

SECURITY 50

**NAJWIĘKSZE
FIRMY SECURITY
NA ŚWIECIE**

Rok 2022 przyniósł wyraźny wzrost przychodów w większości firm z listy Security 50, jednak kończy się problemami globalnymi, które dla branży security mogą w nadchodzącym roku stanowić zarówno duże wyzwania, jak i nowe możliwości.

RYNEK SECURITY

**ZARZĄDZANIE
PROJEKTEM**

Realizacja projektu elektronicznego systemu zabezpieczeń nie jest zadaniem łatwym. Jak każdy długofalowy proces warto podzielić go na etapy. Pomocne są nowe technologie, możliwości usprawniania procedur oraz generowania oszczędności.

**BEZPIECZEŃSTWO
W HANDLU**
**RODZINNE FIRMY
HANDLOWE**

Firmy rodzinne funkcjonujące w handlu detalicznym to z perspektywy branży security niezwykle interesujący obszar. W czasach niestabilności i petzającego kryzysu, którego symptomem są nasilające się kradzieże w sklepach, wymagają one wzmożonej ochrony.

ISSN 2451-5175

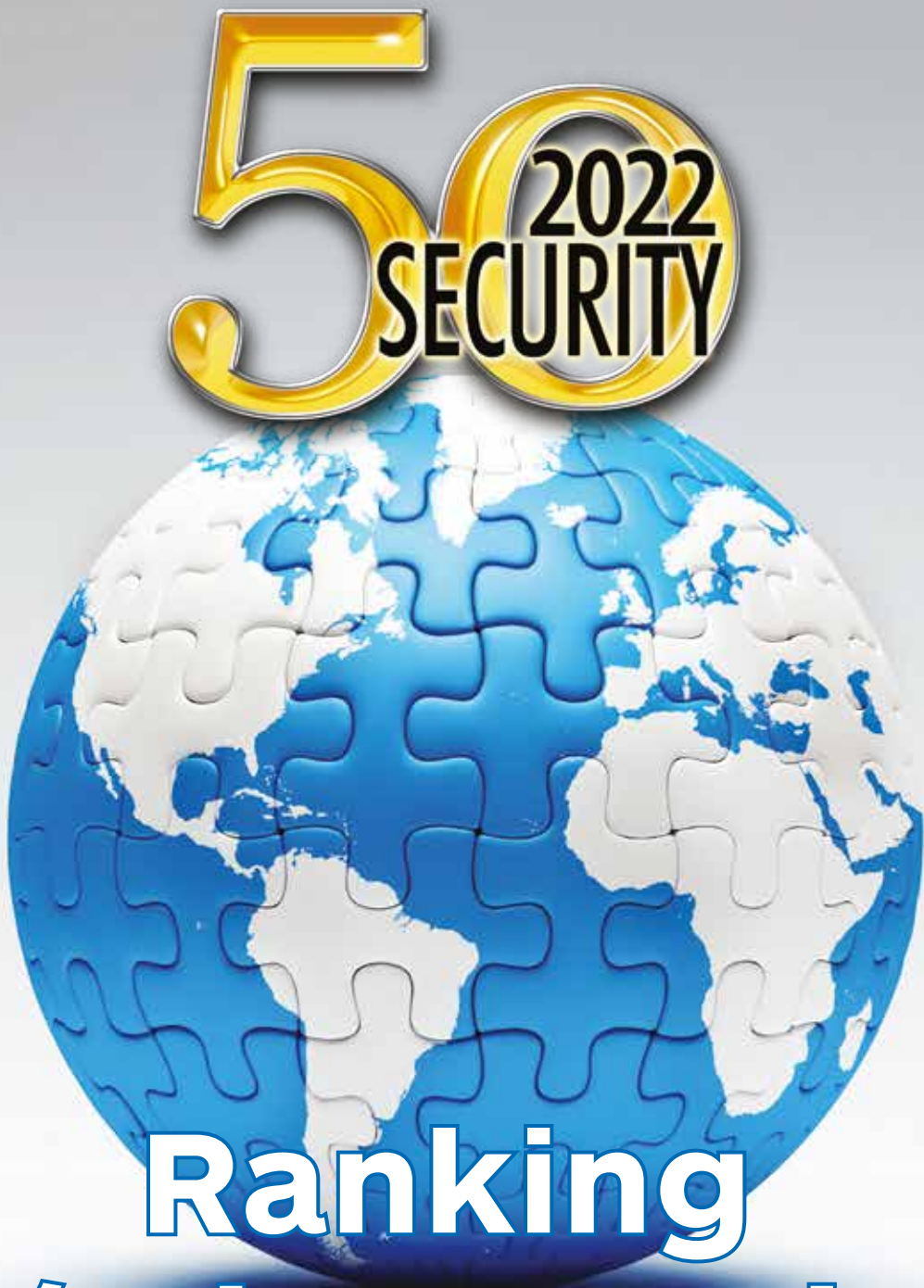


9 772451 517703



15 zł

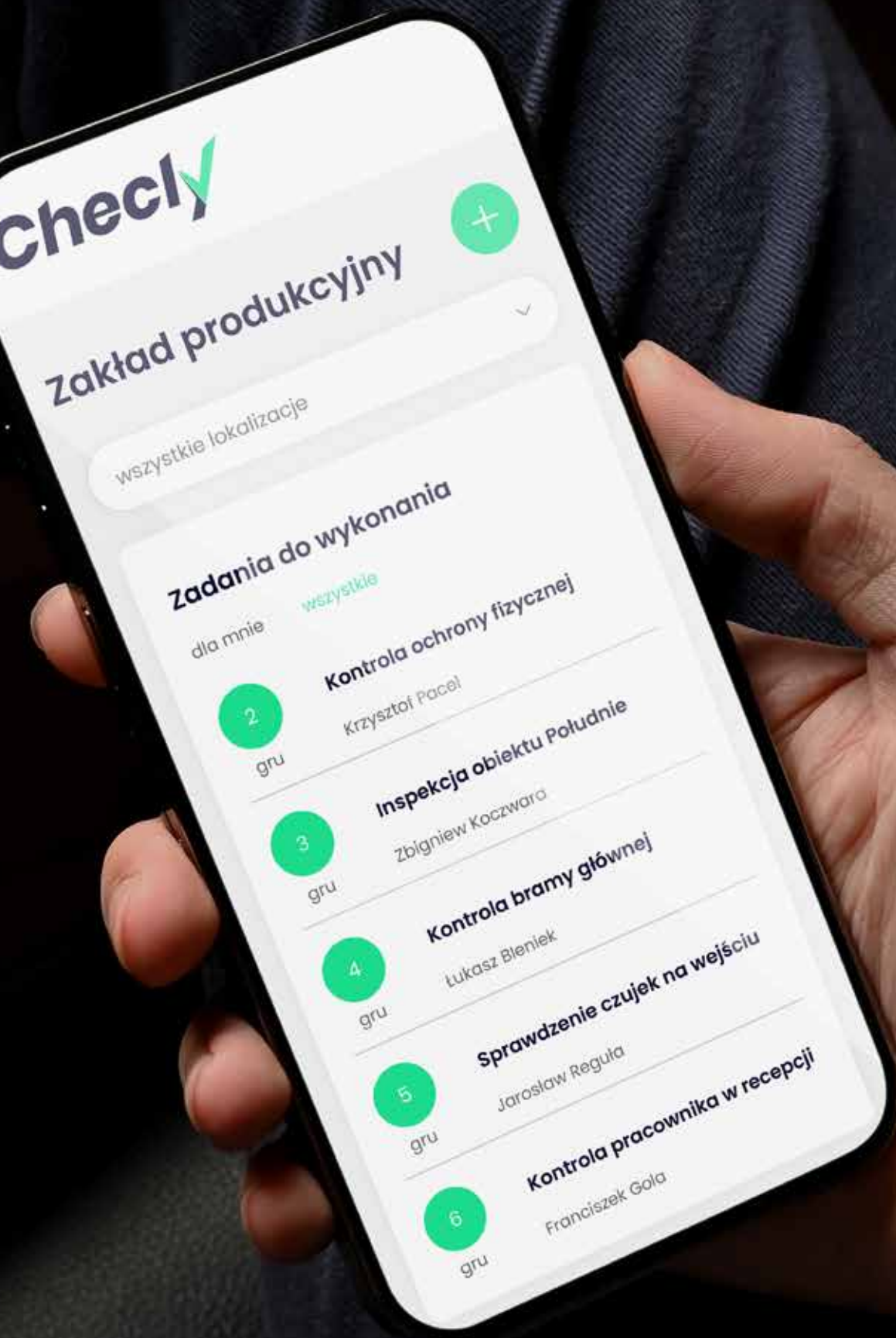
(w tym 8% VAT)



Ranking światowych liderów

 APLIKACJA
MOBILNA


check. create. manage.



checlly.app

Checly

Drodzy Czytelnicy

Tradycyjnie, jak co roku, numer listopadowo-grudniowy rozpoczynamy rankingiem największych firm security na świecie i raportem dotyczącym kondycji rynku przygotowanym przez asmag.com. Pomimo poważnych napięć geopolitycznych i handlowych (USA-Chiny) oraz ograniczeń dostaw podzespołów dla większości organizacji rok 2022 był udany. W tegorocznym zestawieniu największe firmy utrzymały swoje pozycje z poprzedniego roku (s. 38).

