niezbyt spieszenie. Po zorganizowanej policyjnej obławie w mieście udało się napastnika złapać.

W opracowaniach nt. bezpieczeństwa i ochrony galerii handlowych zazwyczaj dominuje temat prewencji antyterrorystycznej. Szczegółowe opracowanie renomowanego RAND Corporation z 2006 r. *Reducing Terrorism Risk at Shopping Centers. An Analysis of Potential, Security Options* czy też polskiego ABW z 2015 r. *Zabezpieczenie antyterrorystyczne wielkopowierzchniowych obiektów handlowych. Uniwersalny poradnik* bardziej lub mniej detalicznie koncentrują się na prewencji antyterrorystycznej zgodnie z założeniem publikacji. Tymczasem w Polsce nie odnotowano klasycznych zdarzeń o charakterze terrorystycznym w centrach handlowych. Zdarzały się bandyckie napady, ataki nożami przez osoby nie zrównoważone psychicznie, ale nie wypełniały one definicji terroryzmu. Nie próbuję przez to powiedzieć, że skoro takich zdarzeń nie ma, to nie należy się na nie przygotowywać. Absolutnie nie to jest moją intencją. Zarówno praktyka, jak i psychologia podpowiadają, że jeśli jakieś zdarzenie nie ma wysokiego prawdopodobieństwa wystąpienia, to determinacja do realnego, a nie tylko dokumentacyjnego przygotowania na taką okoliczność będzie wprost proporcjonalna do ryzyka. Zdarzeń bandyckich, w tym bardzo w naszej kul-

turze bulwersujących przypadków ataku nożem niewinnych i przypadkowych osób, też w zasadzie nie jest dużo. W ciągu ostatnich kilku lat odnotowaliśmy kilkanaście ataków wskazujących na podłoże kryminalne, fundamentalistyczne bądź niezrównoważenie psychiczne napastnika. Dotyczy to zarówno Europy Zachodniej, jak i Polski.

14 października 2012 r. niezrównoważony psychicznie napastnik zaatakował nożem lekarza prelegenta w CHR Galaxy w Szczecinie. W lipcu 2015 r. niezrównoważony emocjonalnie napastnik zaatakował nożem w centrum handlowym na Pradze Południe. 18 lutego 2017 r. policjanci postrzelili niezrównoważoną emocjonalnie kobietę, która groziła nożem klientom hipermarketu przy ul. Malborskiej w Warszawie. W dwóch ostatnich przypadkach nie doszło na szczęście do wtargnięcia agresorów na teren obiektu, jednak parkingi przy centrach handlowych mogą posłużyć jako potencjalne miejsce ataku, gdyż stosunkowo łatwo nie tylko go dokonać, ale też, korzystając z zamieszania, bezpiecznie się oddalić.

Najtragiczniejszy w skutkach był atak szaleńca uzbrojonego w dwa bagnety w galerii handlowej Vivo w Stalowej Woli 20 października 2017 r., w którego wyniku jedna osoba zmarła, a kolejnych 8 zostało ciężko rannych. Ze względu na miejsce ataku, wybrane cele, sposób przeprowadzenia i skalę można go z pewnością uznać za jeden z pierwszych w Polsce przypadków działania aktywnego mordercy. Co ważne, galeria nie była przygotowana na taki atak, a napastnika ujęli – ryzykując życie – cywile. A co by było, gdyby napastnik dysponował bronią palną? To pytanie kluczowe. 26 lipca 2018 r. najprawdopodobniej niezrównoważony psychicznie mieszkaniec powiatu stalowowolskiego ciągnikiem rolniczym staranował drzwi wejściowe do centrum handlowego Tesco w Stalowej Woli, po czym zaczął niszczyć siekierą witrynę sklepu jubilerskiego. Na szczęście nie zaatakował żadnej z osób przebywających w placówce. Po dokonaniu zniszczeń odjechał i staranował bramę wjazdową prowadzącą do komendy policji w Stalowej Woli. Dopiero wtedy udało się go obezwładnić. Ochrona placówki nie była przygotowana na tego typu atak, nie miał on też żadnych cech rabunkowych. Do tej listy należy doliczyć atak nożownika w Arkadii. Również tutaj ochrona obiektu nie była przygotowana na takie zdarzenie.

Zjawisko szerzej opisuje Daniel Boćkowski z Instytutu Historii i Nauk Politycznych Uniwersytetu w Białymstoku w pracy *Duże centra handlowe jako obiekty potencjalnych ataków terrorystycznych*. Chciałbym wskazać coś, co prawdopodobnie wszyscy podskórnie czujemy i nieraz podnosimy w dyskusjach: pracownicy ochrony nie byli, nie są i prawdopodobnie nigdy nie będą wystarczająco dobrze wyszkoleni, żeby poradzić sobie z napastnikami z nożem. Jednym z powodów jest fakt, iż to nie jest ich zadaniem. Pracownik ochrony w centrum handlowym to nie jest eks-komandos gotowy na wszystko. I nie może nim być. Nie uda się też go wyszkolić na tyle, by takiego nożownika z Arkadii skutecznie obezwładnić.

Jakie więc są ich zadania? Na oficjalnym spotkaniu z pewnością w odpowiedzi usłyszymy, że chodzi o zapewnienie bezpieczeństwa klientom galerii i najemcom sklepów. Oczekiwanie klientów prawdopodobnie sprowadzają się do udzielenia pomocy w trudnej sytuacji (kradzież, incydent na parkingu, czyjeś agresywne i niestosowne zachowanie), a także potrzebnych informacji. Łatwiej podczas spaceru w galerii spotkać pracownika ochrony niż trafić na punkt informacyjny lub interaktywną tablicę informacyjną. Pracownicy ochrony powinni więc doskonale znać topografię obiektu, a wręcz najnowszą ofertę. Rzeczywistość jednak jest taka, że mają być po prostu widoczni w pasażu. Stanowią swoisty wizualny symbol poczucia bezpieczeństwa.

Specyfika służby ochrony w galerii handlowej to miks zadań ochrony w zamkniętych centrach handlowych oraz zadań stewarda podczas imprezy masowej. Z jednej strony pracownik ma być widoczny i mieć wsparcie dowódcy zmiany lub centrum monitoringu: daje poczucie wsparcia, pewność,



że jest ktoś, kto udzieli pomocy. Z drugiej – to dynamiczna sytuacja z przemieszczającymi się przypadkowymi ludźmi w ograniczonej przestrzeni, których ma obserwować i reagować na ewentualne niepożądane zdarzenia. Informowanie, udzielanie pierwszej pomocy, asystowanie przy kolizjach na parkingach, reagowanie na agresywne zachowania, realizacja rozporządzeń sanitarnych (kontrola wchodzących do galerii pod kątem posiadania i prawidłowego noszenia masek sanitarnych w czasie pandemii COVID-19) to tylko kilka z szerokiego katalogu zadań pracowników ochrony.

Skala tej „imprezy masowej” lub „zamkniętego osiedla” jest jednak bardzo duża. Jak wyjaśnia Polska Rada Centrów Handlowych (PRCH), dane są zbierane z systemów kamer znajdujących się w centrach handlowych liczących klientów z dokładnością do 98%. *Porównywanie wyników z analogicznymi okresami w poprzednich latach pozwala na określenie obecnych trendów i przeanalizowanie bieżącej sytuacji. Badanie odnosi się także do poprzednich miesięcy roku – wskazano. Według PRCH tygodniowa odświeżalność oscyluje w granicach 82–87% w porównaniu do wyników z 2019 r. Porównując lipiec 2021 do lipca 2020 r., można zauważyć tendencję wzrostową.*

Co to oznacza w liczbach rzeczywistych? Manufaktura cieszyła się zainteresowaniem klientów na poziomie 20 mln odwiedzających w roku 2017. To średnio prawie 55 tys. osób więcej do galerii dziennie. Oczywiście te liczby inaczej się rozkładają w tygodniu, w weekend czy w okresach świątecznych. W jednym z opracowań podano, że średnia dzienna liczba osób odwiedzających CH Arkadia w Warszawie to ok. 150 tys. osób! Odniesienia do miast średniej wielkości same się nasuwają...

W wyniku pandemii skład zespołów ochrony w galeriach został ograniczony do minimum. Typowy zespół to pracownicy wykonujący patrol w pasażach, po jednym na poziom galerii (w najlepszym wypadku), osoby pracujące w strefach rozładunku, na parkingach i w pokoju monitoringu CCTV lub z BMS. W takiej sytuacji angażowano osoby z uprawnieniami i doświadczeniem strażaków.

Szeroko opisywany w łódzkiej prasie był przypadek Stanisława D., pracownika ochrony Manufaktury z zespołu ratowników przedmedycznych, który w ciągu 14 lat pracy uratował życie 30 osobom, klientom centrum. Pan Stanisław nie jest typowym pracownikiem ochrony. Nie jest typem testosteronowego twardziela dążącego do walki. Nie lubi manifestować siły, przemocy. Deklaruje, że przedkłada nad to niesienie pomocy innym. Przed zatrudnieniem się w Manufakturze był strażakiem, gdzie

jego zadaniem również było pomaganie ludziom. Po przejściu na emeryturę przyjął pracę w centrum jako ratownik przedmedyczny. Pracuje tu już 14 lat. Resuscytacji, czyli przywróceniu pracy serca poddał w tym czasie ok. 30 osób, które prawdopodobnie zmarłyby, gdyby nie jego pierwsza pomoc. Cieszy się z każdego uratowanego życia, najbardziej bołą go przypadki, gdy ponosi porażkę. Na jego oczach zmarły dwie osoby, starsza kobieta i młody mężczyzna. Jeśli wolno mi użyć przykładu pana Stanisława, to jest on stewardem modelowym. Nastawiony na działanie pomocowe, posiadający niezbędne umiejętności do skutecznego niesienia pomocy. Dokładnie taki model szkolenia i kształtowania pracownika obowiązuje w strukturach stewardingu. Standardowo każda galeria ma opracowane procedury bezpieczeństwa, które regulują sposób postępowania w przypadku różnego rodzaju zagrożeń, takich jak pożar, atak terrorystyczny, powódź, zagrożenie podłożenia ładunku wybuchowego. Są one stale uaktualniane, a pracownicy ochrony, zarządcy, inne służby porządkowe i najemcy odbywają cykliczne szkolenia przypominające oraz informujące o zmianach. Zgodnie z obowiązującymi procedurami raz na dwa lata przeprowadzamy próbne ewakuacje naszych obiektów, sprawdzając, jak personel, służby i klienci zachowują się w przypadku potencjalnego zagrożenia. Tymczasem praktycy zajmujący się zapewnieniem bezpieczeństwa w galeriach handlowych, głównie dostawcy usług ochrony, mówią o coraz trudniejszym realizowaniu zadań.

Jesteśmy obecnie w bardzo dziwnym momencie. Zarządcy galerii i centrów handlowych deklarują, że bezpieczeństwo jest dla nich niezwykle istotne, ale jednocześnie zwracają uwagę, że oczekują usług raczej nastawionych na stwarzanie poczucia bezpieczeństwa (wizualna obecność pracowników). Chcą stworzyć miejsce, które będzie przez klientów rozpoznawane jako przyjazne i bezpieczne. Pracownicy ochrony powinni być więc raczej miłymi, eleganckimi osobami niekoniecznie z temperamentem policjanta Serpico. Obraz ten zaburzą incydenty, takie jak w Arkadii i Stalowej Woli. Ten trudny moment charakteryzuje się też tym, że prawdziwa rewolucja cyfrowa jest dopiero przed nami. Implementacja zaawansowanych algorytmów działania CCTV, narzędzi do odnotowywania i raportowania incydentów to ciągle jeszcze sfera planowania, a nie rzeczywistość.

Punktem odniesienia dla alternatywnej dla klasycznej ochrony koncepcji zorganizowania systemu bezpieczeństwa w galeriach i centrach handlowych może być tzw. Pokojowy Patrol i Patrol Medyczny podczas festiwalu Pol'and'Rock organizowanego przez Wielką Orkiestrę Świątecznej Pomocy, oczywiście z zachowaniem proporcji i uwzględnieniem specyfiki festiwalu. Traktując ten przykład jako inspirację, warto przeanalizować sposób i model działania Pokojowego Patrolu (klasyczny stewarding doskonale dostosowany do charakterystyki imprezy). Technologia, która została zaprojektowana na potrzeby WOŚP, pozwala utrzymywać i zarządzać precyzyjnie (również co do wykorzystania zasobów) ochroną wydarzenia. Możliwość natychmiastowego zlokalizowania pracownika – członka Patrolu Pokojowego i przesłania mu materiału (zdjęcia, mapy) – sprawia, że znacząco skraca się czas reakcji.

NAZWA CENTRUM HANDLOWEGO	SPECYFIKA
Manufaktura	W odrestaurowanych pofabrycznych wnętrzach jest 110 tys. m ² powierzchni najmu. Zlokalizowano tu muzea, kina, dyskoteki, ponad 250 butików i sklepów, kilkadziesiąt restauracji. Punktem centralnym jest ponad 3-hektarowy rynek pełniący funkcję otwartej przestrzeni publicznej. Łódzka galeria działa od 2006 r.
Arkadia	Działa w Warszawie od 2004 r. i dysponuje 105 tys. m ² powierzchni handlowej. Znajduje się w niej m.in. 230 sklepów i 15-salowe kino. W czerwcu 2016 r. ruszyła przebudowa galerii, która zakończyła się w 2017 r. Obiekt powiększono o 2 tys. m ² . W nowej części budynku powstało 8 restauracji. Największa z nich, z przeszkloną fasadą i tarasem, ma 1200 m ² . Na zewnątrz jest nowa fontanna oraz plac zabaw dla dzieci o powierzchni 2 tys. m ² .
Galeria Port Łódź	Otwarta w Łodzi w 2010 r. Powierzchnia najmu wynosi 103 tys. m ² . Znajduje się tu ponad 200 sklepów i punktów usługowych o zróżnicowanej ofercie. Ponad 33 tys. m ² powierzchni kompleksu zajmuje IKEA. Na zewnątrz obiektu jest strefa rekreacyjno-handlowa o powierzchni 10 tys. m ² z placem zabaw, sceną i zadrzewionym ogrodem.
Magnolia Park	Największe centrum handlowo-rozrywkowo-rekreacyjne na Dolnym Śląsku, zlokalizowane we Wrocławiu. Otwarte 25 października w 2007 r., w marcu 2015 zostało rozbudowane o kolejną część powierzchni handlowej. W efekcie łączna powierzchnia to 99 tys. m ² . W galerii jest 250 sklepów, kawiarni, restauracji i punktów usługowych. W części rozrywkowo-rekreacyjnej znajdują się kino i sala zabaw dla dzieci.
Posnania	Na 99 tys. m ² powierzchni ulokowano 220 butików, 40 kawiarni i restauracji oraz 40 sklepów średnio- i wielkopowierzchniowych. Poznańska galeria została oddana do użytku w 2016 r.
Bonarka City Center	Zostało otwarte w Krakowie w listopadzie 2009 r. Na 91 tys. m ² powierzchni handlowej znajduje się ok. 270 sklepów, 30 kawiarni i restauracji, 20-salowe kino.
Silesia City Center	To drugie duże centrum handlowe na Śląsku, które znajduje się w Katowicach. Na 86 tys. m ² mieści się 310 sklepów. W 2011 r. zostało rozbudowane o 20 tys. m ² . Działa od 2005 r.
Riviera Gdynia	Największe centrum handlowo-rozrywkowe na Pomorzu – 70 tys. m ² powierzchni najmu zostało otwarte pod koniec października 2013 r. W obiekcie ulokowano 250 sklepów, 30 restauracji i kawiarni, 42 sklepy średniej wielkości poniżej 2 tys. m ² i pięć sklepów wielkopowierzchniowych, w tym hipermarket.
Atrium Felicity	Galeria w Lublinie została uruchomiona w marcu 2014 r. Jej powierzchnia wynosi 75 tys. m ² , z czego największą część zajmuje 135 lokali handlowo-usługowych.

W tym przypadku struktura i poziom skomplikowania największych centrów handlowych w Polsce są znacznie większe niż w przypadku pola, na którym zbudowano tymczasowe miasteczko festiwalowe.

Największe centra handlowe w Polsce to ogromne struktury, skomplikowane architektonicznie i prześcigające się w atrakcjach mających przyciągać klientów. Każde ma swoją specyfikę i inne incydenty. Tak wielkie organizmy z intensywnym ruchem osób generują poważną liczbę różnego typu zdarzeń.

Przed kilkoma laty rozmawiałem z osobą odpowiedzialną za bezpieczeństwo HUB produkcyjnego na terenie Niemiec, dokąd codziennie do pracy przyjeżdżało ok. 96 tys. osób, wliczając podwykonawców. Zapytałem, z jakiego rodzaju incydentami bezpieczeństwa ma do czynienia w codziennej pracy. Odpowiedział zdecydowanie i bez większego namysłu, że w zasadzie z większością typowych dla miasta średniej wielkości. Nie inaczej jest w centrach handlowych. Poważne incydenty, np. ataki nożowników, bójki z użyciem niebezpiecznego narzędzia czy samobójstwa, to tylko najbardziej spektakularne zdarzenia występujące raz na wiele miesięcy czy wręcz lat. Drobnych incydentów jest czasami kilkadziesiąt dziennie.

Duży problem stwarza obecnie zachowanie młodzieży w centrach handlowych. Wybryki chuligańskie, wyzywające zachowanie, spożywanie alkoholu i substancji psychoaktywnych oraz wiele innych, problemy na parkingach, alarmy w systemie pożarowym czy drobne uszkodzenia – wszystko to musi być odnotowane i zaraportowane do dyrekcji centrum. Masę krytyczną obrazu zdarzeń z obszaru bezpieczeństwa stanowią właśnie te drobne z pozoru incydenty. Do tego dochodzi wpisywanie się ochrony w misję centrum handlowego, szczególnie po tak głębokim kryzysie, jakim był lockdown.