W odbudowujący się po pandemii rynek globalny uderzyła wojna w Ukrainie, pojawiły się kolejne problemy, np. długotrwały niedobór chipów spowodowany m.in. wzrostem popytu, co sprawiło, że rynki stały się niestabilne. Niedostateczne dostawy były i są poważnym wyzwaniem dotyczącym też graczy z naszej branży. Kondycję firm zabezpieczeń elektronicznych w poszczególnych regionach świata omawiamy na s. 14. Nas najbardziej zainteresowała sytuacja w Europie. Tu również odnotowano wzrost, który powinien być kontynuowany w przyszłym roku, chociaż inflacja powodująca wzrost kosztów gazu, energii i żywności, czynszów i kredytów hipotecznych dotknęła kraje EMEA, podobnie jak resztę świata. Szczegółowo omawiamy globalny rynek kontroli dostępu i telewizji dozorowej (s. 20).

W 2022 r. postępowała cyfrowa transformacja w obszarze systemów VSS i KD. Inwestycje w odpowiednią technologię przekształcają systemy z reaktywnych w proaktywne, umożliwiają nowe zastosowania oraz pomagają organizacjom działać bardziej optymalnie, wydajnie i bezpiecznie. O trendach, które wg ekspertów z firm badawczych i stowarzyszeń pojawią się na rynku security w 2023 r., piszemy na s. 26. Pod względem technologicznym nadal dominowały sztuczna inteligencja i cyberbezpieczeństwo. Po latach nadmiernego szumu wokół AI rozwiązania nią wspierane stają się coraz bardziej opłacalne biznesowo. Sztuczna inteligencja będzie odgrywać większą rolę w obszarze bezpieczeństwa IT – zarówno zagrażających cyberataków, jak i w ochronie przed nimi. A cyberprzestępcy są dziś coraz bardziej aktywni, stosują wysoko zaawansowane narzędzia i najnowsze technologie.

Na s. 32 prezentujemy wyniki badania przeprowadzonego przez portal asmag.com, w którym pytano o dojrzałość i przydatność wdrożeniową technologii. W tym roku wśród technologii dojrzałych i odpowiednich znalazły się: pamięć i analityka w urządzeniach brzegowych, chmura hybrydowa i komunikacja 5G. Za najbardziej dojrzałe i popularne rozwiązanie ankietowani uznali identyfikację wieloelementową.

Na podstawie listy Security 50 widać, że rynek security rośnie, w 2022 r. większości firm odnotowała wzrost przychodów. Jednak rok kończy się problemami, które w przyszłości będą stanowić poważne wyzwania (s. 40).

Pomimo niestabilnej sytuacji życzymy całej branży, aby rok 2023 był udany. Dostawcom systemów zabezpieczeń życzymy jak najmniej opóźnień, integratorom jak najwięcej zakończonych sukcesem projektów, a klientom końcowym jak najmniej przeszkód w prowadzeniu działalności. A przede wszystkim zdrowych i bezpiecznych świąt Bożego Narodzenia i całego roku 2023!

Marta Dynakowska
REDAKTOR NACZELNA

Jan T. Grusznick
Z-CARREDAKTORA NACZELNEGO

Mariusz Kucharski
PREZES ZARZĄDU



REDAKCJA

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
Michalina Nowak

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 Wnęk
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 POLSKA
ZŁOTY PARTNER



SREBRNY PARTNER



A & S POLSKA
WYDANIE
ONLINE

www.aspolska.pl/czasopismo

8 Produkty numeru



- 14** Branża zabezpieczeń elektronicznych w 2022 r. – analiza rynku wg regionów
- 20** Kontrola dostępu i telewizja dozorowa – kondycja globalnego rynku w 2022 roku
- 26** Badania rynku i komentarze branży
- 32** Badanie dojrzałości i przydatności technologii w 2022 r.
- 38** Security TOP 50 – zestawienie największych firm
- 40** Security 50: TOP 10 producentów z sektora telewizji dozorowej i kontroli dostępu

**BEZPIECZEŃSTWO
W HANDLU**

- 46** Handel przyszłości na wyciągnięcie ręki
MICHAŁ MARCINIAK
- 48** Bezpieczeństwo firm rodzinnych. Odcinek 1. Handel detaliczny
JACEK TYBUREK
- 52** Analityka w handlu detalicznym – więcej cennych informacji niż można się spodziewać
AXIS COMMUNICATIONS
- 54** HikCentral dla sieci handlowych
ARMEN MOSKA, HIKVISION POLAND
- 56** Głos Branży – bezpieczeństwo w handlu



*Pragniemy serdecznie podziękować
wszystkim naszym Partnerom,
Klientom i Sympatykom
za zaufanie i współpracę.
Życzymy dalszych sukcesów,
udanych inwestycji
i pomyślności w nadchodzącym
Nowym 2023 Roku*



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





RYNEK SECURITY

- 60** Zarządzanie projektem. Cz. 2. Poszczególne etapy
TOMASZ DACKA
- 64** Rozwiązania security w obiektach muzealnych
HUBERT ŻAK
- 66** Czy „Dama z gronostajem” jest w niebezpieczeństwie? Branża ochrony w trudnej sytuacji
POLSKI ZWIĄZEK PRACODAWCÓW OCHRONA
- 68** Metody komunikacji central alarmowych Galaxy Dimension
TOMASZ GÓRSKI, TAP SYSTEMY ALARMOWE
- 70** Modelowe zabezpieczenie techniczne centrum danych. Nedap Security Management w Data Center Talex
ANNA TWARDOWSKA, NEDAP SECURITY MANAGEMENT
- 72** Pod ziemią może być bezpieczniej
EWELINA DEMBIŃSKA, C&C PARTNERS
- 73** Wytyczne 2N dotyczące automatyki domowej 2N
- 74** Innowacyjne rozwiązania biometryczne
MAREK PIOTROWSKI, ZKTECO
- 76** 35 lat temu zaczęła się nasza historia
TELBUD

BEZPIECZEŃSTWO BIZNESU

- 78** System Zarządzania Ciągłością Działania (BCMS). Część 7. Kolejne kroki – Etap 2. Przeglądy, testy i budowanie świadomości
TOMASZ GUZIKOWSKI



BEZPIECZEŃSTWO POŻAROWE

- 82** Nieprecyzyjne Warunki Techniczne. Czy to rzeczywiście przeszkoda w procesie sprawnego projektowania?
MICHAŁ ZALEWSKI
- 84** Instrukcja Bezpieczeństwa Pożarowego – element systemu zarządzania kryzysowego
ŁUKASZ STĘPIEŃ
- 88** Bezpieczeństwo i ochrona przeciwpożarowa budynków. Ewakuacja w technologii VR
MAŁGORZATA REJMAN, SECURITAS POLSKA



SERWIS INFORMACYJNY

- 90** IX edycja Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy – podsumowanie
SCHRACK SECONET POLSKA
- 94** Jesienny BootCamp
- 96** Informacje firmowe/nowości rynkowe



**Polskie profesjonalne
zintegrowane rozwiązania
VMS**

**Ponad 200 000 instalacji
na całym świecie
Jesteśmy z Wami od
2003 roku**



www.alnetsystems.com

www.axis.com/pl

AXIS M5000-G – wewnętrzna kamera PTZ

OD BANKÓW PO SKLEPY DETALICZNE, M5000-G PTZ JEST IDEALNA DO WIELU RÓŻNYCH ZASTOSOWAŃ WEWNĘTRZNYCH.

↓ Ta kamera o rozdzielczości 15 Mpix jest wyposażona w trzy 5-Mpix przetworniki obrazu i jeden moduł PTZ z zoomem optycznym x10, zapewniającym pełną świadomość sytuacyjną, a także w bezprzewodową łączność we/wy z urządzeniami Z-Wave Plus® w pomieszczeniach do 400 m². Jest wyposażona w światła sygnalizacyjne, pomocne w powstrzymaniu zachowań antyspołecz-

nych i przestępczych – idealne rozwiązanie dla sklepów detalicznych i dużych obszarów wewnątrz budynków. Bezprzewodowa łączność we/wy z urządzeniami Z-Wave Plus® oznacza, że kamera może komunikować się z maks. sześcioma urządzeniami w konfiguracji systemu. Gdy np. zostaną otwarte drzwi lub okno, urządzenie automatycznie powiadomi kamerę o zmianie jej

wstępnie ustawionej pozycji. Nie trzeba też ręcznie włączać światła, ogrzewania lub klimatyzacji – można użyć Z-Wave Plus do ich automatycznego aktywowania. Zastosowana w obiektach handlu detalicznego pozwala np. monitorować temperaturę w zamrażarkach. Wszystkie informacje z Z-Wave są przesyłane do systemu VMS i wyświetlane jako nakładki w strumieniu wizji.

Jedna kamera AXIS M5000-G daje takie korzyści, jak zastosowanie czterech innych modeli. Wystarczy tylko jedna AXIS M5000-G, jeden kabel, jeden adres IP i jedna licencja na oprogramowanie do zarządzania wizją (VMS). Dzięki funkcji *edge storage* można nagrywać bezpośrednio na pokładową kartę pamięci kamery, co ułatwia instalację i konserwację.



www.bcsctv.pl

Kamera BCS-TIP7401ITC-III z funkcją ANPR

BCS-TIP7401ITC-III TO 4-MPIX KAMERA TRZECIEJ GENERACJI ROZPOZNAJĄCA TABLICE REJESTRACYJNE NADJEŻDŻAJĄCYCH POJAZDÓW, PRZEZNACZONA DO AUTOMATYZACJI WJAZDU NA TEREN OBIEKTU.



↓ Bez względu na to, czy będzie to centrum handlowe, park biznesowy, czy prywatna posesja, odpowiednio skonfigurowana kamera odczyta numer tablicy rejestracyjnej i na podstawie wcześniej zdefiniowanych scenariuszy zadecyduje, jakie działania podjąć. Jest wyposażona aż w trzy wyjścia alarmowe

i obiektyw motozoom o ogniskowej 10-50 mm, co umożliwia prawidłowe rozpoznanie tablic z odległości do 30 m. Ponadto kamera potrafi prawidłowo rozpoznać rejestrację nawet wtedy, kiedy pojazd porusza się z prędkością do 60 km/h, nie ma więc konieczności wymuszenia zatrzymania samochodu przed samą barierą, co jest jej dużym atutem. Natomiast na 4 kanałach potrafi pokazać pełnię swoich możliwości, oferując dostęp do takich funkcji, jak rozpoznawanie i identyfikacja twarzy czy gromadzenie metadanych, w których skład

wchodzi rozpoznawanie obiektów i informacji o nich. Kamera ma funkcje poprawiające jakość obrazu (WDR, HLC, ręczne ustawienia promiennika IR oraz migawki), aby nawet w mocno niesprzyjających warunkach skutecznie odczytać numer rejestracyjny. Wejście/wyjście audio umożliwia dwukierunkową komunikację audio między kamerą a operatorem, aby w razie potrzeby móc łatwo skontaktować się z kierowcą pojazdu oczekującego na wjazd. Kamerę można łatwo połączyć z rejestratorami IP BCS Line serii 4K lub aplikacją BCS Manager, zapewniając w ten sposób dodatkowe funkcjonalności, np. wyszukiwanie zdarzeń według rozpoznanych numerów rejestracyjnych, tworzenie raportów z zarejestrowanych zdarzeń bądź możliwość monitorowania trasy pojazdu.

www.ccpartners.pl

Nowa generacja kamer ANPR opartych na sztucznej inteligencji

RODZINA EUROPEJSKICH KAMER VEGA, DOSTĘPNYCH W 4 WARIANTACH (VEGA 10, 11, 30, 33), JEST PRZEZNACZONA DO BARDZO WYMAGAJĄCYCH ZASTOSOWAŃ.



↓ Rozpoznaje tablice rejestracyjne pojazdów poruszających się z prędkością do 180 km/h (Vega 10/11) oraz do 200 km/h do dwóch pasów jednocześnie (Vega 30/33) z skutecznością >99%. Jest urządzeniem bispiektralnym – oprócz kamery ANPR/LPR, zawiera drugą kamerę kontekstową.

Nowa, modułowa platforma STARK umożliwia tworzenie nowych, szytych na miarę aplikacji. Sztuczna inteligencja (AI) zapewnia klasyfikację typu pojazdu (np. motor, ciężarówka), detekcję mo-

delu, marki oraz koloru pojazdu. Dzięki protokołowi Wiegand, kamera jest gotowa do podłączenia do każdego systemu kontroli dostępu w roli inteligentnego czytnika.

Opcjonalnie może mieć wbudowane moduły WIFI/LTE/GPS. W jednej kamerze może być używanych jednocześnie wiele algorytmów LPR (OCR), w tym także firm trzecich.