Charakter pracy pracowników ochrony powinien być przesunięty z modelu „ochronnego” na „usługowo-informacyjny”. Konsjerż-ratownik medyczny, który będzie potrafił zachować się podczas ogłoszenia ewakuacji, wydaje się odpowiednią na współczesne potrzeby. Koncepcja stewardów wyparła klasyczną ochronę z imprez masowych zarówno kulturalnych, jak i sportowych. Centra handlowe, z wymagającym i dynamicznie zmieniającym się klientem stają się kolejnym obszarem zmian. O ile w przypadku opisywanym w poprzednim artykule (a&s nr 5/2021) model stewardingu w przemyśle ma podnosić efektywność wszystkich służb działających w środowisku dużej dyscypliny, o tyle w obiektach handlowych dochodzi kluczowy dla tych miejsc aspekt wsparcia sprzedaży poprzez wykreowanie przyjaznej atmosfery. Dobrym punktem odniesienia mogą być członkowie Patrolu Pokojowego WOŚP.

Wraz z rozwojem technologii z zakresu security, ale i ppoż. w obiektach czy choćby zarządzania parkingami w centrum handlowym presja na redukcję ochrony fizycznej będzie się nasilała. Świetnie zorganizowane centrum monitoringu (integrujące dużą liczbę systemów) wspierające osoby w patrolowaniu pasażów, parkingów, punktów informacyjnych i stref załadunku, zbierające dane nt. zdarzeń mających miejsce w centrum handlowym da przewagę konkurencyjną firmom ochrony, które taki system stewardingu opracują i wdrożą.

Podsumowując, centra handlowe zdecydowanie nie potrzebują (jeszcze) eskomandosów w strukturach ochrony, ale stewardów na pierwszym froncie kontaktu z klientem, wspieranych technologią podnoszącą efektywność ich pracy oraz dostarczających dane zarządcze dyrekcji centrum. ●



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. Obecnie związany z Black Onion Resilience Community.

Sieci handlowe

dostosowane do potrzeb klienta



Od momentu pojawienia się w połowie XX wieku centra handlowe nieustannie zmieniały się, aby nadążyć za nawykami i potrzebami konsumentów. Dawniej skupiały kilka sklepów wielobranżowych, obecnie są to już miejsca kojarzone z pracą, stylem życia, a także rozrywką. Centra handlowe łączące handel detaliczny, restauracje, centra rozrywki, miejsca, gdzie można spędzać czas, a także powierzchnie biurowe stały się powszechne.

Zmieniające się preferencje zakupowe i rosnąca popularność e-commerce przyczyniły się do konieczności wprowadzenia nowych pomysłów, w celu sprostania oczekiwaniom klienta. A ten coraz bardziej ceni swój czas. Podczas wizyty w centrum handlowym oczekuje spersonalizowanej oferty zaspokajającej jego potrzeby, a także komfortu przebywania. Katalizatorem zmian jest też troska o zdrowie i bezpieczeństwo. Od centrum handlowego wymaga się teraz, by było miejscem bezpiecznym i przyjaznym, które dostosowuje swoje usługi i podejmuje działania, kierując się opiniami klientów. Obie kwestie są dla klientów priorytetowe i można je zapewnić na różne, ale powiązane ze sobą sposoby.

Z punktu widzenia bezpieczeństwa fizycznego kluczowym elementem jest monitoring incydentów. Centra handlowe są miejscami, gdzie często dochodzi do kradzieży, aktów wandalizmu lub konfliktów. Pracownicy ochrony muszą wiedzieć o wszelkich zajściach w każdym zakątku. Interwencja na wczesnym etapie jest bardzo cenna, ponieważ personel może zapobiec eskalacji incydentu. Dozór wizyjny z takimi funkcjami, jak inteligentna analiza dźwięku może wspierać pracowników w wykrywaniu niepożądanych zachowań. Przykładowo, analiza dźwięków może być wykorzystywana do monitorowania odgłosów agresji lub tłuczonego szkła. To się doskonale sprawdza w praktyce. Centrum Le Piazze w Bo-

lonii musiało zmodernizować istniejący system monitoringu wizyjnego, aby poprawić skuteczność i lepiej wspierać personel ochrony. Wzbogacając monitoring o sieciowe głośniki, system pasywny przekształcono w instrument proaktywny, który może nadawać wiadomości na żywo lub wcześniej nagrane. Zapobieganie niepożądanym zdarzeniom i zarządzanie awaryjnymi sytuacjami stało się dzięki temu bardziej skuteczne. Przyczyniło się również do wyraźnego obniżenia kosztów, zarówno dzięki zmniejszeniu liczby fałszywych alarmów, jak i wyeliminowaniu patroli na terenie obiektu.

W odniesieniu do bezpieczeństwa zdrowotnego właściciele centrów handlowych są zobowiązani do zapewnienia klientom także środków zachowania higieny i dystansu społecznego. Liczenie osób odwiedzających, by móc kontrolować wskaźnik zajętości, jest niezbędne ze względu na wymagania BHP. Ta sama technologia może być również wykorzystywana przed obszarami, w których klienci są narażeni na bliski kontakt, np. w strefach odpoczynku w celu analizowania natężenia ruchu i automatycznego powiadamiania personelu sprząającego po określonej liczbie wizyt gości.

Rozwiązania umożliwiające liczenie osób doskonale sprawdzają się również przy podejmowaniu decyzji marketingowych oraz operacyjnych. Pozwalają uzyskać precyzyjne informacje dotyczące liczby klientów wchodzących do centrum handlowego i wychodzących z niego. Ruch osób oraz miejsca, gdzie zatrzymują się kupujący, stanowią również źródło przydatnej wiedzy i wskaźników wydajności dla kierownictwa centrów handlowych i najemców.

Centra handlowe mogą stosować strefowe liczenie osób pozwalające zrozumieć czynniki przyciągające klienta czy wybrać najbardziej atrakcyjnych najemców. Analiza demograficzna klientów może posłużyć do zmierzenia sukcesu konkretnej kampanii i informowania o planowaniu kolejnej. W ten sposób można poprawić wydajność sprzedaży centrum handlowego i rozwijać działalność.

Tworzenie spójnego i spersonalizowanego doświadczenia zaczyna się od zrozumienia potrzeb klienta – poznania jego nawyków zakupowych, ulubionych miejsc czy sprawdzenia, ile czasu poświęca na wizytę w centrum handlowym. Warto też mieć świadomość, jakie elementy stanowią utrudnienie czy niewygodę dla klientów. Przykładowo miejscem, które często doprowadza do frustracji, są parkingi. Tu w szybkim znale-

zieniu wolnego miejsca parkingowego może pomóc technologia. Po przyjeździe klienta kamery z zaimplementowaną analityką wizji monitorujące parking mogą dostarczyć kierowcy informację o dostępnych miejscach za pośrednictwem aplikacji mobilnej lub *digital signage*. Technologia może także wesprzeć kierownicę opuszczającego centrum, pomagając w odszukaniu zaparkowanego auta. Dzięki temu zarządzający mogą mieć pewność, że dostępność istotnych usług poprawia klientowi komfort zakupów.

Spróbujmy wybiec nieco w przyszłość. Wyobraźmy sobie sklep, gdzie drzwi otwierają się automatycznie po zeskanowaniu twojego osobistego kodu QR. W sklepie wita cię nagrane wcześniej powitanie, a w tle słychać muzykę. Z głośnika dochodzą informacje dotyczące najnowszych ofert dopasowanych do twoich potrzeb. Wizja cyfrowego sklepu nie jest już odległym marzeniem. Zwłaszcza od wybuchu pandemii koronawirusa cyfryzacja w sektorze detalicznym wyraźnie nabrała tempa, rośnie także akceptacja autonomicznych sklepów przez konsumentów.

Poznaliśmy już supermarkety z kasami samoobsługowymi, które z pewnością się sprawdziły. Jednak trend ten idzie dalej, rozwija się, ewoluując w kierunku supermarketów bez kas i całkowicie bez personelu. Wszystko wskazuje na to, że powoli, aczkolwiek nieustannie trend w kierunku zautomatyzowanych supermarketów będzie rozwijał się także po pandemii.

W Stanach Zjednoczonych Amazon od dawna wykorzystuje rozwiązanie Amazon Go, które umożliwia klientom robienie zakupów zgodnie z zasadą *grab-and-go* (chwyc i idź). Nie ma tu konieczności korzystania z kas, jest to w pełni zautomatyzowane rozwiązanie wykorzystujące kody QR (do zalogowania się i wejścia do sklepu) oraz kamery. Ten zaawansowany model sklepów powoli wkracza również do Europy.

W niektórych europejskich krajach, np. w Niemczech, w pełni zautomatyzowane minisupermarkety próbują znaleźć swoje miejsce w centrach miast. Jednym z przykładów jest „teo”, czyli cyfrowy samoobsługowy sklep sieci supermarketów Tegut w Fuldzie. Klienci mają łatwy dostęp do sklepu dzięki aplikacji zainstalowanej w smartfonie, skanują produkty prosto z półki i dokonują zapłaty w aplikacji lub za pomocą terminala. Wszystko jest dostępne 24 godziny na dobę. 



AXIS COMMUNICATIONS POLAND

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



Oferta Hikvision na pandemiczne czasy

Pandemia COVID-19 nie ustępuje. Sieci handlowe nadal muszą mierzyć się z problemami związanymi z utrzymującymi się obostrzeniami. Sytuacja epidemiczna niesie wiele wyzwań natury safety i security.



Paweł Sobociński

Istotnym wymogiem jest zapewnienie bezpieczeństwa zdrowotnego, nadal bowiem obowiązują obostrzenia sanitarne dotyczące zgromadzeń w miejscach publicznych. Coraz większa liczba klientów w placówkach handlowych, społeczne rozluźnienie w kontekście noszenia maseczek ochronnych czy nieprzestrzegania odpowiedniego dystansu społecznego sprzyjają wzrostowi zakażeń. W tej sytuacji na menedżerach placówek handlowych nadal ciąży odpowiedzialność za klientów i pracowników nie tylko w zakresie standardowej „prewencji wizyjnej”.

W odpowiedzi na te wyzwania Hikvision ma do zaproponowania różne modele kamer oraz terminale termowizyjne, które wykonują pomiary temperatury osób w przestrzeni publicznej w sposób bezdotykowy, a także systemy IP wspierane analityką. Systemy termowizyjne z zaawansowanymi algorytmami analizy obrazu są od początku pandemii dobrze znane naszym klientom ze względu na jakość analizy oraz korzyści płynące z ich użytkowania. Oferta jest odpowiedzią na ich potrzeby związane z zagrożeniami pandemicznymi oraz kolejnymi, będącymi efektem zmian obserwowanych od początku epidemii.



Inny wątek. Najnowsze dane pokazują, iż wzrost kradzieży w obiektach handlowych w porównaniu z rokiem ubiegłym wynosi 20%. Policja podaje, że jednym z powodów jest zuchwałość złodziei spowodowana noszeniem maseczek, dzięki którym czują się nierozpoznawalni. Trudniejszym zadaniem staje się także zidentyfikowanie takiej osoby, która dokonała kradzieży, na podstawie zarejestrowanego materiału.

Rozwiązaniem tych problemów jest zaimplementowanie technologii analizy obrazu w urządzeniach lokalnych systemu dozoru: kamerach i rejestratorach lub na serwerach. Algorytmy pozwalają śledzić osoby podejrzewane lub dokonujące kradzieży, bazując na rozpoznawaniu fragmentów twarzy czy analizie innych charakterystycznych cech. Każde pojawienie się w kadrze poszukiwanej lub podejrzanej osoby na podstawie tych analiz może zostać odpowiednio zakomunikowane.

Kolejnymi funkcjami prewencyjnymi wykorzystującymi analizę obrazu (jako algorytmy oddzielne lub uzupełniające) są modelowanie sylwetki oraz rozpoznawanie/śledzenie towarów. Pierwsza pozwala na analizę ruchów klienta i jego zachowania. Mogą być wykrywane sytuacje, w których dana osoba próbuje schować produkt do kieszeni, torby czy plecaka, a informacja o tym może być wyświetlana na ekranie monitora pracownika ochrony.

Rozpoznawanie i śledzenie towarów na podstawie analizy regatów sklepowych podzielonych na strefy jest uzupełnieniem pierwszej funkcji. W ten sposób można zidentyfikować produkty pobierane z konkretnych miejsc istotnych dla właściciela placówki handlowej. W rozszerzonej formie pozwala na prześledzenie drogi produktu, jaką przebywa od momentu wzięcia z półki po dokonanie transakcji kasowej, a w skrajnym przypadku z uwzględnieniem identyfikacji klienta. W przypadku zerwania tego łańcucha

operator otrzymuje odpowiedni komunikat. Wymiana danych między systemem wizyjnym a POS ma tutaj kluczowe znaczenie. Sam ruch w konkretnych strefach oraz manipulacja monitorowanymi produktami staje się dla użytkownika systemu sygnałem do wyłączenia uwagi.

Podsumowując, dla obiektów handlowych nasza firma może zaprojektować kompleksowe rozwiązanie, które dostarcza informacje dotyczące temperatury osób przebywających w pomieszczeniach, zachowania odpowiedniego dystansu społecznego, noszenia maseczek ochronnych w miejscu publicznym (wraz z alarmem o ich braku), analizy twarzy w masce ochronnej lub bez niej oraz wsparcia ochrony produktowej. Całość jest nadzorowana z poziomu punktu centralnego w postaci platformy zarządzającej sterującej działaniem wszystkich urządzeń podłączonych do systemu. Rozwiązanie oszczędza czas potrzebny na wyegzekwowanie przez osoby kontrolujące odpowiednich działań. Dodatkowo tego typu technologia może pracować na szeroką skalę w systemie rozproszonym. Operator ma za zadanie jedynie reagować na komunikaty dostarczane przez platformę zarządzającą. 📍

HIKVISION POLAND

ul. Żwirki i Wigury 16B
02-092 Warszawa
info.pl@hikvision.com
<https://www.hikvision.com/europe/>





Głos branży

JAK BRANŻA SECURITY MOŻE

POMÓC W ZAPEWNIENIU

BEZPIECZEŃSTWA

W OBIEKTACH HANDLOWYCH

W DOBIE PANDEMII?

GŁOS ZABIERAJĄ

PRZEDSTAWICIELE RÓŻNYCH

SEKTORÓW GOSPODARKI.



Krzysztof Poznański

Polska Rada Centrów Handlowych

Systemy zabezpieczeń z walce z pandemią

Podstawowym zadaniem systemów zabezpieczeń technicznych, takich jak kontrola dostępu, CCTV czy systemy włamanio-we i pożarowe, jest zapewnienie bezpieczeństwa fizycznego w obiektach, również w centrach handlowych. Systemy te sprawdziły się także w czasie pandemii, wspierając ich zarządców we wdrażaniu i egzekwowaniu zaleceń sanitarnych.

Szczególną rolę odgrywają tu systemy telewizji dozorowej, popularnie nazywane systemami CCTV (*closed-circuit television*). W dobie pandemii umożliwiają one zdalną kontrolę przestrzegania przez klientów zaleceń sanitarnych, takich jak noszenie maseczek czy zachowanie dystansu. Operatorzy systemów zabezpieczeń w centrach handlowych wykorzystują je do detekcji osób niestosujących się do obowiązujących zaleceń lub do kontroli miejsc, w których dochodzi do nadmiernego gromadzenia się klientów. Pozwala to na podjęcie odpowiedniej interwencji.

Systemy liczące klientów oparte na kamerach oraz systemach kontroli dostępu pozwalają na monitorowanie i zarządzanie ruchem w centrach handlowych i sklepach, nie dopuszczając do nadmiernego gromadzenia się ludzi lub przekraczania norm liczby kupujących na powierzchni sklepów.

Natomiast nie znalazły zastosowania systemy detekcji temperatury w postaci automatycznych bramek do jej pomiaru, kamer termowizyjnych lub ręcznych oraz bezprzewodowe skanery temperatury, których użycie było rozważane w szczycie pandemii przez niektóre centra handlowe lub sklepy. Powodem była zbyt wysoka cena w dwóch pierwszych przypadkach oraz brak regulacji prawnych umożliwiających reakcję ochrony obiektu w przypadku identyfikacji klientów z podwyższoną temperaturą. Security menedżerowie w centrach handlowych są świadomi funkcjonalności i dostępności technicznych systemów zabezpieczeń, wykorzystują je w ograniczonym zakresie w czasie pandemii. Problemem nie są systemy techniczne i ich wykorzystanie, lecz przepisy prawa, które nie pozwalają na ich zastosowanie lub na podjęcie reakcji w razie stwierdzenia naruszeń regulacji sanitarnych.



Tomasz Grzelak

Rossmann

Nowe zadania przed branżą ochrony

Minęły blisko dwa lata od wybuchu pandemii. Był to okres zmian, na które świat nie do końca był przygotowany i których się nie spodziewał. Swoim zakresem objęły praktycznie każdy obszar gospodarki, a skutki zapewne będą jeszcze długo odczuwalne. Zmiany dotknęły również branżę handlową – zamknięcie skle-

pów, a następnie wprowadzenie wielu ograniczeń z powodu pandemii miało wpływ na wiele przedsiębiorstw. Ich skutki po części dotyczą również branży ochrony, przed którą pojawiło się wiele nowych wyzwań. Z perspektywy czasu moge śmiało powiedzieć, iż udało nam się im sprostać. W naszej branży najważniejsze jest bezpieczeństwo zarówno klientów, jak i pracowników. Wraz z wybuchem pandemii sytuacja w branży ochrony uległa zmianie, wiele firm, szukając oszczędności, ograniczyło lub nawet zrezygnowało ze stałej ochrony, w wielu firmach pracowników oddelegowano do innych zadań, co nie pomagało w wykonywaniu podstawowych obowiązków. Na szczęście zarówno pracownicy ochrony, jak i ich kierownicy wykazali się dużą elastycznością i zaangażowaniem, dzięki czemu uniknęliśmy wielu sytuacji kryzysowych. Należą im się za to duże słowa uznania.