RACS 5 v2

Polski system kontroli dostępu klasy Enterprise

Rozbudowana wizualizacja wektorowa w nowym module map

Obsługa systemów rozproszonych terytorialnie

Integracja z tradycyjnym systemem windowym

Integracja z serwerowymi systemami windowymi firm KONE, Schindler i innych

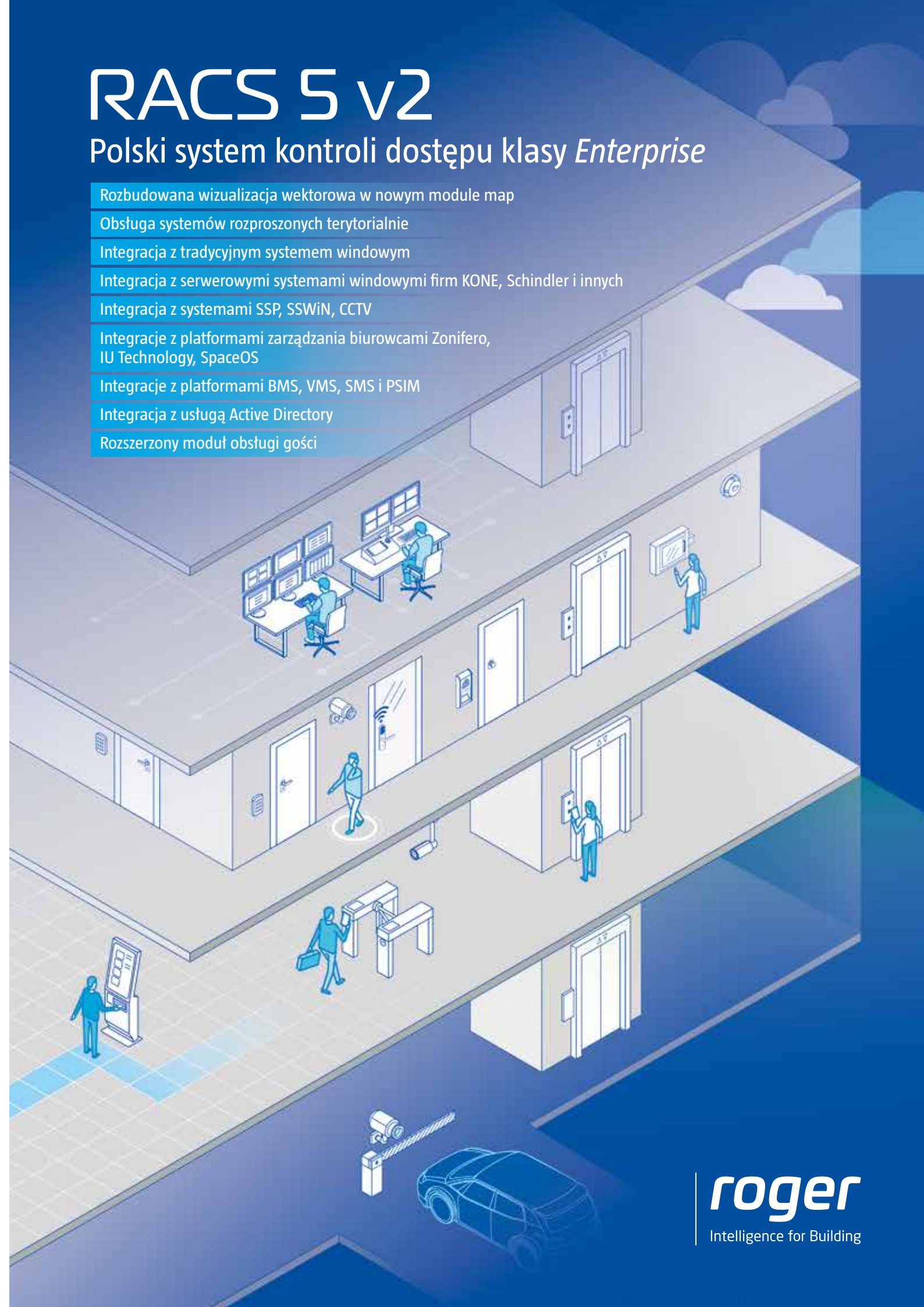
Integracja z systemami SSP, SSWiN, CCTV

Integracje z platformami zarządzania biurami Zonifero, IU Technology, SpaceOS

Integracje z platformami BMS, VMS, SMS i PSIM

Integracja z usługą Active Directory

Rozszerzony moduł obsługi gości



roger
Intelligence for Building

www.hikvision.com/pl

Kamery termowizyjne Seria HeatPro

SERIA HEATPRO FIRMY HIKVISION OBEJMUJE SZEROKĄ GAMĘ KAMER TERMOWIZYJNYCH PRZEZNACZONYCH DO RÓŻNEGO RODZAJU ZASTOSOWAŃ.

↓ Wyposażone w technologię Deep Learning doskonale sprawdzają się zarówno w monitoringu wizyjnym obiektów komercyjnych czy osiedli mieszkaniowych, jak i w ochronie obwodowej na terenach przemysłowych i magazynowych.

Kamery termowizyjne HeatPro mają funkcję inteligentnego pomiaru temperatury monitorowanych obiektów, a także reagowa-

nia i wysyłania alarmów w sytuacji odchylenia od ustalonego progu. Pozwala to na wykrycie i identyfikację obiektów oraz dokładną interpretację zdarzeń w danej scenie, co jest szczególnie ważne w przypadku zagrożenia pożarem czy ryzyka przegrzania urządzeń.

Dzięki funkcji rejestrowania obrazów w różnych warunkach oświetleniowych i atmosferycznych kamery HeatPro zapewniają do-



skonałą świadomość sytuacyjną oraz wysoką stabilność i szczegółowość obrazu niezbędną do prawidłowej ochrony obiektów.

www.linc.pl



Camect Smart Hub

NAJLEPSZA SZTUCZNA INTELIGENCJA ROZPOZNAJE OBIEKTY WIDZIANE PRZEZ KAMERY I GENERUJE ALARMY TYLKO W RAZIE ISTOTNYCH ZDARZEŃ, CAŁKOWICIE ELIMINUJĄC FAŁSZYWE ALARMY DOTYCZĄCE OWADÓW, ZWIERZĄT, LIŚCI, DESZCZU, CIENI ITP. MOŻLIWOŚĆ WYKORZYSTANIA TEGO RODZAJU SYSTEMÓW W MONITORINGU WIZYJNYM SPRAWIA, ŻE LICZBA NIEPOŻĄDANYCH ALARMÓW JEST PRAKTYCZNIE NIEZAUWAŻALNA.

↓ Taki właśnie jest Camect Smart Hub. Potrafi wykryć i rozróżnić ponad 30 rodzajów obiektów – ludzi od zwierząt, samochody od rowerów, pająki od cieni itp. Algorytm cały czas się rozwija, jest stale aktualizowany, co sprawia, że analiza staje się bliższa ideału. To daje skuteczniejszą

ochronę i większe poczucie bezpieczeństwa. Camect współpracuje z większością dostępnych kamer pracujących w standardzie ONVIF, RTSP itp. System obsługuje też głośniki zewnętrzne, co umożliwia wysyłanie odstraszających komunikatów głosowych.

Camect szanuje prywatność użytkownika, wszystkie dane wideo są przechowywane lokalnie, a wideo przesyłane do operatora jest zawsze szyfrowane. Dzięki inteligentnemu odtwarzaniu można przejrzeć cały dzień nagrań w 60 s. Platforma Camect Go umożliwia bezpieczny zdalny dostęp na każ-

dym urządzeniu z zainstalowaną przeglądarką. System jest w pełni zintegrowany z wiodącymi stacjami monitorowania w Polsce. Ponadto oferuje zapis kopii wideo w chmurze, powiadomienie o zdarzeniach, integrację z Alexa/Google i wiele innych. Camect jest po prostu smart!

www.nedapsecurity.com/pl/

Nedap AEOS Locker Management

W CZASACH, GDY NOWĄ NORMĄ JEST PRACA HYBRYDOWA, PRACOWNICY, WYKONAWCY I GOŚCIE POTRZEBUJĄ PRZESTRZENI DO PRACY W OGRANICZONYM WYMIARZE. NIE MAJĄC STAŁEGO BIURKA, MUSZĄ MIEĆ BEZPIECZNE MIEJSCE DO PRZECHOWYWANIA SWOICH RZECZY. TO OZNACZA, ŻE SZAFKI STAJĄ SIĘ NIEZBĘDNĄ I CENNĄ INWESTYCJĄ DLA WIELU FIRM.

↓ Zarządzanie szafkami AEOS to inteligentna odpowiedź na te wymagania. Umożliwia przypisywanie szafek do poszczególnych osób lub grup, zezwala na korzystanie z nich przez określony czas lub bez limitu, blokowanie i odblokowywanie za pomocą dowolnego identyfikatora – karty, telefonu komórkowego, cechy biometrycznej lub kodu QR.

Dashboard AEOS ułatwia zarządzanie tysiącami szafek. Terminal w postaci tabletu zapewnia użytkownikom prostotę użytkowania, a aplikacja mobilna – otwieranie i zamykanie skrytek za pomocą telefonu.

Z kolei połączenie zarządzania szafkami z fizyczną kontrolą dostępu umożliwia szybki dostęp



do danych i zaawansowanego systemu raportowania. Połączenie z systemem KD zapewnia ponadto dostęp do wielu integracji, m.in. z systemami HR.

AEOS Locker Management można wykorzystać, gdy towary lub urządzenia muszą zostać nadane lub odebrane. Rozwiązanie jest często stosowane m.in. przez:

- Działy IT – pracownicy mogą np. bezpiecznie zostawić uszkodzonego laptopa i odebrać go po naprawie.
- Sklepy z narzędziami – instalatorzy mogą odbierać materiały po godzinach pracy.
- Kurierzy – paczki można zostawić w bezpiecznym miejscu, gotowe do odbioru w późniejszym czasie.

Linc
Polska Sp. z o.o.



SR-150
MAŁY RADAR
O DUŻYCH
MOŻLIWOŚCIACH

KORZYŚCI TECHNOLOGII RADAROWEJ:



ZASIĘG DETEKCJI

150 m człowiek / pojazd



KĄT POKRYCIA

120° w poziomie, 30° w pionie, połączenie 3 radarów daje pełne pokrycie 360°



DOKŁADNOŚĆ

poniżej 1m



PLUG & PLAY

łatwa instalacja i wsparcie większości kamer i VMS



HOLISTYCZNY SYSTEM

MASS jest integralną częścią VMS



WYSOKA SKUTECZNOŚĆ

minimum fałszywych alarmów niezależnie od warunków pogodowych



TECHNOLOGIA AI

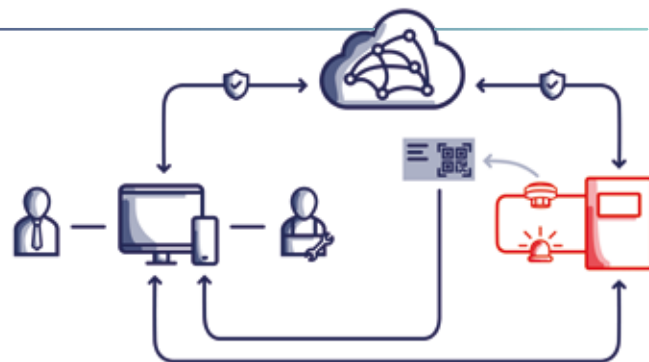
rozpoznawanie i identyfikacja intruzów z wykorzystaniem technologii AI

WWW.LINC.PL/RADARY

www.schrack-seconet.pl

Platforma serwisowa S2

CERTYFIKOWANA (POD WZGLĘDEM BEZPIECZEŃSTWA) PLATFORMA CHMUROWA S2SERVICE UMOŻLIWIA BEZPIECZNE POŁĄCZENIA Z NADZOROWANYMI OBIEKTAMI PRZEZ VPN. WSZYSTKIE ROUTERY PRACUJĄ W CHMURZE S2SERVICE I SĄ ZARZĄDZANE PRZEZ PRODUCENTA, CO GWARANTUJE NAJWYŻSZY POZIOM BEZPIECZEŃSTWA.



NAJWAŻNIEJSZE FUNKCJE

- Najwyższe standardy bezpieczeństwa dzięki szyfrowanym tunnelom VPN i dwuetapowej autoryzacji użytkownika.
- Pełny dostęp do najnowszej dokumentacji produktowej, projektowej oraz informacji serwisowych. Możliwość szybkiego wyszukiwania elementów poprzez kody QR.

- Wbudowane algorytmy do analizy oprogramowania, przyjętych rozwiązań i ich wzajemnej kompatybilności.
- Automatyczna analiza obciążenia systemu. Szczegółowa informacja o możliwościach rozbudowy, elementów wyposażenia zarówno central, jak i peryferyjnych.
- Zdalne zarządzanie zdarzeniami przez Integral Remote zapewnia

stały dostęp do wszystkich komunikatów systemowych i stanu systemu w czasie rzeczywistym.

- Automatyczne generowanie protokołów serwisowych, list przetestowanych elementów i list nieprawidłowości.
- Możliwość szybkiego dodania dokumentacji fotograficznej i listy nieprawidłowości do raportu z przeglądu.

- Zarządzanie zadaniami serwisowymi. Łatwe tworzenie zadań na podstawie listy komunikatów zdarzeń z systemu.
- Wsparcie przy instalacji systemu. Montaż i jednoczesna alokacja elementów z wykorzystaniem aplikacji Integral Scan czytującej kody QR elementów. Tak przygotowaną listę elementów można wykorzystać do programowania centrali.

www.tp-link.com.pl

TP-Link TL-SX3206HPP – ultrawydajny przełącznik PoE++ z portami 10G



TP-LINK TL-SX3206HPP TO PRZEŁĄCZNIK ZARZĄDZALNY, KTÓRY ZOSTAŁ WYPOSAŻONY W CZTERY PORTY POE++ 10G. WSPIERA STANDARD 802.3AF/AT/BT, DOSTARCZAJĄC MOC DO 60 W NA PORT. CAŁKOWITA MOC PODŁĄCZONYCH URZĄDZEŃ WYNOŚI 200 W. PODŁĄCZENIE PRZEŁĄCZNIKA DO ISTNIEJĄCEJ SIECI UMOŻLIWIAJĄ DWA SŁOTY SFP+ 10G.

↓ Dzięki prędkościom 10G switch idealnie nadaje się do wdrożenia punktów dostępowych Wi-Fi 6 oraz w przyszłości Wi-Fi 7. Urządzenie ma rozbudowane opcje zarządzania, znajdzie zastosowanie zarówno w małych, jak i średnich firmach, w których istnieje potrzeba stworzenia stabilnej, nie-

zawodnej i skalowalnej sieci służącej do przesyłania dużych ilości danych. Zarządzanie siecią ułatwia możliwość zdalnego sterowania poprzez chmurę. TP-Link TL-SX3206HPP obsługuje protokół IPv6 oraz posiada opcję konfiguracji VLAN 802.1Q, dzięki której sieć może być dzielona na odizolo-

wane, mniejsze segmenty, co przekłada się na wysoki poziom bezpieczeństwa i wydajność. Umożliwia także szybko wykrywanie najczęstszych ataków DoS, które wcześniej zostały zdefiniowane. Z kolei funkcja ACL (Access Control Lists) ma zastosowanie w przypadku blokowania dostępu do okre-

ślonych zasobów sieci, a IGMP Snooping pozwala na inteligentne skierowywanie strumieni multicastowych tylko do określonych subskrybentów. Przełącznik może być zarządzany przez chmurę dzięki zgodności z platformą Omada SDN. Urządzenie zostało objęte 5-letnią gwarancją.

www.zkteco.eu

Przenośny Terminal RCP S 922

S922 TO WYJĄTKOWY PRZENOŚNY TERMINAL KONTROLI DOSTĘPU ZAPROJEKTOWANY PRZEZ FIRMĘ ZKTECO DO UWIERZYTELNIANIA OSÓB I REJESTRACJI CZASU PRACY W TERENIE, POZA SIEDZIBĄ FIRMY, NP. NA PLACACH BUDÓW, W CENTRACH LOGISTYCZNYCH, DUŻYCH GOSPODARSTWACH ROLNYCH CZY PRZEMYSŁE WYDOBYWCZYM.

↓ Dzięki specjalnej gumowej obudowie urządzenie jest odporne na urazy mechaniczne i wstrząsy, w tym upadki z wysokości 0,5 m. Obudowa terminala zapewnia również wysoki stopień wodo- i pyłoszczelności (klasa ochrony IP65). W górnej części terminala znajduje się uchwyt ułatwiający jego przenoszenie. Urządzenie ma w zestawie zasilacz, ale wbudowany akumula-

tor o pojemności 7600 mAh umożliwia jego długą pracę z dala od zasilania sieciowego. Terminal wyposażono w kolorowy ekran LCD TFT o przekątnej 3,5". Oprócz czytnika różnych typów kart RFID ma też wbudowany doskonałej jakości czytnik linii papilarnych o pojemności pamięci do 50 tys. wzorców linii. Urządzenie wyposażono standardowo w interfejsy TCP/IP i USB.



Terminal S922 jest oferowany w kilku wersjach w zależności od koloru obudowy, typu czytanych kart RFID oraz zestawów wbudowanych interfejsów komunikacyjnych: Wi-Fi, GPRS, 3G (WCDMA) czy 4G.

Dzięki łączności komórkowej urządzenie może zdalnie łączyć się z oprogramowaniem umieszczonym na serwerze i przysyłać do niego dane z terminala w celu ich analizy.

KD
CCTV
SSWiN

urmet
MIWI

INTELIGENTNA
ANALIZA WIDEO
W CENTRACH
HANDLOWYCH:

- zliczanie ludzi / pojazdów
- rozbudowany moduł raportowania
- integracja z kasami fiskalnymi
- mapy ciepła



MIWI URMET Sp. z o.o.
ul. Pojezierska 90 A | 91-341 Łódź
+48 42 616 21 00 | miwi@miwiurmet.pl
www.miwiurmet.pl

ICTProtege.

Milesight

NUVO

IndigoVision
a Motorola Solutions Company



50 2022
SECURITY

Branża zabezpieczeń
elektronicznych w 2022 r.

Analiza rynku wg regionów

Ameryka Północna – ostrożny optymizm, ale i niepewność po COVID

WILLIAM PAO

asmag.com



Rynek zabezpieczeń security w Ameryce Północnej odnotował wzrost inwestycji po pandemii, ponieważ wiele firm wznowiło wstrzymane wcześniej projekty. Jednocześnie problemy charakterystyczne dla rynku amerykańskiego zmusiły użytkowników do zwiększenia nakładów na zapewnienie ochrony. Źródłem niepewności natomiast pozostają kwestie związane z łańcuchem dostaw i inflacją, co może mieć wpływ na rozwój w najbliższym czasie.

Ameryka Północna poniosła ogromne straty w szczycie pandemii, teraz obserwuje się powrót do normalnych działań. Według danych z września br. średnia liczba dziennych zachorowań spada. Ponownie otwierane biura i wznowiane projekty wpływają na ożywienie branży ochrony.

- W ostatnim roku branża zabezpieczeń wprowadziła wiele usprawnień i generalnie zmierza w dobrym kierunku. Znow są organizowane targi i imprezy, klienci odbywają spotkania w biurach, a producenci realizują swoje cele w zakresie przychodów. Wprawdzie w łańcuchu dostaw nadal występują problemy, to pojawia się światło w tunelu – powiedział Jeff Ross, dyrektor ds. marketingu w ACRE Americas.
- W regionie Ameryki Północnej nastąpiło osłabienie popytu na technologie zabezpieczeń. Na początku pandemii obserwowaliśmy przesunięcie środków finansowych z ochrony na inne potrzeby przedsiębiorstw. Teraz widzimy, że użytkownicy końcowi chcą zabezpieczać swoje obiekty za pomocą najnowszej technologii – stwierdził Adam Lowenstein, dyrektor ds. zarządzania produktami w i-PRO Americas.