Swoją cegiełkę dołożyły również firmy z branży security, które bardzo szybko zaproponowały nowe rozwiązania ułatwiające pracę i ograniczające rozprzestrzenianie się wirusa. Systemy liczące osoby w obiektach lub mierzące temperaturę zostaną z nami na długo. Część z rozwiązań nawet zastępuje już pracowników ochrony, np. automatyczne otwieranie szlabanów dla wcześniej zapisanych w bazie numerów rejestracyjnych aut zamiast osoby robiącej to ręcznie czy zdalne recepcje w budynkach biurowych stają się coraz bardziej powszechne. Nie oznacza to oczywiście, że technologia zastąpi człowieka, mimo dynamicznego rozwoju sztucznej inteligencji i uczenia maszynowego nie są to jeszcze idealnie dopracowane rozwiązania.

Moim zdaniem dalszy rozwój monitoringu wizyjnego, analityka obrazu, sztuczna inteligencja na urządzeniach brzegowych, jak kamery czy urządzenia rejestrujące, to droga, którą powinna podążać branża. Dodatkowo jeszcze większa integracja wszystkich systemów bezpieczeństwa znajdujących się w obiekcie (systemy sygnalizacji włamania i napadu, monitoringu wizyjnego, kontroli dostępu, systemy sygnalizacji pożarowej), wraz z jednoczesnym odpowiednim przeszkoleniem pracowników ochrony to idealna droga i zadania, z którymi będziemy musieli się mierzyć.



Tomasz Kozłowski

Grupa Impel

Wyzwania stojące przed firmami ochrony

W obecnych trudnych czasach jest kilka istotnych wyzwań związanych z zapewnianiem bezpieczeństwa w obiektach handlowych. Nadal priorytetem jest przestrzeganie obostrzeń w związku z przeciwdziałaniem rozprzestrzeniania się wirusa SARS-CoV-2. Przez 1,5 roku trwania pandemii COVID-19 wypracowaliśmy i wdrożyliśmy procedury, modyfikując je zgodnie z bieżącymi wytycznymi rządowymi. Niestety część klientów obiektów handlowych odmawia podporządkowania się ogólnie obowiązującym zasadom, np. noszeniu masek ochronnych w pomieszczeniach zamkniętych. Nasi pracownicy bardzo często mają do czynienia z atakami agresji, różnymi prowokacjami ze strony tych osób. To poważny i coraz bardziej powszechny problem.

Kolejnym zadaniem jest zmiana w organizacji pracy związana z otwieraniem w niedziale części placówek przez niektóre sieci handlowe. Wymaga to od nas nie tylko zmian w „grafikach” służb, ale także dodatkowej rekrutacji z powodu zwiększenia liczby godzin pracy. To może być sporym wyzwaniem w końcu roku ze względu na zbliżający się okres świąteczny. Pozy-skanie pracowników na rynku pracy to nadal ogromny problem. Rosną też oczekiwania pracowników ochrony zatrudnionych w obiektach handlowych. Chcą być traktowani na równi z personelem sklepów, otrzymywać podobne gratyfikacje, dodatkowe wynagrodzenie, uczestniczyć w tych samych systemach motywacyjnych. Tymczasem warunki finansowe kontraktów, szczególnie w branży handlowej, nie zawsze pozwalają na ponoszenie dodatkowych kosztów przez dostawców usług ochrony.

Cała branża już w kolejnym z rzędu roku rozpoczęła proces renegotiacji kontraktów, co spowodowane jest inflacją, wzrostem wysokości najniższego ustawowego wynagrodzenia i kosztów prowadzenia przedsiębiorstwa m.in. w efekcie podwyżek cen paliwa i energii elektrycznej. Wierzymy, że podobnie jak w ubiegłych latach proces ten zakończy się pomyślnie i bez zachwiania ciągłości w realizacji usług dla naszych klientów.





Robert Kujawa

Retail Security Academy

Zapobieganie, a nie minimalizacja strat

Pandemia spowodowała w branży retail istotny spadek dochodów w wyniku lockdownów i mniejszej liczby klientów w sklepach. Dla security menedżerów nastały trudne czasy. Pomimo pojawiających się na rynku systemów monitoringu z inteligentną analizą obrazu w sytuacji dużej niepewności dochodów rzadkością jest inwestowanie właścicieli sklepów w takie rozwiązania. Pracownicy ochrony w znacznym stopniu zmuszeni są korzystać z tych samych systemów co przed pandemią. Nawet w dużych sklepach sieciowych klientów robiących zakupy na terenie placówki liczy pracownik, a nie inteligentny system monitorujący. Zaangażowanie pracowników ochrony i sklepów w kontrolę przestrzegania obostrzeń wynikających z COVID-19, a także większa anonimowość klientów spowodowana noszeniem maseczek wpłynęły na wzrost kradzieży sklepowych. Potwierdzają to dane Komendy Głównej Policji, z których wynika, że w trzech kwartałach br. stwierdzono o ponad 3 tys. więcej przestępstw niż w roku ubiegłym. Badania opublikowane w 2021 w RETAIL SECURITY SURVEY także wskazują, że złodzieje sklepowi są coraz bardziej agresywni i nie unikają przemocy. Sytuacja ta – zdaniem licznych przedstawicieli branży – będzie się pogłębiać, a liczba kradzieży rosnąć. Odnosząc do rynku retail tacińskie przysłowie *Si vis pacem, para bellum*, można skonstatować: Jeśli chcesz mieć zyski, ograniczaj straty. Takie podejście daje szansę na ograniczenie utraconych korzyści i inwestycję środków finansowych w najnowsze rozwiązania. Jak jednak

ograniczać straty przy zmniejszających się nakładach na systemy antykradzieżowe i usługi ochrony? Moim zdaniem konieczna jest ścisła współpraca pomiędzy sprzedawcami i security menedżerami. Nawet najlepsze systemy przeciwdziałające kradzieżom tylko sygnalizują usiłowanie kradzieży lub dostarczają materiały dla celów procesowych. Personel mający bezpośredni kontakt z klientem powinien podlegać systematycznym szkoleniom teoretycznym i praktycznym, których celem będzie ZAPOBIEGANIE, a nie tylko minimalizacja strat po zdarzeniu. Menedżerowie bezpieczeństwa i sprzedawcy wsparci dostępnymi systemami przeciwdziałającymi kradzieżom powinni tworzyć jednolitą strukturę zapobiegania stratom, współdziałać, a nie – jak wskazuje dotychczasowa praktyka wielu organizacji – tworzyć dwa niezależne organizmy. Najlepszym systemem antykradzieżowym są lojalni i wyszkoleni pracownicy.



Ewelina Zalewska

Super-Pharm

Najważniejsze jest bezpieczeństwo

O pandemii COVID-19 słyszymy codziennie, w sklepie, na ulicy, we wszystkich mediach. Po roku obostrzeń każdy z nas nauczył się pewnych zasad, które towarzyszą nam na co dzień, np. dezynfekcja rąk, noszenie maseczek w sklepach i galeriach handlowych czy w transporcie publicznym. W Super-Pharm od początku zagrożenia epidemiologicznego wszystkie placówki wprowadziły prewencyjne procedury dbające o bezpieczeństwo oraz ochronę zdrowia i życia klientów oraz pracowników. W dalszym ciągu stosujemy się do zasad bezpieczeństwa, przestrzegając zaleceń i wytycznych Ministerstwa Zdrowia. Firma Super-

-Pharm zachęca też klientów drogerii i pacjentów aptek do robienia zakupów w bezpieczniejszej formie online, bez wychodzenia z domu. Rola działu Loss Prevention nie ogranicza się tylko do dbania o mienie firmy, ale też o bezpieczeństwo naszych klientów i pracowników. Czuwamy nad poprawnością działania wszystkich systemów zabezpieczeń, takich jak telewizja dozorowa, systemy alarmowe i przeciwpożarowe. Prętnie rozbudowujemy centralny monitoring wizyjny, dzięki któremu mamy jeszcze lepszy przepływ informacji o pojawiających się zagrożeniach. Wprowadzamy nowości zwiększające wydajność i efektywność naszych systemów. Duży nacisk kładziemy na szkolenia pracowników. Uczymy każdego, jak właściwie zachować się w każdej sytuacji. Reagujemy i rozwiązujemy na bieżąco napotkane problemy. Upraszczamy procesy oraz tworzymy jasne procedury. Zdajemy sobie sprawę, jak wielką rolę odgrywają przeszkoleni pracownicy, którzy codziennie pracują w sklepach. Wyszczególniamy kadra Security District Managerów każdego dnia czuwając nad uzupełnianiem wiedzy naszych pracowników oraz służby ochrony.



Bogumił Szymanek

Axis Communications

Axis wspiera handel detaliczny

Przedsiębiorstwa działające w branży handlowej mają różne potrzeby i wymagania ze względu na mnogość rodzajów prowadzonej działalności i jej skali. Sztuką jest zrozumienie specyfiki i potrzeb konkretnego klienta i dostarczenie rozwiązań wpisujących się w strategię rozwoju oraz specyfikę pracy firmy. Często systemy zabezpieczeń skupiają się na zapewnieniu ogólnego bezpieczeństwa – wtedy kluczowa jest niezawodność i wysoka jakość materiału wideo, którą dostarczają m.in. dyskretne kamery kopułkowe. Firmy z branży retail zmagają się również z problemami dużych strat, dlatego priorytetem jest ich minimalizowanie poprzez wcześnie wykrywanie podejrzanych zachowań, odstraszanie potencjalnych złodziei i szybkie wykrywanie sprawców. Jest to również branża mocno zorientowana na efektywność, więc konieczne jest wdrażanie rozwiązań pozwalających na optymalizację pracy z klientem, zarządzanie magazynem czy pomiar efek-

tywności kampanii marketingowych. Wiele spośród wymienionych potrzeb mogą zaspokoić zintegrowane rozwiązania Axis. Systemy dozoru wizyjnego stanowią podstawę oferty firmy, a dobrą praktyką jest wykorzystanie pełni możliwości kamer, stosując rekomendowane oprogramowanie do zarządzania materiałem wizyjnym Axis Camera Station, łatwe i intuicyjne w obsłudze. Wyszukiwanie nagrań wspierane przez funkcję Smart Search pozwala na szybkie odszukanie nagrań przedstawiających obiekt, np. w zdefiniowanym kolorze – pojazd lub osobę w ubraniu o tym kolorze. W ramach jednego czytelnego interfejsu użytkownika Axis Camera Station można również obsłużyć system kontroli dostępu Axis Secure Entry oparty na kontrolerach Axis A1601. Firma oferuje też dyskretne kamery nasobne Body Worn Mini Cube Sensor dla służb ochrony, np. placówek bankowych ulokowanych w centrum handlowym czy miejsc, które wymagają nagrywania zdarzeń (z perspektywy pracownika). Kamery zainstalowane nad wejściami mogą liczyć osoby wchodzące do sklepu, a właściciel otrzymuje rzetelne informacje nt. odwiedzin czy liczby osób na terenie obiektu. Zintegrowanie rozwiązań audio Axis nie tylko umila czas spędzany w obiekcie, ale również pozwala nadawać treści marketingowe, specjalne komunikaty czy powiadomienia dla pracowników. Ciekawe jest powiązanie analizy obrazu z systemem audio, np. po wykryciu zbyt długiej kolejki wezwanie dodatkowego pracownika obsługi albo reakcja audio na zbyt długie przebywanie osoby w danej strefie. Dzięki temu nie tylko redukuje się potencjalne straty, ale i poprawia wrażenia zakupowe klientów. Wyjaśnianie zdarzeń i reklamacji usprawnia możliwość wyszukiwania materiałów wideo po numerach dokumentów z punktów obsługi sprzedaży czy magazynu. Kamery Axis to wydajne komputery pracujące na krawędzi sieci. Coraz więcej kamer Axis otrzymuje wsparcie dla algorytmów sztucznej inteligencji i głębokiego uczenia. Axis wprowadza te zaawansowane technologie w wielu produktach – również dla handlu detalicznego.



Marcin Walczuk

BCS

Jak wykorzystać systemy po pandemii

W branży handlu detalicznego od początku pandemii musiały zająć i zaszczyt dość duże zmiany. Wynikało to z wprowadzanych kolejnych obostrzeń stosowanych w celu powstrzymania rozprzestrzeniania się wirusa czy z troski o bezpieczeństwo kupujących. Konieczność zakładania maseczek ochronnych, przestrzeganie limitu osób w obiektach handlowych i zachowywanie dystansu społecznego miały wydatnie pomóc w realizacji tych celów. Z pomocą w przestrzeganiu wspomnianych ograniczeń przyszła technika i funkcje analizy obrazu dostępne w systemach monitoringu wizyjnego. Część z takich systemów działających w obiektach handlowych wymagała jedynie drobnych usprawnień, takich jak aktualizacja oprogramowania wspierającego funkcje analityczne czy dołożenie kamer mających spełniać określone zadanie. W innych przypadkach trzeba było budować system od podstaw, co oczywiście wiązało się koniecznością poniesienia dodatkowych kosztów.

Mimo ograniczenia części obostrzeń nie rezygnujemy na razie z dodatkowych funkcji urządzeń dozoru, głównie dlatego że nie uporaliśmy się jeszcze z koronawirusem. Nie wiadomo, ile kolejnych jego fal jeszcze przed nami i czy nie przyniosą one kolejnych ograniczeń. Co jednak w sytuacji, kiedy będziemy mogli już o tym wszystkim zapomnieć, a urządzenia przestaną pełnić funkcje, do których pierwotnie je zamontowano? Kamery, których zadaniem było rozpoznawanie, czy klient wchodzi do sklepu ma na twarzy maseczkę, można wykorzystać w monitorowaniu/identyfikowaniu klientów, tworząc ew. listę osób niepożądanych/podejrzanych o kradzież. Kamery można też przenieść i wykorzystać do monitorowania innej części sklepu. Z kolei kamery przeznaczone teraz do liczenia osób wchodzących do obiektu handlowego w celu monitorowania dopuszczalnej zajętości przestrzeni można będzie wykorzystać jako narzędzie analityki biznesowej do określania liczby klientów, którzy dane miejsce odwiedzają. Systemy tworzone z myślą o naszym bezpieczeństwie w trakcie pandemii po jej

zakończeniu nie muszą okazać się bezużyteczne. Wystarczy jedynie znaleźć dla nich nowe przydatne zastosowanie. W jednym przypadku będzie to wykorzystanie używanych do tej pory funkcji w nowy sposób, w innym z pomocą może przyjść producent urządzeń, proponując aktualizację oprogramowania, dzięki której urządzenie zyska nowe funkcje odpowiednie do potrzeb klienta.



Paweł Sobociński

Hikvision

Potencjał nowych technologii

Pandemia oraz związane z nią obostrzenia, które odcisnęły piętno na rynku handlu detalicznego, stały się swojego rodzaju czynnikiem mobilizującym rynek do szybszych przemian w kontekście biznesowym (rozwój e-commerce oraz omnichannel), przy dużym nacisku na rozwój inwestycji w nowe technologie. Najbardziej widocznymi zmianami w obiektach handlowych są wzmoczone inwestycje w zaawansowane systemy liczące, pomiaru temperatury, detekcji maseczek, systemy dezynfekcyjne lub dekontaminacyjne.

Podane przykłady to tak naprawdę tylko wierzchołek góry lodowej nadchodzących dużych zmian związanych z automatyzacją procesów zachodzących w przestrzeni sklepowej. Poza tym, czego już doświadczaliśmy w poprzednich latach w postaci testowych rozwiązań lub fragmentaryzacji technologii, obecnie wraz z partnerami technologicznymi i klientami końcowymi dostrzegamy wielki potencjał w zastosowaniach rozbudowanej analizy obrazu, w tym wspieranej sztuczną inteligencją AI czy technologii IoT i Big Data. Ich efektem są pierwsze w pełni autonomiczne spożywcze sklepy samoobsługowe. Tego typu rozwiązania świadczą o skuteczności rozbudowanych systemów wizyjnych.

Kolejnym naturalnym etapem przemian staje się przeniesienie tych technologii do środowiska innych, mniejszych lub większych obiektów handlowych, w formie pełnej lub częściowej jako wsparcie w konkretnych strefach poddawanych analizie/ochronie. Skalowalność to również bardzo istotny argument omawianych rozwiązań, ponieważ można je stopniowo adaptować do coraz większych obiektów. Potencjał takich rozwiązań w przestrzeni handlowych to: możliwość uruchomienia placówek handlowych całodobowych, ➔

W trudno dostępnych miejscach, przy ograniczeniu wymagań pod względem obsługi (brak lokalnych pracowników), szybkość zakupów (ograniczenie kolejek, gdyż proces płatności jest zautomatyzowany). W obecnych czasach to rozwiązanie zapewnia także bezpieczeństwo sanitarne (łatwa możliwość ograniczenia liczby osób w placówce). Podsumowując, potencjał drzemie w nowych technologiach i obecnym pędzie do automatyzacji procesów, ograniczania kosztów i maksymalizacji zysków.