COVID-19 wpłynął na zmianę sposobu myślenia wielu użytkowników w Ameryce Płn. o niezbędnych do przeprowadzenia inwestycji. Firmy skupiły się na cyfryzacji i zdalnych/hybrydowych modelach pracy.

- Wciąż jeszcze odczuwamy skutki pandemii, zwłaszcza wpływ pracy w domu i związane z tym otwarcie na komunikację w sieci. Priorytetem pozostaje bezpieczeństwo, ale w ramach tych wdrożeń nastąpił przyspieszony zwrot w kierunku łączności mobilnej i dostępności zdalnej, wy-

muszony blokadami podczas lockdownu, a także powolnym powrotem do biur – ocenił Charles Pitman, kierownik ds. marketingu produktów w firmie Genetec.

Najszybciej rozwijające się sektory i technologie

Zapotrzebowanie na systemy zabezpieczeń są widoczne w wielu sektorach.

- Nadal rośnie zapotrzebowanie na integrację systemów zabezpieczeń na różnych rynkach wertykalnych, po części związane z konsekwencjami pandemii, i wdrażanie innowacji technologicznych, z naciskiem na transformację cyfrową. Chociaż wszystkie sektory rynku zanotowały wzrost, w Convergent zauważyliśmy, że był on znacznie większy na rynkach finansowym, opieki zdrowotnej, w instytucjach rządowych, centrach danych i przedsiębiorstwach użyteczności publicznej – powiedział Mike Mathes, wiceprezes wykonawczy Convergent.

Jeśli chodzi o technologię, w obszarze security nadal dominują analiza wizyjna i rozwiązania w chmurze. Nastąpił znaczny wzrost zainteresowania rozwiązaniami chmurowymi i mobilnymi, szczególnie w odniesieniu do systemów kontroli dostępu i zarządzania wizją (VMS).

- Wiele organizacji dostrzega, że tradycyjne rozwiązania lokalne (on-premise) mogą być kosztowne w utrzymaniu, trudne do aktualizacji i czasochłonne w zarządzaniu. Przejście do chmury i oferty mobilnej wzmacnia infrastrukturę organizacji, oszczędza koszty i pozwala na osiągnięcie większego poziomu bezpieczeństwa – stwierdził J. Ross.

Niedobory wyzwaniem i szansą

Mimo znacznej poprawy na rynku północnoamerykańskim utrzymujące się zagrożenia mogą osłabić perspektywy wzrostu. Wśród nich są problemy z zachowaniem płynności łańcucha dostaw, które nękają cały świat. To one stanowią test na zdolność dostawców do zapewnienia towarów na czas pomimo niedoborów komponentów i problemów logistycznych.

- Zaktócenia w łańcuchu dostaw były niekorzystne dla wszystkich. Jednak firma i-PRO w wielu przypadkach była w stanie złagodzić je dzięki własnej fabryce i strategii niepolegania w tak dużym stopniu na dostawach podstawowych podzespołów od dostawców elektroniki – ocenił A. Lowenstein. – Produkty wysyłamy drogą powietrzną zamiast morską, aby maksymalnie skrócić czas realizacji zamówień. Wprowadziliśmy też usługę Quick Delivery Service z 24-godzinny terminem dostawy kluczowych modeli, aby umożliwić naszym partnerom realizację wymagań projektowych w odpowiednim czasie.

Problemy związane z dostawami wywołały również pozytywne efekty.





– Zakłócenia w łańcuchu dostaw, których doświadcza świat, zachęciły firmy do uniezależniania się od towarów z jednego źródła. Myśląc przyszłościowo, szukają rozwiązań o otwartej architekturze, które gwarantują im większy wybór i elastyczność dostosowaną do potrzeb i bieżącej dostępności – skomentował Charles Pitman.

– Ograniczenia w łańcuchu dostaw spowodowały, że klienci zamiast stosować tradycyjne podejście, są bardziej elastyczni i otwarci na ocenę, instalację i zarządzanie alternatywnymi rozwiązaniami. Producenci czytników kart i kart KD również doświadczają dużych opóźnień ze względu na ograniczoną podaż chipów mikroprocesorowych i innych surowców. Sytuacja ta powoduje szybsze przystosowanie i przejście na mobilne systemy uwierzytelniania wykorzystujące smartfony – dodał Mike Mathes.

Kwestie dotyczące łańcucha dostaw ściśle wiążą się z inflacją i obserwowanym wzrostem cen różnych produktów, w tym systemów zabezpieczeń.

– Wszystkie gałęzie produkcji doświadczają wzrostu cen z powodu zakłóceń w łańcuchu dostaw, inflacji i innych czynników zewnętrznych. Ze względu na wzrost kosztów w ostatnim roku uczestnicy łańcucha dostaw byli zmuszeni do podniesienia cen, a niektórzy dostawcy i resellerzy nie mogli sami zrekomensować podwyżek – powiedział J. Ross. – Niektórzy producenci zabezpieczeń podnieśli ceny swoich produktów o 10–20% w obu Amerykach. Inni ograniczyli swoje programy rabatowe. Dla i-PRO, mimo że dotknął nas skokowy wzrost kosztów frachtu lotniczego, nie podnieśliśmy cen. Naszym zamiarem jest utrzymanie stabilnych cen i zaabsorbowanie dodatkowych wydatków do czasu, gdy rynek

ustabilizuje się po pandemii. To część zobowiązania wobec naszych resellerów, aby mogli rozwijać biznes i mieć optymalną ofertę dla klientów – podkreślił Adam Lowenstein.

Co czeka nas w 2023 r.

W Ameryce Północnej w roku 2023 sytuacja nadal będzie niepewna.

– Przewiduje się, że rynek obu Ameryk będzie rość do końca 2022 r., co wpłynie na zwiększenie przychodów. W 2023 r. rynek północnoamerykański jednak spowolni z powodu większej niepewności gospodarczej – stwierdził Charles Pitman z firmy Genetec. Mimo to rynkowi gracze wyrażają ostrożny optymizm. Wyzwania pozostają, ale bezpieczeństwo wciąż jest priorytetem, zwłaszcza w takim kraju jak USA. Tu kwestie bezpieczeństwa i ochrony są przedmiotem największej troski: w 2022 r. miały miejsce dziesiątki incydentów z udziałem broni. Najpoważniejszym z nich była strzelanina w szkole średniej w Uvalde w Teksasie, w której zginęły 22 osoby.

– W 2023 r. rynek zabezpieczeń w Ameryce Północnej powinien nadal rosnąć. Stymulatorem wzrostu będą zarówno pandemia, jak i postęp technologiczny oraz coraz większa liczba krytycznych zagrożeń mających miejsce w 2022 r. Bezpieczeństwo pozostanie najwyższym priorytetem we wszystkich sektorach, natomiast ważne, aby liderzy biznesu i Security Managerowie szukali możliwości wdrożenia, integracji lub modernizacji systemów zabezpieczeń w celu optymalizacji ochrony. Mogą np. zwrócić się do ekspertów, którzy pomogą im to osiągnąć szybko i skutecznie – zauważył Mike Mathes.

Wpływ COVID-19 na bezpieczeństwo

W regionie EMEA osłabł wpływ COVID-19, jednak wnioski po 3-letniej pandemii mają obecnie głęboki wpływ na bezpieczeństwo. Sektor zabezpieczeń technicznych w tym regionie poradził sobie z konsekwencjami obostrzeń pandemicznych i prawdopodobnie szybciej niż inne porównywalne sektory odrobi zaległości. Mimo to można zaobserwować pewne zmiany w strategii bezpieczeństwa po wyciągnięciu wniosków.

– Większy nacisk kładzie się na raportowanie w czasie rzeczywistym i konwergencję danych. Zainteresowaniem cieszą się też rozwiązania oparte na sztucznej inteligencji, ponieważ użytkownicy końcowi starają się ograniczyć wymóg zaangażowania operatora w zdarzenia alarmowe. Celem jest również zastąpienie tradycyjnej siły roboczej systemami zabezpieczeń – podkreślił Mark Horton. – Nie jest przesadą, że COVID-19 ma ogromny wpływ na bezpieczeństwo i samopoczucie ludzi, a to przekłada się na wzrost nakładów na systemy zabezpieczeń. Zespoły ochrony, by wspomóc wysiłki związane z zapewnieniem bezpieczeństwa sanitarnego w czasie pandemii, zaczęły traktować priorytetowo analitykę wideo, taką jak liczenie zajętych miejsc czy mierzenie odległości między osobami – wyjaśnił Uri Guterman, szef działu produktów i marketingu w Hanwha Techwin Europe.