Jakub Sobek

Linc Polska

Wyższy poziom bezpieczeństwa w handlu

Odnosząc się do bezpieczeństwa w handlu detalicznym, pierwsze na myśl przychodzi bezpieczeństwo w zakresie klasycznych kradzieży sklepowych lub wewnętrznych dokonywanych przez pracowników. Oprócz detekcji takich zdarzeń ważne jest też wspieranie działań marketingowych/biznesowych opartych na danych, wydajności procesów, optymalizacji kolejek oraz obsługi. Zwrócenie uwagi na poprawę jakości tych czynności może zwiększyć dzienną sprzedaż i zmniejszyć potencjalne straty. Technologia wideo może także pomóc sprostać różnym wyzwaniom pandemii, przed którymi wszyscy stoimy. Dzięki zintegrowanej analizie elastyczne i skalowalne systemy wideo mogą być wykorzystywane do wykrywania masek oraz dystansu społecznego. Są także pomocne w zliczaniu osób przebywających w danym sklepie. Ostatni czas pokazał, jak istotna jest łatwa zmiana konfiguracji oraz zastosowań systemów monitoringu wizyjnego. Handel detaliczny jest jednym z największych sektorów, w których technologia wideo może zapewnić bardzo potrzebne wsparcie. Zewnętrzni złodzieje sklepowi stanowią dwie trzecie przypadków kradzieży, natomiast pracownicy i dostawcy pozostają jedną trzecią. To pokazuje, że kamery nie powinny swoim zasięgiem omijać żadnych istotnych obszarów monitorowanego obiektu. Wytypowanie newralgicznych przestrzeni powinno zostać poprzedzone wcześniejszą analizą ryzyka. Obecnie kamery mogą również skutecznie wspierać pracowników ochrony w detekcji nietypowych zdarzeń, np. pozostawienie torby, agresywne zachowania lub upadek osoby. W ten sposób przestrzeń sklepową może być naprawdę bezpiecznym miej-

scem. Warto jednak pamiętać, aby instalowany system był dyskretny. To, czy kamera jest duża i dobrze widoczna, czy mała – nie odstraszy potencjalnego złodzieja. Dyskretny system sprawia, że klienci czują się w sklepie bardziej komfortowo. Nie dajmy się jednak porwać przedświadczeniom szaleństwu zakupowemu, czego Państwu i sobie życzę.



Piotr Rodak

Schrack Seconet

Przyszłość przed zdalnym świadczeniem usług serwisowych

Pandemia koronawirusa w istotny sposób zmieniła sposób funkcjonowania wielu firm w Polsce. Sytuacja niejako wymusiła i przyspieszyła zmiany technologiczne, które ułatwiły przystosowanie się do nowej trudnej rzeczywistości. Innowacje nie omiły również branży systemów sygnalizacji pożarowej. Konieczność ograniczenia bliskiego kontaktu osobistego (tzw. dystans społeczny) czy dostępu do wielu obiektów (pozamykanie kina, siłownię, restaurację) spowodowała, że firmy zaczęły interesować się rozwiązaniami i systemami, które umożliwiłyby ograniczenie do niezbędnego minimum fizycznej obecności swojego personelu w obiektach klienta. Schrack Seconet od wielu lat oferuje systemy, które – dzięki narzędziom zdalnego dostępu – umożliwiają wykonywanie niektórych czynności serwisowych lub diagnostycznych w sposób bezpieczny, bez konieczności fizycznego udawania się na teren obiektu. Takie podejście pozwala obniżyć koszty serwisu czy skrócić czas reakcji w przypadku zgłoszeń serwisowych przy jednoczesnym zachowaniu wysokiego poziomu bezpieczeństwa samej instalacji. Wychodząc naprzeciw oczekiwaniom instalatorów, Schrack Seconet wprowadza obecnie do oferty kolejne rozwiązania, które rozwijają tę kategorię produktów. Dostęp do wszystkich instalacji w trybie online, narzędzia autodiagnostyczne, które w czasie rzeczywistym analizują i weryfikują konfigurację, rozbudowane narzędzie zarządzania i planowania serwisów czy wsparcie przy generowaniu protokołów serwisowych – wszystko to skutecznie odciąża firmy instalatorskie, pozwalając na dalsze ograniczenie fizycznej obecności w obsługiwanych obiektach z zachowaniem wysokiego poziomu bezpieczeństwa.



Anna Piaskowska

Securitas Polska

Rola firm ochrony w obiektach handlowych

Skala zadań realizowanych przez pracowników ochrony w obiektach handlowych jest dzisiaj ogromna. Rozciąga się od ochrony fizycznej o charakterze prewencyjnym i informacyjnym wynikającym z obowiązujących aktów prawnych i dokumentów dotyczących zapobiegania, przeciwdziałania i zwalczania koronawirusa, poprzez obsługę systemów zabezpieczeń technicznych czy zliczanie osób, a kończy na udzielaniu pierwszej pomocy przedmedycznej. Lista naszych zadań w obiektach handlowych rozrosła się wraz z pandemią, ponieważ kwestia ochrony zdrowia stała się kluczowym wyznacznikiem działania obiektów handlowych. Przestrzeganie zasad i obostrzeń sanitarnych w obliczu rosnącej liczby nowych przypadków zakażenia się koronawirusem, w tym stosowane przez obiekty handlowe zasady DDM (dystans, dezynfekcja, maseczka), jest jednym z dodatkowych zadań pracowników ochrony. Niestety nie zostaliśmy wyposażeni w możliwość egzekucji obowiązujących przepisów. Kwestia kontrolowania prawidłowego noszenia maseczek przez klientów w centrach handlowych została niedawno poruszona przez przedstawicieli PRCH podczas rozmów z Ministrem Zdrowia. Obowiązek prawidłowego używania maseczek jest niestety ciągle kwestionowany przez wielu klientów. Dużym wyzwaniem są prowokacyjne zachowania osób, które celowo nie zakładają maseczek, awanturując się i tym samym utrudniając wykonywanie zadań pracownikom ochrony. Prowokacje są celowo nagrywane i publikowane w mediach społecznościowych. Takie sytuacje nie są łatwe, wymagają od pracowników wyważonego działania. Mając powyższe na uwadze, Securitas opracował szereg wytycznych i scenariuszy postępowania. Naszym pracownikom, pracującym na pierwszej linii kontaktu z klientami, zapewniliśmy odpowiednie szkolenia z zakresu zarządzania emocjami oraz wprowadziliśmy procedury, które znacznie ograniczyły eskalację prowokacji i są pomocne w realizacji obostrzeń sanitarnych. Securitas stara się również podkreślać rolę społecznej odpowiedzialności za zdrowie i bezpieczeństwo wszystkich osób przebywających na terenie centrów handlowych. Współpracujemy w tym zakresie z zarządcami placówek handlowych. ☺

NOWE OBLCZE BEZPIECZEŃSTWA POMAGAMY CZYNIĆ TWÓJ ŚWIAT BEZPIECZNIEJSZYM MIEJSCEM



Nieustannie badamy nowe technologie i wdrażamy najlepsze rozwiązania. Znamy specyfikę branż klientów i umiemy ograniczać ryzyko. Stosowane przez nas zintegrowane rozwiązania techniczne sprawiają, że nasza praca jest efektywna i skuteczna. Wiemy jednak, że to nasi pracownicy sprawiają, że jesteśmy najlepsi, dlatego oferujemy synergii, która wynika z połączenia tych dwóch światów.



Securitas

www.securitas.pl

Adresowalne sygnalizatory akustyczne ZETTLER

Przed wdrożeniem projektu danego systemu ochrony przeciwpożarowej zaleca się przeprowadzenie oceny ryzyka pożarowego obszaru, który ma zostać objęty ochroną. Na tej podstawie można określić rodzaj i specyfikację wymaganych urządzeń.



Stosowanie sygnalizatorów akustycznych jest obowiązkowe w ramach systemu wykrywania i sygnalizacji pożarowej. Bogata oferta produktowa Zettler umożliwia zastosowanie różnych rodzajów sygnalizatorów, co pozwala dostosować instalację do potrzeb klienta. Sposób montażu, kolor, wodoszczelność czy dodatkowa lampka błyskowa to cechy, spośród których klienci mogą wybierać.

PĘTLOWE, ADRESOWALNE SYGNALIZATORY ZETTLER SĄ DOSTĘPNE:

- w kolorach białym i czerwonym,
- do montażu wewnątrz oraz na zewnątrz (IP67),
- do montażu natynkowego oraz wpuszczanego (np. w ścianę karton-gips),
- w wersji ściennej lub jako gniazdo dowolnego detektora punktowego,
- w wersji z lampką błyskową lub bez.

CHARAKTERYSTYKA SYGNALIZATORÓW AKUSTYCZNYCH ZETTLER:

- kompaktowe i dyskretne,
- zasilanie i transmisja danych z pętli; nie wymaga dodatkowego okablowania i zasilania,
- wbudowany izolator zwarć,
- możliwość wyboru jednego z wielu tonów,
- realistyczny, konwencjonalny ton dzwonka,
- programowalne poziomy głośności
- wybieranie tonu i głośności za pomocą oprogramowania do konfiguracji centrali,
- programowalne częstotliwości migania (wersja z lampką błyskową),
- niezależne, adresowalne sterowanie sygnalizatorami akustycznym i optycznym (wersja z lampką błyskową).



OPTIMALIZACJA KOSZTÓW – WIĘCEJ URZĄDZEŃ W PĘTLI

Nowe sygnalizatory akustyczne firmy ZETTLER charakteryzują się niskim poborem prądu, umożliwiając podłączenie większej liczby urządzeń do pętli, co ułatwia projektowanie i instalację systemów. Dzięki naszemu centralom sygnalizacji pożarowej PROFILE Flexible dysponujemy pętlami o dużej obciążalności prądowej do 1 A, z maks. 250 adresami, co pozwala na wykorzystanie większej liczby sygnalizatorów akustycznych. Oznacza to ograniczenie liczby pętli w celu zwiększenia bezpieczeństwa obiektu i obniżenia kosztów instalacji, przy jednoczesnym zachowaniu zgodności z normami.

MNIEJ UTRUDNIEŃ – AUTOMATYCZNY TEST WŁASNY

Regularne testowanie systemów sygnalizacji pożarowej jest konieczne, ale często prowadzi do wielu utrudnień, szczególnie w takich budynkach, jak szpitale lub hotele. Sygnalizatory akustyczne z nowej gamy firmy ZETTLER są na tyle inteligentne, że w razie konieczności umożliwiają

przeprowadzenie samoczynnego autotestu, nie powodując przy tym utrudnień w funkcjonowaniu obiektu. Natychmiastowa funkcja monitorowania dźwięku odbitego (RSM) umożliwia przeprowadzenie pełnego autotestu urządzeń akustycznych, z czasem aktywacji wynoszącym ułamek sekundy na każde urządzenie.

Tak krótki czas testowania ogranicza do minimum poziom utrudnień i zmniejsza negatywny wpływ na użytkowników budynków. To z kolei pozwala podczas prawdziwego alarmu pożarowego utrzymać szybkość reakcji na wysokim poziomie, a także zmniejszyć prawdopodobieństwo wystąpienia fałszywego alarmu.

Działanie funkcji autotestu nie opiera się na elektronicznych pomiarach lub symulacjach, lecz na rzeczywistych wartościach. Taka metoda testowania jest bardzo dokładna. Dzięki jej wykorzystaniu użytkownik końcowy może mieć pewność co do wydajności działania systemu.

Autotesty mogą być wykonywane w dowolnym momencie. Można je zaprogramować tak, aby odbywały się wg wcześniej ustalonego harmonogramu, odpowiedniego dla osób przebywających w budynku i bez powodowania jakichkolwiek zakłóceń w pracy i utrudnień dla użytkowników. ☺



JOHNSON CONTROLS
INTERNATIONAL

ul. Krakowiaków 50
02-255 Warszawa
pawel.jozwik@jci.com



ARGUS RV-C

– certyfikowana platforma do zarządzania bezpieczeństwem pożarowym



System ARGUS RV-C klasy PSIM firmy Telbud został opracowany z wykorzystaniem sprawdzonych rozwiązań stosowanych do sterowania oraz nadzoru stacji i rozległych sieci elektroenergetycznych na terenie całego kraju. Charakteryzuje się dużą stabilnością działania, zaawansowanymi mechanizmami ochrony komunikacji i wysokim bezpieczeństwem cyfrowym. Może integrować inne systemy zabezpieczeń technicznych w zakresie monitoringu i sterowania.

Platforma jest wynikiem pracy wyłącznie polskich inżynierów i programistów – umożliwia to jego szybkie dostosowanie do bieżących potrzeb użytkowników i zmieniających się wymagań prawnych w zakresie ochrony przeciwpożarowej. ARGUS RV-C ma świadectwo dopuszczenia CNBOP-PIB.

Możliwość sterowania elementami systemów ochrony technicznej z poziomu platformy integrującej pozwala na realizowanie automatycznych interakcji pomiędzy tymi systemami w odpowiedzi na sygnały alarmowe lub ostrzegawcze generowane przez którykolwiek z nich.

OBSŁUGA Z POZIOMU STACJI ROBOCZYCH PC

Obsługa systemu może być prowadzona z poziomu stacji roboczych PC wyposażonych w oprogramowanie klienta aplikacji wizualizacyjnej ARGUS RV, pracującej pod systemem operacyjnym Windows. Stacje te mogą się składać z kilku monitorów LCD i współpracować z wizualizacją na wielkoformatowej ścianie graficznej. Stany całego systemu ochrony są agregowane w przejrzystym dzienniku zdarzeń, do którego wpływają z rozdzielczością milisekund.

KOMUNIKACJA MIĘDZY URZĄDZENIAMI SYSTEMU

Stabilną komunikację między urządzeniami systemu osiągnięto dzięki połączeniu serwerów zabudowanych w szafach rack, terminali operatorskich, koncentratorów interfejsów i przełączników sieciowych z ringiem światłowodowym Ethernet TCP/IP, a także powiązaniu oddalonych szafek modułów wejścia/wyjścia z szafką koncentratora ringiem magistrali RS-485, podobnie do połączeń pomiędzy centralami SSP.

Niezawodność komunikacji systemu ARGUS RV-C z integrowanymi systemami i urządzeniami ochrony przeciwpożarowej uzyskano poprzez bezpośrednie połączenia sieciowe pomiędzy odpowiednimi portami Ethernet w układzie punkt-punkt, zamiast wykorzystania dedykowanej dla systemów bezpieczeństwa sieci LAN. System umożliwia również stosowanie połączeń redundantnych na interfejsach sieciowych i szeregowych.

Oprogramowanie koncentratora interfejsów jest zintegrowane z systemowym oprogramowaniem serwera ARGUS RV przy wykorzystaniu komunikacji po sieci Ethernet TCP/IP z bezpiecznymi protokołami DNP3 lub IEC 104. ☺

Typowym przykładem takich interakcji jest kierowanie predefiniowanych kamer obrotowych PTZ na miejsca zdarzenia alarmowego sygnalizowanego przez system ochrony obwodowej oraz włączenie dodatkowego punktowego oświetlenia i mechanizmów zaawansowanego śledzenia obiektu.

KOMPLETNY SYSTEM

Świadectwo dopuszczenia systemu ARGUS RV-C obejmuje wszystkie elementy w zabudowach wyposażonych w urządzenia zasilające, komunikacyjne i zabezpieczające. Urządzenia te pozwalają na tworzenie zintegrowanych systemów zarządzania bezpieczeństwem pożarowym bez konieczności używania dodatkowych zewnętrznych elementów, które nie mają certyfikacji, takich jak serwery czy przełączniki sieciowe.

Do systemu można podłączyć moduły DCM-100, które uzupełniają system ppoż. o wejścia/wyjścia dwustanowe służące do sterowania m.in. systemem oddymiania, jak również innymi elementami podlegającymi automatyce budynkowej. Moduły serii DCM-100 można rozbudowywać o kolejne, zwiększając tym samym dostępność wejść/wyjść w systemie.

System ten można też wykorzystać do przeprowadzenia skutecznej ewakuacji personelu z zagrożonego obszaru.

TELBUŁ

ul. Krauthofera 23
60-203 Poznań
www.telbud.pl



REMOTE WITH SCHRACK SECONET



– RAZEM w czasach pandemii



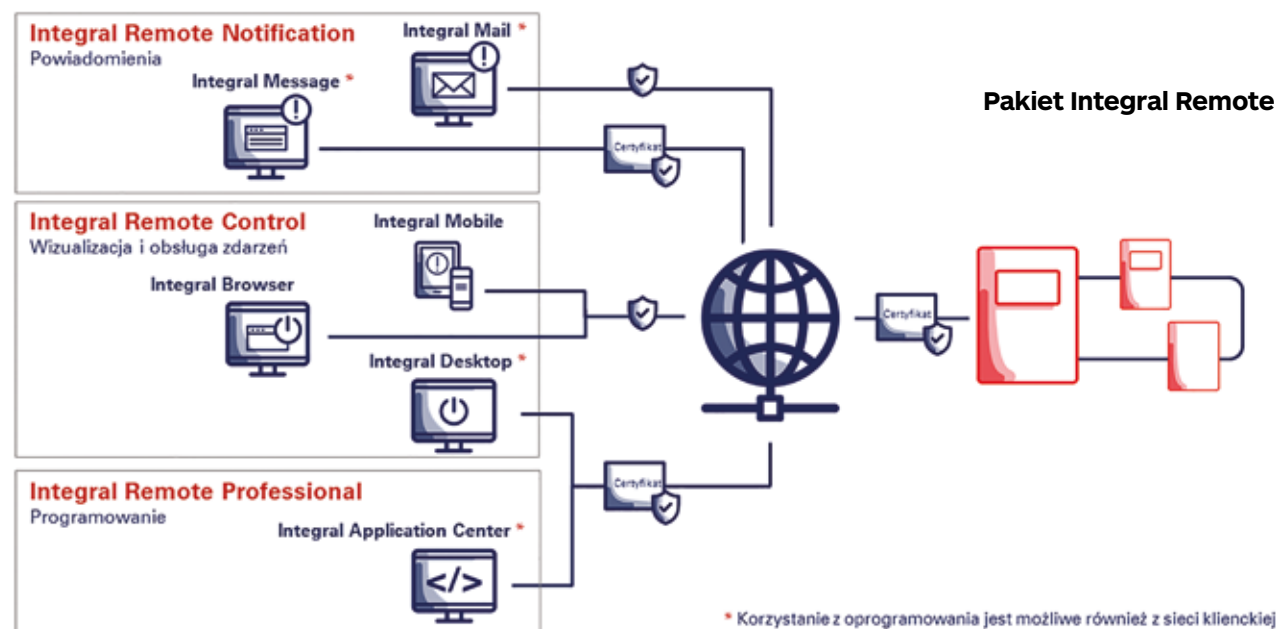
Już wtedy, na początku niepewnego jutra, zdaliśmy sobie sprawę, że podjęta wcześniej decyzja o rozwoju narzędzi serwisowych wspierających zdalny dostęp była właściwa. Nadszedł czas na zdecydowane przyspieszenie ich rozwoju i unowocześniania, by jeszcze bardziej usprawnić obsługę systemów bezpieczeństwa w obiekcie i rozszerzyć wsparcie dla użytkownika ze strony firm serwisujących. Doświadczenia ostatnich kilkunastu miesięcy przekonują do tego, by jeszcze szczegółowiej analizować organizację zarządzania systemami zabezpieczeń technicznych w celu zapewnienia ciągłości ich działania w sytuacji ograniczonego dostępu do obiektu i jego instalacji. Należy wziąć pod uwagę także potencjalne odizolowanie specjalistów od możliwości lokalnego nadzoru obiektu i bezpośredniej obsługi urządzeń.

W pierwszej połowie 2020 r., w czasie rozpędzającej się pandemii, przygotowaliśmy artykuł dotyczący naszych najlepszych rozwiązań, które zdecydowanie ułatwiają codzienną obsługę i nadzór serwisowanych obiektów. Zaprezentowaliśmy narzędzia zdalnego dostępu do systemu sygnalizacji pożarowej Schrack Seconet – Integral Remote.

Nasza uwaga powinna być skoncentrowana na doborze urządzeń wyposażonych w funkcje systemowe umożliwiające bezpieczny zdalny dostęp do instalacji bezpieczeństwa i zapewnieniu personelowi technicznemu pełnego zakresu nadzoru, a służbom serwisowym dodatkowych funkcji zdalnej konfiguracji, takich jak przy połączeniu lokalnym, przy jednoczesnym zapewnieniu wymaganych środków bezpieczeństwa. Wszystkie rozwiązania Schrack Seconet do zdalnej obsługi zostały opracowane i wykonane w taki sposób, aby umożliwić maksymalne wsparcie w tym zakresie poszczególnym użytkownikom systemów w zależności od pełnionej roli i posiadanych kompetencji.

INTEGRAL REMOTE

Pakiet rozwiązań na urządzenia mobilne i stacjonarne, umożliwiający zdalny dostęp do systemu sygnalizacji pożarowej Integral EvoX, to kolejne sprawdzone i niezawodne rozwiązanie z oferty Schrack Seconet, pozwalające na nadzór, obsługę i zarządzanie instalacją.



cją sygnalizacji pożarowej bez konieczności wizyty w obiekcie. Ze względu na pandemię i jeszcze bardziej ograniczony dostęp do serwisowanych obiektów narzędzia wchodzące w skład Integral Remote zostały udoskonalone i rozszerzone o nowe funkcje. Poszczególne aplikacje i narzędzia wchodzące w skład pakietu umożliwiają w trybie online wykonywanie wszystkich wymaganych operacji z zakresu nadzoru i/lub konfiguracji SSP. Niezależnie które aplikacje wybierze, zyskujemy gwarancję kontroli obiektu przez 24 godziny na dobę, a także możliwość zdalnego zdiagnozowania usterek i (w niektórych przypadkach) rozwiązania problemu (bądź wsparcie użytkownika) bez konieczności wizyty w obiekcie. Jeżeli przyjazd jest konieczny, służby serwisowe pojawiają się odpowiednio przygotowane i wyposażone w wymagane części zapasowe.

Szczególnie w ostatnim czasie zalety pakietu Integral Remote dostrzegają uczestnicy rynku bezpieczeństwa pożarowego, zarówno inwestorzy, jak i firmy obsługujące i serwisujące systemy. Od pojawienia się ograniczeń związanych z pandemią wprowadziliśmy specjalną ofertę cenową dla wszystkich narzędzi wchodzących w skład Integral Remote.

PLATFORMA S2SERVICE

Platforma S2Service to najnowszy pakiet narzędzi w ofercie Schrack Seconet zaprojektowany i stworzony przez Schrack Seconet w oparciu o rozwiązanie chmurowe przygotowane specjalnie do rozszerzonej zdalnej obsługi, nadzoru i zarządzania instalacjami bezpieczeństwa pożarowego, wspomagające proces inwestycyjny na każdym jego etapie. Projektanci/instalatorzy poprzez platformę informatyczną pracującą w chmurze mają dostęp do pełnej dokumentacji technicznej i serwisowej każdego elementu systemu. Baza dokumentacji jest automatycznie synchronizowana z serwerami Schrack Seconet, gwarantując dostęp do wszystkich aktualizacji. Rozwiązanie pozwala inwestorom i firmom instalatorskim obniżyć koszty serwisu i skrócić czas reakcji na zgłoszenia serwisowe. Specjalna bezpieczna infrastruktura IT umożliwia zdalny dostęp i wygodne zarządzanie wszystkimi systemami sygnalizacji pożarowej Schrack Seconet obsługiwany przez firmę z poziomu jednej platformy serwisowej. Informacje o obsługiwanych instalacjach, wraz z aktualną dokumentacją techniczną, protokołami serwisowymi i harmonogramami prac serwisowych są przechowywane w jednym bezpiecznym miejscu, a rozbudowane narzędzia analityczne usprawniają i ułatwiają planowanie prac serwisantów. Podgląd zdarzeń w czasie rzeczywistym i automatyczne generowanie protokołów serwisowych zawierających kluczowe informacje (np. zdjęcia, uwagi serwisowe) zapisywane w chmurze w trakcie prac serwisowych w pełni automatyzuje proces i znacznie skraca jego czas. Platforma chmurowa z wielostopniową autoryzacją dostępu dla użytkowników oraz szyfrowane połączenia tunelowe VPN z nadzorowanymi instalacjami sygnalizacji pożarowej zapewnia najwyższy poziom bezpieczeństwa. Możliwości S2Service pozwalają na wykonywanie dużej części prac serwisowych w bezpieczny sposób zdalnie, bez konieczności udawania się do obiektu. Wszystkie nieprawidłowości są na bieżąco analizowane i raportowane, a fizyczną obecność obsługi technicznej na miejscu instalacji można ograniczyć do niezbędnego minimum. Obsługa, korzystając z bezpiecznego połączenia, może szybciej reagować na zgłoszenie serwisowe, a w czasie normalnej eksploatacji dbać o prawidłowy, wysoki poziom sprawności i aktualności oprogramowania swoich instalacji. W przypadku instalacji ze starszymi urządzeniami Schrack Seconet narzędzie, po analizie bieżącej konfiguracji i wersji oprogramowania, umożliwia sprawne zaplanowanie procesu rozbudowy czy modernizacji.

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM POŻAROWYM SIS-FIRE

W zapewnieniu ciągłości działania obiektu kluczową rolę odgrywa system integrujący urządzenia przeciwpożarowe (SIUP).



Realizuje on zaawansowane funkcje nadzoru, sterowania i zarządzania urządzeniami ppoż. wraz z innymi zintegrowanymi z nim urządzeniami/systemami mającymi bezpośredni wpływ na bezpieczeństwo pożarowe obiektu. SIUP SIS-FIRE, oprócz lokalnych stacji operatorskich, umożliwia zastosowanie również stanowisk do zdalnego zarządzania, co ułatwia przekierowanie kompetencji nadzoru poza obiekt do zewnętrznych centrów zarządzania. Takie rozwiązanie zdecydowanie usprawnia bieżącą eksploatację, szczególnie w przypadku ograniczeń związanych z dostępem do obiektu. Dotychczasowe realizacje i wdrożenia systemu SIS-FIRE w Polsce potwierdzają, że jest on z powodzeniem wykorzystywany do centralnego nadzoru i zarządzania rozproszonymi instalacjami bezpieczeństwa pożarowego w ramach organizacji danego klienta.

SIUP, jako jedyny system bezpieczeństwa, jest umocowany prawnie do zarządzania ewakuacją ludzi. Ma to ogromne znaczenie nie tylko w przypadku wystąpienia pożaru, ale też podczas innych zdarzeń kryzysowych (np. wyciek toksycznego gazu w obiekcie przemysłowym). W sytuacji zagrożenia system aktywnie wspiera operatora dzięki specjalnym instrukcjom/procedurom postępowania przygotowanym na podstawie instrukcji bezpieczeństwa pożarowego i innych procedur bezpieczeństwa obiektu. Tym, co dodatkowo wyróżnia SIUP, jest możliwość dynamicznego ręcznego przesterowania (zmiana automatycznego scenariusza działania) zintegrowanych urządzeń ppoż. i technicznych obiektu w odpowiedzi na niekontrolowany rozwój pożaru czy inne zdarzenia kryzysowe. Zastosowanie SIUP do zdalnego nadzoru i zarządzania wymaga zapewnienia odpowiednich środków bezpieczeństwa w zakresie ciągłości działania infrastruktury informatycznej (np. redundancja krytycznych tras komunikacyjnych i/lub urządzeń) oraz odpowiedniej ochrony w zakresie szeroko rozumianego cyberbezpieczeństwa.

Wszystkie narzędzia do zarządzania i zdalnej obsługi obiektów, zwłaszcza rozproszonych, tworzymy i stale udoskonalamy, by zapewnić klientom i użytkownikom naszych systemów jeszcze wyższy poziom bezpieczeństwa. Mamy nadzieję, że nasze starania wspierają i będą wspierać działania naszych najlepszych Partnerów w Polsce na każdym etapie inwestycji, a inwestorom i firmom serwisującym nie tylko znacznie ograniczą koszty, ale przede wszystkim podniosą komfort pracy i użytkowania. ☺

SCHRACK SECONET POLSKA

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



System Zarządzania Ciągłością Działania (BCMS)

Cz. 1. Czy w ogóle jest to komuś potrzebne?

Każda organizacja dąży do maksymalizowania swojej wartości oraz osiągania jak największych przychodów przy zachowaniu możliwie najniższych kosztów. Mówiąc wprost, celem organizacji powinno być przynoszenie dochodów jej właścicielom i akcjonariuszom. Czy zawsze jednak maksymalizowanie przychodów, zysków oraz ograniczanie kosztów działalności operacyjnej jest uzasadnione?



Tomasz Guzikowski

Jeżeli zakładamy, że podejmujemy działalność na krótko, bądź prowadzimy biznes tzw. sezonowy lub oparty na krótkotrwałej modzie, takie podejście może być słuszne i nie będzie miało większego wpływu na efekt. Trochę inaczej rzecz się ma, gdy chcemy zbudować wartość firmy w dłuższej perspektywie. Wówczas zadajemy sobie pytania dotyczące m.in. inwestycji, strategii rozwoju, struktury kosztów, utrzymania w sprawności maszyn i urządzeń, pozyskiwania nowych klientów, zapewnienia dostaw surowców i półproduktów, a także wielu innych elementów, które mają na celu nie tylko utrzymanie się firmy na rynku, ale także jej rozwój. Z kolei aby zapewnić rozwój firmy, bez wątpienia musimy zapewnić ciągłość jej funkcjonowania. Czy to oznacza, że musimy wdrożyć system zarządzania ciągłością działania?

Wymagania systemu zarządzania ciągłością działania wg normy europejskiej EN ISO 22301 zostały opracowane i opublikowane stosunkowo niedawno. Czy zatem wcześniej organizacje nie zarządzały bądź nie utrzymywały ciągłości działalności? Generalnie początki systemowego podejścia do budowania odporności organizacji na wszelkiego rodzaju zaburzenia w działalności, w tym również ciągłego doskonalenia, sięgają połowy XX wieku. Obecnie w wielu obowiązujących aktach prawnych o charakterze ogólnym bądź branżowym, dyrektywach, standardach polskich i zagranicznych, rekomendacjach i opracowaniach stanowiących źródła dobrych praktyk można znaleźć kluczowe odniesienia do rozwiązań mających na celu zapewnienie ciągłości działania.

Przykładami takich dokumentów są m.in. ustawa o zarządzaniu kryzysowym, ustawa – Prawo bankowe, dyrektywa Rady Europy w sprawie rozpoznavania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, norma PN-1-27001 „Systemy zarządzania bezpieczeństwem informacji”, rekomendacje D i M stanowiące wytyczne do zarządzania rodzajami ryzyka towarzyszącymi bankowym systemom informatycznym i telekomunikacyjnym oraz w zakresie ostrożnego i stabilnego zarządzania ryzykiem operacyjnym w banku i wiele innych.

Uznaje się, że pierwszym standardem, który kompleksowo opisywał zagadnienia ciągłości działania, był standard BS 25999, a pierwszą instytucją, która publikowała najlepsze praktyki w zakresie zarządzania ciągłością działania, był utworzony w 1988 r. Disaster Recovery Institute International (DRII). Jest to organizacja non profit o zasięgu międzynarodowym, która w początkowym okresie swojej działalności skupiała partnerów w Ameryce Płn. i Azji. W 1994 r. utworzono w Europie Business Continuity Institute (BCI), organizację działającą na podobnych zasadach.

Poza tymi aktami prawnymi, normami i standardami każda organizacja niejako instynktownie wdraża działania mające na celu zapewnienie osiągnięcia celów, w tym utrzymania ciągłości działalności. Czy fakt, że system zarządzania ciągłością działania nie jest udokumentowany, czy też wprost oparty na konkretnej normie, oznacza, że firma nie potrafi tej ciągłości utrzymać? Odpowiedź na to pytanie jest dość oczywista.

Oczywiście, nie.

Założmy, że mamy do czynienia z działalnością opartą na prostym procesie produkcyjnym, gdzie mamy zapewniony zdywersyfikowany łańcuch dostaw, popyt na produkty zapewniający ich stały odbiór, dodatnie przepływy pieniężne i dostęp do siły roboczej, w której to działalności nie odnotowano istotnych zdarzeń wewnętrznych czy zewnętrznych mogących mieć wpływ na utratę jej wartości. Jednym słowem otoczenie wewnętrzne i zewnętrzne jest idealne.

Niestety taki stan rzeczy nie trwa wiecznie, dlatego firmy opracowują i wdrażają m.in. strategie rozwoju, wprowadzanie na rynek nowych produktów, pozyskiwanie nowych klientów, poszukiwanie nowych źródeł zasobów itp. Opracowują również instrukcje technologiczne, procedury i instrukcje postępowania w zakresie utrzymania ruchu itd. Są to elementy, które mają bezpośredni wpływ na utrzymanie ciągłości działania organizacji. Inną kwestią jest to, które z procesów realizowanych w organizacji są kluczowe, a ich przerwanie może mieć bezpośredni wpływ na ciągłość jej działania.

Obecnie tylko niektóre obszary działalności w pewnym zakresie są zobowiązane do wdrażania elementów systemu zarządzania ciągłością działania bądź wprost systemem opartego na normie ISO 22301. Do takich branż należą m.in. instytucje bankowe, które poprzez przepisy ustawy Prawo bankowe są zobowiązane do posiadania planów działania zapewniających ciągłe i niezakłócone prowadzenie działalności i realizacji procesów w sytuacjach awaryjnych. Kolejni to przedsiębiorcy telekomunikacyjni, dla których ustawa Prawo telekomunikacyjne jednoznacznie określa konieczność posiadania planów awaryjnych. Muszą one obejmować również m.in. współpracę z innymi firmami telekomunikacyjnymi i zagranicznymi operatorami telekomunikacyjnymi. Podobnie rzecz się ma wobec instytucji i przedsiębiorstw energetycznych, pocztowych oraz organów odpowiedzialnych za zarządzanie kryzysowe czy ubezpieczeniowe społeczne.

Pozytywne jest to, iż również organizacje działające w innych obszarach gospodarki same zauważają, że bez kompleksowej strategii i planowania utrzymania zarówno bieżącej działalności, jak i umiejętności reagowania na awarie nie da się zapewnić rozwoju i zachowania konkurencyjności na rynku. A często ich brak może prowadzić do poważnych problemów lub wręcz upadłości firmy.

Wspominałem wcześniej o standardzie BS 25999 oraz o dokumencie, który go zastąpił, jakim jest obecnie norma europejska PN-EN ISO 22301:2020-04 (*Bezpieczeństwo i odporność – Systemy zarządzania ciągłością działania – Wymagania*). Norma ta, opracowana przez czołowych specjalistów w zakresie ciągłości działania, określa ramy systemu zarządzania ciągłością działania, które można wykorzystać we wdrożeniu praktycznie w każdej organizacji. Właściwe wdrożenie Systemu Zarządzania Ciągłością Działania przygotowuje organizację, aby odpowiednio i skutecznie reagować na pojawiające się lub potencjalne incydenty, dzięki czemu znacznie zmniejsza się ryzyko i poziom potencjalnych szkód wynikających z ich wystąpienia. Co więcej, przedsiębiorstwo poszerza wiedzę na temat swojej organizacji, znacznie efektywniej wykorzystuje własne zasoby, jest bardziej konkurencyjne i szybciej reaguje na zmiany. ☺

TOMASZ GUZIKOWSKI



Menedżer z wieloletnim doświadczeniem w obszarze zarządzania bezpieczeństwem i ciągłością działania, w tym bezpieczeństwa procesowego i zawodowego, ochrony infrastruktury krytycznej, ochrony informacji niejawnych w budownictwie i dużych zakładach produkcyjnych należących do grupy zakładów dużego ryzyka powstania awarii przemysłowej. Obecnie zarządza obszarem bezpieczeństwa w koncernie chemicznym CIECH.