Technologie i rynki wertykalne

Pod względem technologicznym w regionie EMEA nadal dominowały sztuczna inteligencja i cyberbezpieczeństwo.

– W 2022 r. w regionie EMEA wiele organizacji zaczęło stosować sztuczną inteligencję i powiązane z nią głębokie uczenie oraz uczenie maszynowe. Specjaliści do spraw bezpieczeństwa coraz lepiej ją poznali, staje się ona podstawą pakietów technologii bezpieczeństwa. To ekscytujące, ponieważ AI nie tylko podnosi poziom bezpieczeństwa, ale także dostarcza informacji potrzebnych do usprawnienia ich funkcjonowania. Większa dokładność i świadomość sytuacyjna, pewniejsze przewidywanie to tylko niektóre zalety, jakie może zaoferować analityka wizyjna wspomagana AI – powiedział Uri Guterman. – W Mobotix uważamy, że cyberbezpieczeństwo i AI są głównymi czynnikami wzrostu rynku. Dostrzegliśmy, jak ważna jest odporność infrastruktury na cyberataki. Z kolei rozwiązania oparte na AI otwierają zupełnie nowe możliwości przekładające się na zwiększenie poziomu bezpieczeństwa. To przekształca rynek – ocenił Thomas Lausten.

Jeśli zaś chodzi o rynki wertykalne, handel detaliczny okazał się wytrzymały. Wobec słabnącej pandemii sprzedawcy ponownie otworzyli sklepy i poradziły sobie z większą liczbą klientów.

– Nadal dobrze prosperowały duże uniwersytety, zwłaszcza że zagraniczni studenci wracają do kampusów, a liczba przyjęć rośnie. Duże korporacje, bankowość, centra danych i organizacje typu blue chip wdrażają programy zmian, modyfikując i konsolidując zajmowaną powierzchnię lub wykorzystując istniejące systemy zabezpieczeń elektronicznych i BMS, zapewniające analitykę biznesową, dane i wgląd np. w zajętość budynku, zużycie energii, zdrowie i bezpieczeństwo. – Ali Enser, dyrektor generalny Reliance High-Tech., wymienił sektory, które wykazały się odpornością.

Na Bliskim Wschodzie szczególnie dużą odpornością wykazała się bankowość.

– W tym regionie zaobserwowaliśmy utrzymujący się wysoki popyt w sektorach bankowym i finansowym. Organizacje inwestowały w unowocześnienie swoich możliwości w zakresie zarządzania materiałem wizyjnym, przechowywania danych i scentralizowanego monitorowania zgodnie z surowymi

standardami regulacyjnymi, które stymulowały rynek przez ostatnie cztery lata, m.in. regulacjami SAMA (Saudi Central Bank) – stwierdził Dennis Choi, GM IDIS Middle East & Africa. – Nasz największy klient bankowy w Królestwie Arabii Saudyjskiej kontynuował modernizację nowo nabytych oddziałów, tradycyjnych systemów ATMS, jak również bankomatów mobilnych, które są ważne dla tak wielu konsumentów.

Wyzwania

Na rynku EMEA na bezpieczeństwo i przyzwyczajenia użytkowników wpływają problemy z łańcuchem dostaw, wojna w Ukrainie i rosnące koszty związane z pogłębiającą się inflacją. Niedostateczne dostawy były i są poważnym wyzwaniem dla graczy z branży security.

– Ograniczenia związane z COVID-19 spowodowały spadek produkcji i doprowadziły do zamknięcia portów w Chinach, a to utrudniło pracę dostawcom, którzy polegają na komponentach tam produkowanych – wyjaśnił James Min, MD IDIS Europe. – Najpoważniejsze braki dotyczyły mikrosterowników (MCU), co ograniczyło dostawy rejestratorów i produktów wymagających procesorów. Przepływ towarów został również zakłócony przez rosnące koszty surowców i podzespołów oraz wyższe koszty energii, a także niedobór siły roboczej w produkcji i logistyce. – Niektórzy producenci kamer i urządzeń kontroli dostępu realizowali zamówienia w terminie od 6 do 12 miesięcy! W niektórych przypadkach produkty te można zastąpić, ale nie zawsze. Problemy z dostawami w większości zmaleły latem, ale niektóre znaczące opóźnienia istnieją nadal, dotycząc głównie liderów branży – powiedział Ali Enser. – Generalnie niedobór chipów wpłynął na każdy produkt w naszym portfolio. Rynek potrzebował czasu, aby podnieść się po COVID-19, mnóstwo fabryk w Chinach dotknęły powtarzające się w zeszłym roku blokady, dostawy były opóźnione, a konflikt w Ukrainie mocno uderzył w odbudowujący się rynek globalny – skomentował Tomáš Vystavěl, Chief Product Officer w 2N. – Na szczęście sytuacja się poprawia. To nie tylko zasługa dostawców komponentów. Producenci tacy jak my zainwestowali znaczne środki w badania i rozwój, przeprojektowanie produktów ze swojego portfolio. Zrobiliśmy to po to, aby zamiast elementów niedostępnych na rynku wykorzystać te, które są dostępne, i zapewnić rozsądny czas realizacji.

Kraje EMEA również dotyka inflacja powodująca wzrost kosztów gazu, energii, żywności, czynszów i kredytów hipotecznych. To może mieć wpływ na rynek security.

– We wszystkich branżach występują presje inflacyjne wpływające na koszty surowców i energii. Niektórzy z większych producentów mogą zaabsorbować część tych kosztów, więc nie ma ogromnego wzrostu cen ich produktów. Problem ten można usunąć dzięki zwinności firmy, zakupowi materiałów w ilościach hurtowych oraz możliwości przeprojektowania w przypadku znacznego wzrostu cen surowców – zauważył Uri Guterman.

Zapowiedź na następny rok

Oczekuje się, że w przyszłym roku tendencja wzrostowa będzie kontynuowana. Tomáš Vystavěl ma nadzieję, że wzrost będzie co najmniej taki sam jak przed pandemią COVID-19.

– Impulsem do wzrostu będzie stosowanie technologii zdalnego dostępu. Jednak nie wszyscy są gotowi na odejście od RFID. Odpowiedzią mogą być czytelniki wielotechnologiczne, łączące dwie lub nawet trzy technologie kontroli dostępu w jednym urządzeniu: Bluetooth, RFID, klawiatura – podkreślił.

John Davies także spodziewa się wzrostu w regionie EMEA w 2023 r., choć mniejszego niż w tym roku ze



EMEA – pogłębiające się niedobory i obawy związane z recesją

Rok 2022 był dla rynku zabezpieczeń w regionie EMEA ogólnie dobry. Odnotowano wzrost, który ma być kontynuowany w przyszłym roku, jednak niedobory dostaw, inflacja i wojna w Ukrainie wpływają na niepewność i zwiększają ryzyko. Branża, dzięki różnym pozytywnym czynnikom, jednak dobrze sobie radziła w tym roku.

– Pod względem generowanych przez naszą firmę przychodów region EMEA był drugi po Azji. Odnotowaliśmy duży wzrost w sektorach telekomunikacyjnym i użyteczności publicznej. Sektor naftowo-gazowy pozostaje oczywiście silny, ponieważ cena ropy naftowej odbiła po krachu w 2020 r. Popyt w regionie EMEA pozostaje wysoki, dlatego w 2023 r. planujemy kolejne inwestycje w tym regionie – powiedział Mark Horton, wiceprezes Bandweaver Technology.

– Na początku 2022 r. problemem w niektórych krajach nadal był COVID-19, natomiast od końca lutego niepewność na rynkach wywołała wojna w Ukrainie. Stało się jasne, że bezpieczeństwo – fizyczne i cyfrowe – jest coraz częściej tematem kluczowym, a firmy działające na tym rynku mogą liczyć na dobre perspektywy wzrostu – stwierdził Thomas Lausten, dyrektor generalny Mobotix.





względem na ekonomiczne skutki wyższych kosztów utrzymania i rosnące ceny energii.