Przerwanie łańcucha dostaw

Zagrożenie tylko dla dużych przedsiębiorstw?

Łańcuch dostaw oznacza zestaw czynności i sieci połączeń od źródła produktu do klienta końcowego. Obejmuje różnych dostawców i przedsiębiorstwa, zaopatrując kolejne ogniwa.



Mirosław Lukowski

Jest wiele definicji łańcucha dostaw. Najszerzą z nich przedstawiła firma Mecalux¹, wg której „łańcuch dostaw (supply chain) to proces prowadzony od momentu złożenia zamówienia przez klienta do dostarczenia produktu lub usługi i rozliczenia transakcji. W związku z tym termin ten obejmuje planowanie, realizację i kontrolę wszystkich czynności związanych z przepływem materiałów i informacji, poczynając od zakupu surowców, przez szereg procesów przetwórczych, skończywszy na dostarczeniu produktu klientowi. Można zatem zdefiniować łańcuch dostaw jako zestaw czynności i sieci połączeń od źródła produktu do klienta docelowego. Łańcuch ten obejmuje różnych dostawców i przedsiębiorstwa, zaopatrując kolejne ogniwa. Obecnie łańcuchy dostaw charakteryzują się wysoką złożonością ze względu na internacjonalizację, zwiększenie intensywności różnego rodzaju przepływów pomiędzy przedsiębiorstwami a klientami oraz zmiany zachodzące w modelach globalnej konsumpcji.

¹ <https://www.mecalux.pl/>

Łańcuch dostaw składa się z trzech głównych etapów:

- ZAOPATRZENIE – dotyczy sposobu, miejsca i momentu pozyskania oraz dostarczenia surowców służących do produkcji wyrobów.
- PRODUKCJA – czyli przekształcenie surowców w wyroby gotowe.
- DYSTRYBUCJA – wszelkie czynności umożliwiające dostarczenie produktów do miejsca docelowego. Jest to możliwe za pośrednictwem sieci dystrybutorów, magazynów, sklepów stacjonarnych lub internetowych (w przypadku działalności e-commerce).

Łańcuch dostaw nie tylko ma ogromne znaczenie dla funkcjonowania poszczególnych zakładów, placówek handlowych czy dystrybutorów, ale także znacząco wpływa na cenę produktu dla klienta końcowego.

Czy tak kluczowy element w procesie produkcji i sprzedaży może odbywać się bez kalkulacji ryzyka? Dzisiaj z całą pewnością wiemy już, że nie może. A jeszcze trzy lata temu tylko duże zakła-

dy produkcyjne i przemysłowe posiadały właściwe struktury i świadomość, jak ważne jest zapewnienie ciągłości łańcucha dostaw.

Doświadczenie z ostatnich dwóch lat pokazuje, że świat nie do końca był przygotowany na pandemię, której nikt się nie spodziewał, a której skutki odczuwamy nie tylko lokalnie, ale także globalnie. Dziś każdy ważny proces powinien zaczynać się od oceny ryzyka utraty płynności funkcjonowania przedsiębiorstwa. Transformacja struktur ochrony – od formacji ochronno-bojowej (skoncentrowanej na ochronie osób i mienia za pomocą dostępnej techniki) do organizacji wsparcia procesów biznesu – to nie konieczność, ale naturalny proces ewolucji branży. Poznanie procesów i mechanizmów działania biznesu oraz zasad funkcjonowania zakładu przemysłowego, produkcyjnego czy handlowego pozwala na działania struktur ochrony, które już na etapie planowania niektórych procesów mogą je odpowiednio zabezpieczyć. Jednym z takich elementów jest łańcuch dostaw.

Każde przedsiębiorstwo, którego płynność zależy od tego procesu, powinno zacząć od właściwego jego zabezpieczenia. Tu powinny zadziałać mechanizmy zabezpieczające dostawy, takie jak dywersyfikacja dostawców zarówno elementów, jak i produktów, zabezpieczenie alternatywnych dróg dostaw czy korzystanie z różnych dostawców usługi transportowej, odpowiednie polisy i ubezpieczenia, a przede wszystkim wyprzedzanie potencjalnych problemów. Jest to możliwe dzięki właściwej analizie ryzyka.

Każdy duży przedsiębiorca jest tego świadomy i posiada struktury, które opracowują plany alternatywne. A co z małym przedsiębiorcą? Czy powinien przeprowadzić analizę łańcucha dostaw, zasięgnąć rady profesjonalistów zajmujących się oceną ryzyka? A może mały przedsiębiorca uważa, że to zbędne, bo przecież sam najlepiej wie, co jest dobre dla jego małej lokalnej firmy?

Rozpatrzmy problem na przykładzie. Załóżmy, że Kowalski założył mały biznes, np. warzywniak. Wynajął lokal, a ze względu na niewielki kapitał kupił stare auto, którym jeździ na pobliską giełdę po towar. Kowalski na giełdzie kupuje towar, inwestując duże środki, bo jest piątek, a towaru musi wystarczyć do poniedziałku, tymczasem w drodze powrotnej samochód ulega awarii. Stare auto ma tylko ubezpieczenie OC i assistance po wypadku, laweta to dodatkowy koszt, więc postanawia poradzić sobie na własną rękę. Sklep jest zamknięty, a Kowalski poświęca czas i środki na naprawę samochodu. W tym czasie część wrażliwego towaru może ulec zepsuciu... A wystarczyło pomyśleć o lepszym ubezpieczeniu auta.

Zakłócenia w łańcuchu dostaw mogą nie tylko zatrzymać procesy produkcyjne czy opóźnić funkcjonowanie biznesu. Trwałe zaburzenia mogą powodować o wiele groźniejsze konsekwencje, nawet upadek przedsiębiorstwa. Konsekwencje odczują wszyscy, nie tylko przedsiębiorstwa, ale też zwykli obywatele, ponieważ na zbliżające się święta może zabraknąć np. zabawek, gdyż większość produkcji odbywa się w jednej części świata.

Każdy przedsiębiorca, niezależnie od tego, czy działa na rynku lokalnym, czy międzynarodowym, czy obraca dużym kapitałem, czy małą gotówką, powinien mieć świadomość, że łańcuch dostaw ze złe skalkulowanym ryzykiem i z nieodpowiednio przygotowanym planem działania w sytuacjach kryzysowych skutkuje groźnymi konsekwencjami. W najgorszym wypadku nawet utratą możliwości prowadzenia biznesu lub w wersji optymistycznej droższym produktem końcowym powodującym pogorszenie się konkurencyjności i spadek sprzedaży. Mamy dziś w Polsce wielu specjalistów potrafiących to ryzyko ocenić, skalkulować i wskazać ścieżki, które minimalizują efekt zaburzenia łańcucha dostaw. Warto przeprowadzić taką ocenę nawet w przypadku małej rodzinnej placówki.

MIROSŁAW LUKOWSKI

Ekspert w dziedzinie bezpieczeństwa handlu. Od 20 lat związany z branżą security. W latach 2017-2019 krajowy koordynator w Dziale Ryzyka Prewencji i Ochrony Sieci Carrefour Polska. Dziś prezes Hyder Tech, spółki wdrażającej nowe technologie związane z najnowszymi zabezpieczeniami zwalczającymi zagrożenia powodowane przez wirusy, bakterie i roztocza.

Etapy łańcucha dostaw (supply chain)



Źródło: <https://www.mecalux.pl/blog/lancuch-dostaw-co-to-jest>

Bezpieczna organizacja

Aspekty techniczne szeroko rozumianego bezpieczeństwa są bez wątpienia istotne, lecz wymagają profesjonalnej obsługi przez człowieka. Do pełni szczęścia brakuje tu również elementu stricte zarządczego (*governance*). To tutaj technika i ludzie zaczynają współgrać w sposób adekwatny do potrzeb organizacji. Przyjrzyjmy się kilku sposobom, jak można rozumieć tę tematykę „z góry” (tzw. *helicopter view* – z lotu ptaka) oraz w ujęciu bezpieczeństwa przetwarzanych danych.



Tomasz Dacka

BEZPIECZEŃSTWO NA E-PAPIERZE

Coraz częściej pracujemy na dokumentach elektronicznych, porzucając formę papierową. Dokumentacja natomiast, bez względu na swoją formę, pełni znaczącą funkcję w życiu codziennym jednostek organizacyjnych:

- określa jasne zasady działania dla wszystkich, jest zatem zrozumiała,
- określa jasno prawa i obowiązki, wytycza strefy,
- pomaga zrozumieć proces (odnosi się do innych dokumentów uzupełniających),
- wprowadza rozliczalność,
- z założenia powinna być samodoskonaląca poprzez aktualizacje iteracyjne,
- podnosi świadomość bezpieczeństwa,
- podkreśla działanie kierownictwa z tzw. należytą uwagą (*due care, due diligence*).

Jeśli oczekujemy od pracowników określonego zachowania w określonych sytuacjach, musimy te zasady jasno komunikować. Trudno oczekiwać od instalatora poprawnie wykonanej instalacji, nie wyposażając go w odpowiednie narzędzia i wiedzę, jak z tych narzędzi korzystać.

Najważniejszym dokumentem powinna być polityka bezpieczeństwa. Dokument ten, komunikowany przez najwyższe kierownictwo jednostki organizacyjnej (tzw. C-Team), powinien w jasny, zwięzły sposób opisywać cele bezpieczeństwa, tym samym potwierdzając zaangażowanie i wsparcie kadry zarządzającej. Taki poziom ogólności wymaga jednak doprecyzowania. Wykonuje się to za pomocą trzech innych typów dokumentów (gradacja może być różna i zależna od wymagań poszczególnych jednostek organizacyjnych):

- **Standard** – dokument również o ogólnym charakterze, dotyczący mierników oceny zgodności z polityką bezpieczeństwa. Mówi o tym, co należy wykonać.
- **Procedura** – zawiera opis, jak krok po kroku osiągnąć dane zadanie; powinna być raczej dokumentem „sztywnym”.
- **Wytuczna** – pojawi się tam, gdzie nie ma pokrycia w procedurach (obszar nie został jeszcze odpowiednio rozpoznany, a istnieje potrzeba szybkiej regulacji lub cały proces jest na tyle skomplikowany, aby pokryć go „sztywną” procedurą). Wytuczne mogą również zawierać odstępstwa od procedur.

Są to dokumenty wewnętrzne firmy. Powinny być zgodne z obowiązującą regulacją prawną oraz, gdy to zasadne, opatrzone odpowiednią klauzulą.

Przekładając to na obszar bezpieczeństwa fizycznego, można przykładowo określić:

1. standard bezpieczeństwa fizycznego,
2. procedurę wejścia do obiektu chronionego,
3. wytuczne w sprawie obsługi VIP-ów.

Jak widać na powyższym przykładzie, wytucznych i procedur może być bardzo dużo. Nie da się jednak opisać wszystkiego dokładnie. Z biegiem czasu oraz przyrostem dokumentacji dużym wyzwaniem staje się ich spójność. Sytuacją, której chce-

my uniknąć, jest wzajemne wykluczanie się zapisów dokumentacji. Przy uzgadnianiu dokumentacji z obszaru bezpieczeństwa fizycznego bardzo często biorą udział zespoły interdyscyplinarne. Dochodzi zatem do sytuacji, że dany proces musi spełniać wymogi przedstawicieli różnych obszarów, które nie zawsze mają ten sam cel (np. biznesowi zależy na ułatwieniu dostępu dla klientów, podczas gdy względy bezpieczeństwa wymagają wprowadzenia restrykcji w tym zakresie).

Dokumentacja powinna być przeglądana co najmniej raz w roku i w razie potrzeby uzupełniana. Zdarzają się jednak sytuacje, kiedy przegląd należy przeprowadzić ad hoc (np. po poważnym incydencie bezpieczeństwa lub przy zmianie regulacji prawnych). Zmiany w dokumentacji powinny:

- być uzgadnianie ze wszystkimi zainteresowanymi stronami,
- zostać udokumentowane, wraz z historią zmian,
- sprawdzone i przetestowane.

KTO ZARZĄDZA DANymi?

Systemy ochrony fizycznej (zarówno elektroniczne, jak i np. dzienniki posterunków ochrony) gromadzą duże ilości danych, w tym wrażliwych. Dokumentacja mówiąca o tym, jak dany proces ma się odbywać, jest niewystarczająca bez wskazania, kto i w jakim zakresie jest odpowiedzialny za przetwarzane dane. Mówimy wtedy o obszarze *data governance*. Polityka w tym zakresie powinna ustalić główne role:

- **Właściciel danych (*data owner*)**
 - zazwyczaj osoba z poziomu kierowniczego odpowiedzialna za zapewnienie poufności, integralności i dostępności danego aktywu informacyjnego, zaopatrzenie informacji odpowiednim poziomem dostępu oraz zapewnienie odpowiedniej ochrony. Właściciel danych zazwyczaj deleguje dwie pozostałe role (opisane poniżej).
- **Data Steward** – osoba odpowiedzialna za odpowiednią „jakość” danych. Steward danych odpowiednio określa status informacji (etykietuje informacje), odpowiada za to, że informacje są zbierane i przetwarzane zgodnie z regulacjami.
- **Data Custodian** – zarządza systemem, w którym dane są przetwarzane. W puli obowiązków opiekuńcza danych jest zapewnienie odpowiedniego dostępu, szyfrowania oraz sposobów archiwizowania i przywracania danych.

Często w organizacjach można spotkać się z innymi nazwami tych stanowisk, zakres obowiązków natomiast pozostaje podobny.

RETENCJA DANYCH

Jak długo należy przechowywać dane? Odpowiedź na to pytanie nie jest oczywista i zależy od kilku czynników:

- wewnętrznych regulacji organizacji (polityk),
- regulacji prawnych,
- wytycznych PUODO.

Zaleca się wprowadzać dywersyfikację retencji w zależności od charakteru informacji, np. nie z każdej kamery obraz przez nią generowany musi być przechowywany przez 90 dni.

UTYLIZACJA DANYCH

Dobrą praktyką jest przetwarzanie danych tak długo, jak to konieczne. W momencie przekroczenia tego czasu należy danych się pozbyć. Jednak to, że dla danej organizacji aktywa informacyjne nie są już potrzebne, nie oznacza, że sytuacja jest podobna dla naszych adwersarzy. Na rynku działa wiele firm, które oferują profesjonalną utylizację danych. Fakt zniszczenia musi zostać potwierdzony i udokumentowany, a firma, której powierzamy to zadanie, powinna zostać dokładnie wyselekcjonowana.

Jak zatem pozbyć się niechcianych danych?

Dokumenty papierowe – na pierwszy rzut oka sprawa wydaje się jasna, dokumenty wyrzuca się do śmieci z zachowaniem zasad segregacji. Abstrahując od nieprzypadkowych osób zajmujących się sprzątaniem w biurach, należy również zwrócić uwagę na to, czy śmietniki umiejscowione „na zewnątrz” są odpowiednio zabezpieczone przed nieuprawnionym dostępem. Dobrą zasadą jest niszczenie dokumentów papierowych przed ich wyrzuceniem, niszcarki do papieru można obecnie kupić nawet w popularnych dyskontach. Jeśli zachodzi potrzeba dokładniejszej metody utylizacji, należy zastosować proces spalania albo przerabiania na masę papierniczą poprzez rozpuszczanie w wodzie i sproszkowanie.

Dokumenty elektroniczne – jest sprawą oczywistą, że usunięcie pliku czy nawet formatowanie dysku nie zapewniają wystarczającej ochrony przed przywróceniem danych w momencie, kiedy komuś na tym bardzo zależy. W takim wypadku należy rozważyć:

- Nadpisywanie/*disk wiping* – specjalistyczne oprogramowanie zapewnia wyczyszczenie starych danych za pomocą ustawienia 0 (zera) w każdym bicie. Metoda ta jednak nie jest nieodwracalna, zaleca się w takim wypadku nadpisywanie losowymi 0 oraz 1 (zerami i jedynekami) wszystkich sektorów danego medium.
- Format niskiego poziomu – większość dostawców dysków twardych umożliwia ich reset do ustawień fabrycznych. Efekt jest podobny do poprzedniej metody.
- Fizyczne zniszczenie – dysk można zniszczyć fizycznie w specjalnie do tego przystosowanych niszcarkach.
- Rozmagnesowanie – poprzez poddanie dysku silnemu oddziaływaniu pola elektromagnetycznego.
- Szyfrowanie – poddanie szyfrowaniu wszystkich danych woluminu. Odczytanie danych nie jest możliwe bez posiadania klucza deszyfrującego.

PATRZ, KOMU UFASZ

W kontekście bezpieczeństwa organizacji wiele mówi się o ludziach. Wymienia się departamenty odpowiedzialne za cyberbezpieczeństwo, bezpieczeństwo fizyczne czy regulacyjne. Mało natomiast spotyka się informacji w omawianym kontekście na temat działów HR odpowiedzialnych za kluczowy zasób każdej firmy – ludzi. Pełnią one istotną funkcję w procesach:

- rekrutacyjnych – wybór odpowiednich osób do przypisanych zadań wakat; na tym etapie powinno się też odbywać sprawdzenie kandydatów i kandydatek (tzw. *background check*);
- operacyjnych – wprowadzenie pracownika do organizacji, komunikowanie zasad bezpieczeństwa, przeprowadzanie okresowych rozmów czy wsparcie w organizacji szkoleń rozwijających kompetencje;



- zakończenie współpracy – zaprzestanie świadczenia stosunku pracy (bez względu na powody) również powinno być usystematyzowane, rozmowy na tym etapie (tzw. *exit interviews*) mogą dostarczyć organizacji cennych informacji.

Działy HR odgrywają ważną rolę także w komunikowaniu pracownikom zmian dotyczących zasad bezpieczeństwa czy kampanii typu *security awareness*.

Ważny jest też sam proces wprowadzania pracownika (tzw. *on-boarding*). Dobrze przeprowadzony uświadamia pracownika, wprowadza w świat bezpieczeństwa, ostrzega, czego nie wolno (i dlaczego) robić, by nie narazić się na przykre konsekwencje, jak postępować z przetwarzaniem informacji. Dzięki temu zmniejszamy prawdopodobieństwo występowania niecelowych incydentów bezpieczeństwa.

Obecne czasy stanowią również wyzwanie z punktu widzenia zapewnienia odpowiedniej ilości i jakości pracy. Bezpieczeństwo należy zapewniać 24/7, nawet podczas urlopów czy niedyspozycji kluczowych pracowników. Nie bez znaczenia pozostaje również kwestia zagrożeń wewnętrznych (tzw. *insider threats*). Następujące zasady pomagają zaadresować ryzyka związane z powyższymi zagrożeniami:

Rozdzielenie obowiązków – oznacza, że żaden z pracowników nie powinien posiadać zbyt dużej decyzyjności ani odpowiedzialności, powinno się je rozdzielić pomiędzy zaufanych pracowników. Unikamy w ten sposób również sędziowania we własnej sprawie.

Obowiązkowy urlop – każdy pracownik zobowiązany jest do odpoczynku w minimalnym wymiarze dni. Podczas urlopu inna osoba zastępuje danego pracownika, którego dotychczasowa praca może być audytowana.

Zamiana ról – na danym stanowisku nie można pracować dłużej niż określony czas, co pozwala organizacji na uniknięcie zbyt dużego przywiązania do danego pracownika oraz zapewnia transfer wiedzy pomiędzy zespołami.

PODSUMOWANIE

Ludzie, technika, procedury. Te trzy elementy stanowią o sile ochrony każdej organizacji. Muszą się wzajemnie wspierać i rozumieć. Nawet najlepszy system ochrony elektronicznej będzie nieefektywny, jeśli będzie obsługiwany przez nieprzystosowany do tego personel. Jeśli człowiek będzie dobrze obsługiwał technikę, ale nie będzie świadom kroków, jakie powinien podjąć w danej sytuacji, zdarzenie nie zostanie obsłużone poprawnie, a na tym nam przecież zależy. Jasno określony cel kompleksowej ochrony obiektu, jego zrozumienie i wsparcie przez kadrę zarządzającą, odpowiednio dobrany personel oraz technika są gwarantem sprawnie działającego systemu ochrony.

To temat wymagający dużego wysiłku i zaangażowania wielu obszarów w każdej organizacji. Jeśli dołożymy do tego ciągle zmieniające się zagrożenia (oczekuj nieoczekiwanego), zmiany regulacyjne oraz cele biznesowe organizacji, rysuje się przed nami trudne wyzwanie. Zapewne również dlatego daje nam ono tyle satysfakcji. Bądźmy świadomie bezpieczni. ☺



TOMASZ DACKA

Ekspert bezpieczeństwa fizycznego. Z branżą związany ponad 12-letnim doświadczeniem, zwolennik holistycznego podejścia do zarządzania bezpieczeństwem. Prywatnie entuzjasta architektury przedwojennej Warszawy.

Innowacyjne rozwiązania integracji systemów bezpieczeństwa

Światowa nowość na polskim rynku klasy PSIM-CSIM



Skontaktuj się z nami w sprawie dedykowanej prezentacji

MEGAVISION TECHNOLOGY Sp. z o. o.

Heliotropów 1

04-796 Warszawa

tel. +48 22 292 3 292

psim@psim.pl

Prowadzący konferencję EBS Security 5.0 (od prawej):
Krzysztof Stalewski, Ralph Talmont i Krzysztof Stalewski

Konferencja EBS Security 5.0

Pod koniec października 2021 r. odbyła się online międzynarodowa konferencja zorganizowana przez polską firmę EBS. Prowadzona po angielsku, tłumaczona na j. polski i hiszpański, zgromadziła uczestników z 42 krajów.

Uczestników powitał **Krzysztof Stalewski, prezes Zarządu EBS**: Mam przyjemność otworzyć kolejne międzynarodowe wydarzenie z nadzieją, że prezentacje, które dla państwa przygotowaliśmy, będą interesujące i inspirujące.

Konferencję prowadził **Ralph Talmont, konsultant ds. komunikacji, ekspert w dziedzinie technologii, kreatywności i komunikacji, jeden ze współzałożycieli TEDxWarsaw**:

Dzisiaj przyjrzymy się tematowi security z różnych perspektyw. Główny panel będzie skoncentrowany na obecnych trendach w branży zabezpieczeń. Przedstawimy też najnowsze rozwiąza-



nia systemów alarmowych, w tym EBS – Smart communicators jako odpowiedź na światową ewolucję w infrastrukturze telekomunikacyjnej. Trzecim filarem będzie temat Lone worker monitoring, rozwiązań do zdalnego monitorowania pracowników ochrony.

Do udziału w konferencji zaproszono prelegentów z Polski, Niemiec, Turcji, Republiki Południowej Afryki, USA, Kolumbii. W wystąpieniach zastanawiano się, w jakim kierunku zmierza branża zabezpieczeń technicznych w kontekście connected world czy smart home. Podjęto też temat zastosowania rozwiązań w chmurze obliczeniowej, coraz bardziej popularnych zwłaszcza w czasie pandemii.

Uczestnicy mieli również okazję zapoznać się z wyzwaniami i specyfiką amerykańskiego rynku security. Choć rynek amerykański różni się od europejskiego, spojrzenie z innej perspektywy z pewnością zaowocuje pozytywnymi projektami dla obu stron. Gospodarze konferencji zapoznali uczestników ze swoimi rozwiązaniami, m.in. z zastosowaniem sztucznej inteligencji w usłudze monitorowania z wykorzystaniem ekosystemu ActiveView. Przedstawili też najnowsze produkty: AVA PRO Easy Install oraz LX connected.

Partnerami konferencji były firmy: **Google Cloud, Orange Polska, Thales, Sevenways, bluesolve partners.**

Firma EBS jest polskim producentem systemów zabezpieczeń oraz rozwiązań do automatyzacji biznesu, która działa już od 30 lat. Jej rozwiązania pracują na 5 kontynentach, zainstalowano ponad 3 mln urządzeń. Firma współpracuje z największymi agencjami ochrony i instytucjami rządowymi na całym świecie, ma własny zakład produkcyjny i dział R&D.

EBS dostarcza gotowe rozwiązania dla dostawców usług z branży ochrony. Jako pierwsza na świecie stworzyła rozwiązanie do zdalnego monitorowania pracowników ochrony w czasie rzeczywistym LONE WORKER MONITORING. Od lipca 2021 r. większościowym udziałowcem firmy EBS jest UAB Sevenways Group, litewski holding inwestycyjny.

EBS

ul. Bronistawa Czecha 59
04-555 Warszawa
<https://ebssmart.com>
office@ebssmart.com



Smart City Expo Poland 2021

Po dwuletniej przerwie, w październiku br. odbyły się targi technologii miejskich Smart City Expo Poland. W trakcie konferencji organizatorzy wręczyli nagrody za najlepsze wdrożenia technologii i usług „smart” w polskich miastach. Laureatami zostali: miasto Bolesławiec, Milestone Systems, Baid Group oraz Orange Polska.



↓ Za przemyślane i spójne inwestycje, łączące nowoczesne technologie z potrzebami mieszkańców miasta, nagrodę odebrał prezydent Bolesławca. W mieście wdrażane są inwestycje oparte na technologii Internetu rzeczy, w tym system zdalnego odczytu wodomierzy i identyfikacji awarii, system zarządzania oświetleniem, rowerów miejskich i system czujników jakości powietrza. W kategorii „Bezpieczeństwo publiczne” uznanie zyskał „Katowicki Inteligentny System Mo-

onitoringu i Analizy KISMiA”. W jego ramach funkcjonuje niemal 300 kamer rozszaniach na ponad 160 km² miasta, w którym mieszka niemal 300 tysięcy osób. Za system wdrożony przez Milestone Systems nagrodę odebrał Marcin Palka. Targi Smart City Expo Poland poświęcone są nowoczesnym technologiom miejskim i zastosowaniu ich w zarządzaniu miastem. W targach udział wzięło 60 wystawców z kraju i zagranicy.

IV Ogólnopolski Kongres Naukowo-Techniczny



Fot. Robert Szczechowiak

SAFE PLACE 2021

20-22 października 2021 r. w Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego w Warszawie odbył się IV Ogólnopolski Kongres Naukowo-Techniczny SAFE PLACE 2021 Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej. Dobre praktyki i rekomendacje. Wzięło w nim udział ponad 400 uczestników, co świadczy o merytorycznej sile wydarzenia, w którym corocznie biorą udział nowi uczestnicy indywidualni i instytucjonalni.

↓ Wysoki poziom merytoryczny i organizacyjny wydarzenia był możliwy dzięki współpracy organizatorów z instytucjami naukowymi, które pełniły funkcję współorganizatorów naukowych. Tegoroczną edycję SAFE PLACE zorganizowano w nowym miejscu, łącząc kongresowe obrady z obchodami 70. rocznicy powstania WAT oraz 10. rocznicą powołania dyscypliny nauk o bezpieczeństwie. Prezentowane panele tematyczne zostały rozbudowane, a dzięki obecności teoretyków i praktyków w znacznej części udało się omówić najważniejsze zagadnienia dotyczące bezpie-

czeństwa antyterrorystycznego budynków użyteczności publicznej. Położono większy nacisk na aspekty praktyczne z obszaru rozwiązań technicznych, prezentowane przez partnerów wydarzenia. Trzy październikowe dni upłynęły pod znakiem merytorycznych prelekcji, paneli dyskusyjnych i debat eksperckich, a także prezentacji nowoczesnych rozwiązań z zakresu bezpieczeństwa antyterrorystycznego. Innowacyjna formuła warsztatowa, jeszcze skuteczniej łącząca aspekty teoretyczne i praktyczne, spotkała się z pozytywnym odbiorem uczestników wydarzenia.

Dbamy o bezpieczne miasta

POZNAJ NASZ SYSTEM
DO INTELIGENTNEGO
MONITORINGU

Oferujemy w pełni Polskie rozwiązanie dla miast i gmin oparte na AI i Big Data.

Zapewniamy:

- otwarty model licencjonowania,
- zarządzanie ruchem drogowym,
- integrację społeczną,
- analizę obrazu i dźwięku,
- kontrolę jakości powietrza.

www.civileo.pl





SERWIS
INFORMACYJNY

www.aspolska.pl

Security BootCamp 2021

W październiku 2021 r. odbyła się druga edycja Security BootCamp, terenowego szkolenia dla specjalistów z branży security. Spotkanie pozwoliło podzielić się nowymi doświadczeniami, których przez trwającą pandemię COVID-19 jest coraz więcej. W pięknej jesiennej aurze hotelu Nosselia w Krzyczkach Szumnych można było zobaczyć i przetestować nowości technologiczne w rozwiązaniach security.

Drugi dzień szkolenia wypełniła gra strategiczna pt. „Incydent jak każdy inny... czyli jak ustrzec się kradzieży mienia, którego nigdy nie było w magazynie”. Poprowadził ją jej pomysłodawca Jacek Grzechowiak, Risk Response.

PARTNERAMI WYDARZENIA BYŁY FIRMY:

Axis Communications, Genetec, Nedap Security Management, Novatel oraz Securitas Polska.

Mariusz Kucharski

a&s Polska

→ Security BootCamp jest drugą edycją wydarzenia dla szefów bezpieczeństwa, security menedżerów z największych w Polsce firm i instytucji. To wspaniała zabawa, świetna integracja, mnóstwo kontaktów biznesowych, branżowych i merytorycznych. W spotkaniu wzięło udział 60 uczestników – specjalistów ds. security oraz 5 partnerów technologicznych. Dziękujemy wszystkim za przybycie. Dziękujemy za wspaniałe warsztaty merytoryczne. Dziękujemy za świetną zabawę.

Mariusz Bak

Securitas Polska

→ Na naszym stoisku klienci i partnerzy mieli okazję zobaczyć najnowszą technologię firmy Thruvision. Jest to przesiewowe skanowanie osób, bezpieczne dla zdrowia. Umożliwia wykrycie większego spektrum niebezpiecznych przedmiotów, nie tylko metalowych. Wieczorem zorganizowaliśmy prezentację rozwiązania MobileCam, mobilnej platformy monitoringu, autonomicznego rozwiązania, które możemy stosować w miejscach, gdzie nie ma żadnej infrastruktury technicznej.

Bogumił Szymanek

Axis Communications

→ Pokazywaliśmy najnowsze technologie z oferty Axis Communications, m.in. kamerę termowizyjną z najnowszym oprogramowaniem Axis Perimeter Defender. Uczestnicy wydarzenia mogli również przetestować kamerę obrotową PTZ z technologią Quick Zoom. Kamera potrafi poniżej jednej sekundy przejść do każdej krotności zoomu, nawet na duże odległości. Za jej pomocą jesteśmy w stanie odczytać tablice rejestracyjne z odległości nawet 150 m.

Anna Twardowska

Nedap Security Management

→ Omówiliśmy funkcje, którymi powinien cechować się dobry system kontroli dostępu. Dużo było tematyki związanej z cybersecurity w naszych rozwiązaniach, a także o tym, jak kopiujemy dobre praktyki ze świata IT do naszych rozwiązań. Ciekawym elementem był quiz przygotowany dla uczestników, który wzbudził w drużynach ducha rywalizacji, a przy tym była to świetna zabawa w miłej atmosferze.

Adam Gregorczyk

Novatel

→ Z udziałem naszych partnerów technologicznych firm Zenitel, Hytera, Vokkero prezentujemy i pokazujemy systemy, które wspierają podstawowy zmysł człowieka, jakim jest słuch.

Tomasz Nawrat

Genetec

→ Na stoisku testowaliśmy nasze oprogramowanie. Przy dużej liczbie zdarzeń, które niekoniecznie muszą być fałszywe, doprowadziliśmy do tego, aby operator systemu, który dzisiaj jest przytłoczony wielką liczbą fałszywych alarmów, miał możliwość reagowania tylko na te incydenty, które są faktycznie prawdziwe.

Jacek Grzechowiak

Risk Response

→ Dzisiejsza gra decyzyjna dotyczyła tematu, który roboczo nazwałem *Jak uchronić się przed kradzieżą mienia, którego nigdy nie było w magazynie*. Warsztat był przeznaczony dla security menedżerów i osób zajmujących się bezpieczeństwem, a wszystko odbyło się pod hasłem: nic nie jest tym, czym się wydaje.

Ryszard Kozłowski

Straż Miejska w Łodzi

→ Wspaniałe okoliczności przyrody, wspaniała pogoda, mnóstwo nowych znajomości i dobrej wiedzy, którą mam nadzieję będziemy wykorzystywać w codziennej służbie.

Paweł Pęchorzewski

Zalando

→ Oczywiście bardzo dużą wartością była możliwość poznania różnego rodzaju rozwiązań technicznych, zabezpieczeń technicznych używanych w bezpieczeństwie.

Piotr Rusin

Autostrada Eksploatacja

→ Przyjechałem, ponieważ w ciągu dwóch lat od ostatniego spotkania bardzo dużo zmieniło się w technice zabezpieczeń.

Paweł Macheta

Goodyear Dębica

→ Bardzo fajna impreza, bardzo skuteczna i wszystkim polecam.

Janusz Syrówka

innogy Polska

→ Najistotniejszą dla mnie kwestią była możliwość rozmawiania z ludźmi z branży, poznania się, wymiany doświadczeń, opinii, pożartowania.



SICUREZZA 2021

380 wystawców z 27 krajów, ponad 50 szkoleń w ciągu trzech dni! Kolejna edycja targów Sicurezza w Mediolanie przechodzi do historii. Zostanie zapamiętana jako szczególna i wyjątkowa, organizatorzy zadbali bowiem, by odbywała się w świecie „nowej normalności”. Nie zabrakło nowinek technologicznych, zaawansowanych technicznie rozwiązań dostępnych na rynku, potwierdzających i wyznaczających najnowsze trendy. Wszystko to przy aromatycznej włoskiej kawie...

↓ Sicurezza to jedno z największych wydarzeń biznesowych dla branży security. Obecność firm z całego świata i bogata oferta produktów, usług i innowacyjnych rozwiązań gwarantują rozmach i różnorodność ekspozycji. Odbywająca się co dwa lata impreza odpowiada na wyzwania stojące przed branżą, a także potrzeby wystawców i licznych zwiedzających. Tak było i tym razem! Trzy targowe dni były wypełnione atrakcyjną tematyką: od przewidywania trendów rynkowych, przez wskazówki techniczne i regulacyjne, po nowości produktowe prezentowane na stoiskach firmowych. Wszystkie wydarzenia miały wspólny cel: zapewnić profe-

sjonalistom solidne wsparcie i rozwinięcie konkretnych umiejętności. I choć wiedza techniczna oraz znajomość wytycznych i przepisów są kluczowe, same w sobie nie wystarczą, aby zagwarantować wzrost przychodów. Impreza pozwoliła ponownie odkryć wagę bezpośrednich relacji międzyludzkich na żywo. Największą grupą wystawców, z oczywistych względów, były firmy rodzime. Uwagę przyciągały stoiska producentów systemów alarmowych – firmy Tecnoalarm SRL i Nicom Secualarm SRL. Udało nam się porozmawiać z wiodącą nie tylko na włoskim rynku elektroniki, ale także w Europie i na świecie firmą MASTER Living Technology.

– Od prawie 40 lat znani jesteśmy z jakości, badań, innowacji, komunikacji. Cały czas staraliśmy się nadążać za potrzebami rynku i elastycznie dostosowywać się do wymagań. Cieszymy się, że po raz kolejny z dumą możemy prezentować nasze usługi na Sicurezza i nawiązać kolejne kontakty! – mówi Marco Balossini, starszy programista w MASTER Living Technology. Nie zabrakło światowych marek, np. Milestone Systems, Axis Communications, Salto czy Selcom. – Na rynku działamy od prawie 20 lat. Na targach Sicurezza jesteśmy po raz pierwszy. To dla nas kolejna świetna okazja, aby pokazać się szerokiemu gronu specjalistów, mimo że jeste-

śmy znani na całym świecie. Jest bardzo duże zainteresowanie naszymi rozwiązaniami i oczekiwanie na kolejne nowości – podkreśla Natacha Fernandes, kierownik Działu Marketingu w Selcom. Wśród wystawców były również polskie firmy: Grenton, Merawex, Pulsar, P-Audio Technologies i Somblas. Rozmawialiśmy z przedstawicielami czterech z nich.

Marta Lipiec-Pannazzolo, Grenton

Jesteśmy producentem systemów smart home, czyli automatyki domowej. Dzięki naszym produktom dom może być wygodniejszy, bezpieczniejszy i bardziej oszczędny. Na Sicurezza obserwujemy duże zainte-

resowanie naszymi produktami. Cieszymy się, że mogliśmy wrócić na targi, nawiązać nowe kontakty i przede wszystkim być blisko rynku, bo to jest dla nas najważniejsze.

Bogdan Krzyścik, Merawex

Z mojej obserwacji wynika, że na tegorocznej edycji jest mniej stanowisk niż w poprzednich latach. Co nie zmienia faktu, że ludzi zainteresowanych jest sporo, zwłaszcza że każdy jest ciekawy, jak to wygląda po pandemii. Mamy dużo zapytań odnośnie do zasilaaczy do systemów ppoż., systemów alarmowych i kontroli dostępu. Poza tym ludzie są spragnieni kontaktów bezpośrednich, nie wszystko możemy zrobić zdalnie. Cieszymy się, że wróciliśmy, próbujemy i działamy dalej!

Natalia Wciśło, Pulsar

Jesteśmy obecni już na kolejnej edycji i cieszymy się, że mimo restrykcji i trudnych czasów mogliśmy znowu tu-

taj się pojawić. Sicurezza stała się na wysokości zadania – wszystko jest bardzo profesjonalnie i dobrze zorganizowane. Pandemia nie była dla nas łaskawa, tak jak dla większości firm. Na początku było ciężko, ale już się odbijamy i wierzymy, że będzie coraz lepiej!

Jakub Kaszyca, P-Audio Technologies

Mam przyjemność być na targach po raz pierwszy i nie ukrywam, że to, co się dzieje tutaj, przerosło moje oczekiwania. Jest mnóstwo ludzi i bardzo duże zainteresowanie. SICUREZZA daje duży zastrzyk motywacji do działania! ☺

Czasopismo „a&s Polska” było oficjalnym patronem medialnym targów.

Zapraszamy do obejrzenia fotorelacji na portalu aspol-ska.pl. Tekst i fot. Michalina Nowak

Advisor Management

Zintegrowane środowisko obsługi systemów bezpieczeństwa



Innowacyjny



Skuteczny



Idealny dla klienta

Aritech jest globalną marką firmy Carrier reprezentującą rozwiązania zabezpieczeń dla klientów prywatnych, komercyjnych i korporacyjnych. Oferujemy zintegrowaną platformę bezpieczeństwa w obszarze systemów alarmowych, kontroli dostępu, wideo i wykrywania pożaru. Aritech cieszy się zaufaniem klientów od ponad 40 lat.

Odwiedź: pl.firesecurityproducts.com



Nowości w ofercie Axis



Axis Scene Intelligence i udoskonalona wersja Smart Search

Dwie innowacje umożliwiają połączenie analiz wideo wykonywanych na brzegu sieci i serwerze oraz metod głębokiego uczenia. Technologia Axis Scene Intelligence zapewnia wydajniejszą, bardziej precyzyjną detekcję i klasyfikację obiektów. Z kolei dzięki udoskonalonej wersji funkcji Smart Search przeszukiwanie baz danych jest proste i szybkie.

↓ Technologia Axis Scene Intelligence (ASI) wykorzystuje opracowany przez firmę procesor ze specjalną jednostką wyposażoną w funkcje głębokiego uczenia. Dzięki temu można tworzyć wydajniejsze narzędzia analityczne pracujące na brzegu

sieci. ASI wykorzystuje do analiz algorytmy sprawdzone i wytrenowane w rzeczywistych środowiskach i dostarcza wiarygodne metadane nawet w najtrudniejszych warunkach dozoru (np. słabe oświetlenie czy szeroki zakres dynamiki ruchu obiektu), znacząco ograniczając fałszywe alarmy.

Wraz z ASI oferowana jest zaktualizowana wersja funkcji Smart Search, dostępna w oprogramowaniu do zarządzania materiałem wizyjnym AXIS Camera Station. Smart Search 2 wykorzystuje dane nt. ruchu obiektów pochodzące z obrazów kamery Axis, przetwarzane przy użyciu mechanizmów uczenia maszynowego i głębokiego uczenia. Przyspiesza to klasyfikację takich obiektów, jak osoby, samochody osobowe i ciężarowe, rowery, przy lepszej identyfikacji kolorów. Najnowszą wersję AXIS Camera Station, zawierającą funkcję Smart Search, można pobrać ze stron Axis Communications.  Więcej na: www.axis.com/pl

To czego szukasz jest bliżej, niż myślisz!

Koniec z marnowaniem czasu na wielogodzinne przeglądanie nagrań z monitoringu. Oparty na BriefCam – XProtect Rapid REVIEW pozwoli skrócić ten czas do zaledwie kilku minut.

↓ Nowe rozwiązanie Milestone Systems umożliwia szybkie i inteligentne analizowanie materiałów wideo. Wynik analizy to konkretne ujęcia pokazujące m.in. podejrzany pojazd, osobę czy tablicę rejestracyjną. Korzystanie z XProtect pozwala zidentyfikować podejrzany samochód, ustalić dokładny czas i miejsce przebywania obiektu/osoby, co w przypadku zaginionych dzieci jest kluczowe w śledztwie. Oprogramowanie może sprawdzić się także w środowisku pracy, gdy przykładowo chcemy zlokalizować osoby bez maseczki.



XProtect Rapid REVIEW to analityka danych wizyjnych wykorzystująca już istniejące sieci monitoringu wizyjnego. Za pomocą sztucznej inteligencji połączonej z *deep learning* XProtect Rapid REVIEW wykrywa poszukiwane osoby lub rzeczy w nagranych i odtwarzanych materiałach z wielu kamer. Zaawansowana technologia VIDEO SYNOPSIS® umożliwia operatorowi jednocześnie wyodrębnić obiekt, który pojawił się w różnych momentach nagrania.

– Chcieliśmy umożliwić firmom i rządowi pełen wachlarz możliwości wykorzystania materiałów z monitoringu wizyjnego. Analityka danych może znacznie przyspieszyć śledztwa, pomoże też, gdy borykamy się np. z niedoborem operatorów – powiedział Björn Skou Eilertsen, dyrektor ds. technologii w Milestone Systems. XProtect Rapid REVIEW to dodatkowy produkt, który jest płynnie zintegrowany z Milestone XProtect Smart Client. Nowe rozwiązanie XProtect Rapid REVIEW jest dostępne od 30 listopada.  Więcej na www.milestonesys.com/

Bezpieczeństwo cybernetyczne

identyfikatorów zblizeniowych



Identyfikatory zbliżeniowe stanowią kluczowy element bezpieczeństwa cybernetycznego systemu kontroli dostępu. Najpopularniejszą grupą identyfikatorów zbliżeniowych są identyfikatory standardu EM 125 kHz, które nie są w żaden sposób zabezpieczone cybernetycznie i mogą być kopiowane przy użyciu łatwo dostępnego sprzętu lub przez osoby świadczące tego rodzaju usługi.

↓ Drugą grupą powszechnie wykorzystywanych identyfikatorów są identyfikatory standardu 13,56 MHz MIFARE®. Występuje tu wiele odmian identyfikatorów różniących się technologią przechowywania danych na karcie. Systemy KD mogą odczytywać z identyfikatora MIFARE® tzw. numer seryjny (skr. CSN) lub numer zaprogramowany w pamięci karty (skr. SSN). Numer CSN jest nieszyfrowany i może być powielany. Numer SSN jest szyfrowany za pomocą indywidualnie ustawianych haseł i przez to jest zabezpieczony przed kopiowaniem.

W odniesieniu do kart standardu MIFARE® należy mieć na uwadze:

- Wykorzystanie numeru CSN karty MIFARE® nie chroni przed kopiowaniem. Uwaga ta dotyczy wszystkich rodzajów odmian kart MIFARE®
- Wykorzystanie numeru SSN karty MIFARE® wymaga stosowania czytników obsługujących szyfrowane sektory karty SSN
- Większość dostępnych na rynku czytników standardu MIFARE® nie oferuje obsługi szyfrowanych sektorów karty, a jedynie odczyt nieszyfrowanego numeru CSN
- Czytniki MIFARE® marki Roger mają możliwość odczytu szyfrowanego numeru karty MIFARE® (SSN)
- Wykorzystanie numeru SSN karty wymaga odpowiedniej konfiguracji czytników w systemie KD
- Nie są jeszcze znane metody złamania zabezpieczeń kart MIFARE® DESFire® oraz MIFARE Plus® pracujących w trybie SL3

Stosowanie kart MFC-4 (MIFARE® DESFire®) lub MFC-7 (MIFARE Plus®) i obsługujących je czytników Roger zapewnia najwyższy poziom cyberbezpieczeństwa.  Lista czytników na www.roger.pl



POLON-ALFA

Tradycja I NOWOCZESNOŚĆ



- NAJWIĘKSZY POLSKI PRODUCENT KOMPLEKSOWYCH SYSTEMÓW SYGNALIZACJI POŻAROWEJ I APARATURY RADIOMETRYCZNEJ
- PONAD 60 LAT DOŚWIADCZENIA
- SZEROKA GAMA INNOWACYJNYCH ROZWIĄZAŃ W ZAKRESIE OCHRONY PRZECIWPOŻAROWEJ
- NOWOCZESNE URZĄDZENIA OPRACOWYWANE PRZEZ ZESPÓŁ WYKWALIFIKOWANYCH I KOMPETENTNYCH INŻYNIERÓW
- SPECJALISTYCZNE SZKOLENIA I WSPARCIE TECHNICZNE DLA PROJEKTANTÓW ORAZ INSTALATORÓW W KRAJU I ZA GRANICĄ

AVUTECH + BRIVO

= przyszłość integracji

Innowacyjny system rozpoznawania tablic rejestracyjnych producenta AVUTECH jest naszą odpowiedzią na rosnące zapotrzebowanie polskiego rynku. Kamery AVUTECH serii X połączone z platformą CORTEX CLOUD znajdują zastosowanie m.in. w systemach parkingowych, smart city, logistyce, gdzie zwiększają bezpieczeństwo, wygodę lub usprawniają zarządzanie ruchem pojazdów i osób.

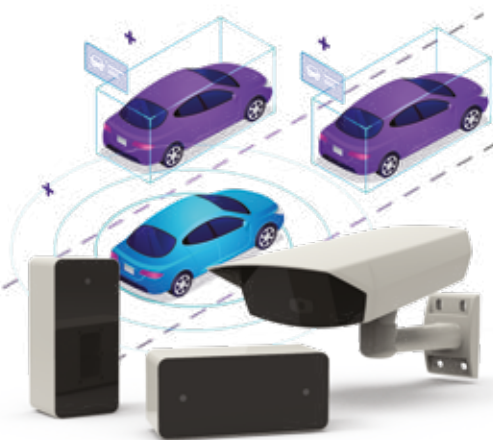
↓ Kamery, wykorzystując ogromną moc przetwarzania neuronowego, wykonują równolegle różne zadania uczenia maszynowego, np. odczytują tablice rejestracyjne pojazdów i śledzą ruch osób. Mogą pracować

samodzielnie lub jako zintegrowane z dowolnym systemem KD, np. Brivo. Oprogramowanie CortexFramework AVUTECH po rozpoznaniu tablicy rejestracyjnej dokonuje konwersji danych do 26-bitowego formatu Wie-

gand obsługiwane przez system Brivo Onair. Dzięki temu w jednej aplikacji można łatwo i szybko wyszukiwać zarówno osoby wchodzące do budynku, jak i pojazdy wjeżdżające i wyjeżdżające z parkingu.

Można też tworzyć zbiorcze raporty ze wszystkich zdarzeń. Siłą silnika CortexFramework jest duża elastyczność i możliwość integracji także z systemami VMS, POS czy PSIM. ☉

Więcej na: www.smart-i.pl



CZY TWÓJ SYSTEM MONITORINGU

zasługuje na 5 gwiazdek?

Wysoka jakość, stabilność działania oraz wiele usług w jednym, doskonałym rozwiązaniu IP – ADPRO eFT by Xtralis by Honeywell. To rozwiązanie oferuje pełny dostęp zdalny dla takich funkcji rejestratora, jak uzbrajanie/rozbrajanie, zdjęcia w formacie QUAD czy wysoka stabilność działania, wykorzystując własny protokół komunikacyjny.

↓ Technologia zastosowana w eFT w celu zapewnienia możliwie najwyższej jakości nagrywania optymalizuje przesyłanie obrazu poprzez wielostrumieniowy transfer danych z kamer, dostosowując transmisję wizji do danego łącza. eFT jest dostępne w wersji z 8 kanałami wideo i 8 kanałami analitycznymi.

Detekcja wtargnięć jest kluczowa w ochronie perymetrycznej, a firma Xtralis może zaoferować jedno z najbardziej skutecznych rozwiązań w tym zakresie. Wysoką wydajność detekcji zapewnia analiza wideo IntrusionTrace przystosowana do pracy na zewnątrz, 24h na dobę, 365 dni w roku. Niezawodność, precyzję detekcji i praktycznie minimum fałszywych alarmów zawdzięcza analizie tysięcy godzin materiałów wideo z różnych okresów i miejsc. Dzięki prostej konfiguracji chronionej strefy ta wideoanaliza może być wykorzystane w wielu różnych lokalizacjach.

Przez lata rozwijane algorytmy analizy wizyjnej zapewniają skuteczną ochronę obiektów nawet w trudnych warunkach. Oprogramowanie ADPRO VCP umożliwia obsługę alarmów z wielu obiektów w centrum monitorowania alarmów. Co ma znaczenie, wideoanaliza ADPRO by Xtralis by Honeywell jest kompatybilna z większością popularnych kamer. Wszystko w sposób łatwy i skuteczny. ☉

Więcej na: www.linc.pl

Moduł CCTV i MOBILE

w systemie integrującym ARGUS



Poznańska firma Telbud SA jest producentem platformy integrującej systemy ochrony technicznej ARGUS klasy SMS/PSIM.

↓ ARGUS jest sprawdzonym rozwiązaniem pod względem bezpieczeństwa i stabilności pracy. Działa obecnie m.in. w obiektach infrastruktury krytycznej, które charakteryzują się dużym rozproszeniem terytorialnym i brakiem ograniczeń co do liczby integrowanych obiektów i systemów.

Platforma ARGUS ma opcjonalnie dołączane moduły ARGUS CCTV i ARGUS MOBILE.

ARGUS CCTV umożliwia zaawansowane sterowanie sygnałami z kamer dozoru. Sterowanie odbywa się bezpośrednio z interfejsu użytkownika. Pozwala też m.in. na wyświetlanie obrazów na wielu monitorach, śledzenie sytuacji alarmowych, odtwarzanie zdarzeń czy tworzenie kopii zapasowych.

Z kolei ARGUS MOBILE to moduł przeznaczony do urządzeń mobilnych iOS lub Android. Oferuje takie funkcjonalności, jak podgląd zdarzeń i sterowanie. Oprogramowanie mobilne umożliwia też uruchomienie funkcji, które doprowadzają użytkownika do wskazanego miejsca na mapie obiektu. ☉

Więcej na: www.telbud.pl

Konkurencja płakała, gdy się dowiedziała ;)



Najnowsza centrala sterująca urządzeniami przeciwpożarowymi Integral EvoX M.

świadcstwo dopuszczenia CNBOP-PIB

Drodzy Partnerzy, Klienci, Przyjaciele i wszyscy sympatycy naszej firmy, z okazji Świąt Bożego Narodzenia życzymy Państwu przede wszystkim zdrowia, spokoju i chwil wytchnienia w gronie najbliższych.

Dziękujemy za wspólne działania w mijającym roku życząc, aby rok 2022 przyniósł upragnioną stabilizację, równowagę i był pełen sukcesów.

Życzymy Państwu bezpiecznego Nowego Roku!

Zespół Schrack Seconet Polska Sp. z o.o.

**SCHRACK
SECONET**



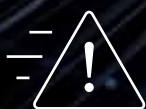
ReX 2

Podwajacz zasięgu sygnału radiowego z obsługą fotograficznej weryfikacji alarmów



2
GRADE
EN 50131

PD 6662
2017



Wysyła alarmy
w 0,3 sekundy



Komunikacja
na odległość
do 1700 m

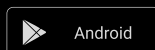
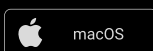


Przesyła zdarzenia i
wizualną weryfikację
alarmów



Obsługuje połączenie
przez router

Darmowe aplikacje dla instalatorów i
użytkowników końcowych
ajax.systems



Milego oglądania