– TDSi przewiduje 15-procentowy wzrost, który odzwierciedla stałą tendencję na rynku. W Wielkiej Brytanii i Unii Europejskiej będzie on związany z kontynuowaniem modernizacji starszych budynków i infrastruktury, które wymagają uwspółcześnienia i wyposażenia w nowoczesne rozwiązania zabezpieczeń – ocenił.

Można oczekiwać, że rynek na Bliskim Wschodzie także wypadnie dobrze.

– Europa obawia się zbliżającej się recesji, która może mieć wpływ na turystykę i podróże biznesowe w całym regionie. W Turcji zauważa się inne podejście – słaba lira pobudza turystykę, a turyści tłumnie odwiedzają plaże oraz zabytki kultury, jedzą słynne na całym świecie potrawy tureckiej kuchni oraz wybierają się na zakupy do tętniących życiem dzielnic handlowych i na historyczne bazy. To stymuluje popyt na nowoczesny dozór wizyjny w sektorze handlu detalicznego i hotelarstwa – powiedział Dennis Choi. – Królestwo Arabii Saudyjskiej planuje jedno z najbardziej ekscytujących i ambitnych projektów infrastrukturalnych na świecie, jednocześnie sporo inwestując w mniejsze programy w sektorach hotelarskim, handlu detalicznego i bankowym oraz w zamówienia rządowe. Podobnie jest w Zjednoczonych

Emiratach Arabskich, gdzie są prowadzone nowe, przełomowe projekty wielofunkcyjne, z adaptacją AI na dużą skalę.

Jednak wciąż jest za wcześnie, aby zakładać, że wszystko przebiegnie gładko, biorąc pod uwagę, że wspomniany negatywny wpływ będzie nadal osłabiać szanse wzrostu na rynku zabezpieczeń w regionie EMEA.

– W skali całego kraju zaobserwowaliśmy wzrost cen o ok. 10%. Niektórzy producenci podnieśli ceny nawet o ponad 15%. Powodem był niedobór chipów, wzrost kosztów pracy, spiętrzony popyt przekraczający podaż, inflacja, wzrost cen energii i kosztów surowców. Nie spodziewamy się, że będą się one utrzymywać w dłuższej perspektywie, ale stanowią aktualne i realne zagrożenie – skomentował Ali Enser.

James Min przypomina, że mimo początkowego negatywnego wpływu pandemii rynki w Europie szybko się dostosowały i uodporniły. Jednak nie należy lekceważyć czekających zagrożeń gospodarczych.

– Istnieje możliwość dużej recesji, ponieważ gospodarki zmagają się z wyższymi cenami energii, zakłóceniami dostaw, presją inflacyjną i zmniejszoną siłą nabywczą konsumentów. Wiele będzie zależało od wyniku wojny w Ukrainie oraz od tego, czy rządy i banki centralne będą w stanie utrzymać skuteczną, wspólną reakcję na liczne napięcia, jakie one powoduje – zauważył J. Min.



Azja – projekty w infrastrukturę inteligentnych miast stymulują wzrost

Rynek zabezpieczeń w Azji, tak jak cała gospodarka azjatycka, osiągnął w 2022 r. dobre wyniki, chociaż różnią się one w zależności od regionu. Większość krajów cieszyła się dwucyfrowym wzrostem, co w dużej mierze miało związek z inicjatywami rządowymi dotyczącymi rozbudowy infrastruktury oraz inteligentnych miast.

Według Międzynarodowego Funduszu Walutowego w tym roku Azja, jako całość, ma odnotować wzrost PKB na poziomie 4,9%. W ramach regionu zaawansowane gospodarki azjatyckie mają wzrosnąć średnio o 2,7%, natomiast rynki wschodzące – o 5,4%. Te inwestycje pozytywnie wpłynęły na rynek security w całym regionie.

– Po kilku latach pandemii w 2022 r. rynek zabezpieczeń nabrał tempa, gdy złagodzone ograniczenia w podróżowaniu i reżimie sanitarnym – powiedział Tony Wang, dyrektor generalny Convergent APAC.

Z kolei rynek security w Malezji w 2022 r. odnotował znaczną poprawę w porównaniu z rokiem poprzednim.

– Spodziewamy się ciągłego wzrostu o co najmniej 30%. Od czasu blokady większość naszych klientów zainwestowała w nowe sklepy i logistykę, magazyny, co zapewni nam bardzo potrzebną sprzedaż – skomentował Ian Foo, dyrektor ds. rozwoju biznesu w malezyjskiej firmie Melectron.

Następstwa COVID słabną

Chociaż COVID-19 nadal stanowi problem zdrowotny w Azji, jego wpływ na rynek security maleje po ponownym otwarciu firm i wznowieniu projektów.

– W okresie pandemicznych blokad negatywny wpływ wynikał przede wszystkim z braku możliwości wdrożenia i instalacji systemów. Jednak po otwarciu popyt odbił się od dna – powiedział Aditya Khemka.

Ian Foo twierdzi, że skutki COVID-19 będą odczuwalne w minimalnym stopniu, ponieważ większość rynków została otwarta.

– Na naszą sprzedaż wpływają użytkownicy końcowi i projekty średniej klasy. Kiedy zachodzi taka potrzeba, klienci są skłonni inwestować w bezpieczeństwo – ocenił.

Należy jednak zauważyć, że rośnie zakres cyberzagrożeń, a Azja nie jest tu wyjątkiem.

– Cyberprzestępcy są coraz bardziej aktywni, stosują bardziej zaawansowane narzędzia i najnowsze technologie – zauważył Amit Kulkarni, EVP of Cybersecurity w Allied Digital.

– Większość kadry zarządzającej sądzi, że jej organizacje są odpowiednio przygotowane na cyberatak. Incydenty cybernetyczne zagrażają każdej firmie. Dlatego zespoły do spraw bezpieczeństwa muszą być gotowe do reagowania na nie, odzyskiwania i przywracania systemów tak szybko, jak to możliwe, aby zminimalizować szkody wynikające ze zdarzeń cybernetycznych.

Projekty z zakresu infrastruktury i smart city

Kluczowym czynnikiem wzrostu rynku security w regionie jest rozwój inteligentnych miast i inwestycje w infrastrukturę. Wśród godnych uwagi projektów infrastrukturalnych i smart city w Azji są obecnie: faza pierwszej linii 21 metra w Szanghaju, Hai Lang LNG Gas Power Center w Wietnamie oraz projekt inteligentnej autostrady M4 w Australii.

Indie również mają swój udział w projektach, które mogą przynieść korzyści dla branży zabezpieczeń technicznych.

– Indie koncentrują się na ambitnych projektach inteligentnych miast i stymulowaniu rozwoju infrastruktury transportowej, co oznacza, że wszystkie te nowe inwestycje wymagają instalacji kamer dozorowych. To zwiększy obroty na naszym rynku – podkreślił Aditya Khemka. – Również wiele samorządów stanowych w Indiach uczestniczy w projektach, inwestując w urządzenia do miejskich systemów monitoringu wizyjnego, aby podnieść poziom bezpieczeństwa mieszkańców. Przykładowo zarządzający Telanganą koncentrują się obecnie na monitoringu ulic Hyderabadu, najbardziej monitorowanego dziś miasta na świecie.

Ceny i łańcuchy dostaw

Problem zaburzeń globalnego łańcucha dostaw dotknął również Azję. Zaobserwowano tu braki produktów i wzrost cen urządzeń systemów zabezpieczeń. Na szczęście sprzedawcy i dostawcy wykazali się odpornością i elastycznością, aby utrzymać się na rynku.

– Problem z ciągłością łańcucha dostaw miał znaczący wpływ na branżę security w całym regionie APAC i nadal stanowi duże wyzwanie. Co więcej, dotyczy nie tylko niedoboru podzespołów i urządzeń, ale także trudności w zakresie logistyki. To wyzwanie dla producentów i usługodawców – stwierdził Tony Wang. – Aby osiągnąć lepsze wyniki, w Convergent staramy się przyjąć podejście proaktywne, kładziemy nacisk na współpracę międzyregionalną, szeroką komunikację i zarządzanie ekosystemem.

– Im większy popyt na urządzenia systemów zabezpieczeń, tym poważniejszy niedobór chipsetów. Ze względu na zaburzenia dostaw wzrost cen jest sprawą naturalną. Ceny naszych produktów staraliśmy się utrzymać na tyle, na ile możemy, ale nie jesteśmy w stanie wchłonąć kosztów w całości – wyjaśnił Ian Foo. – Mamy szczęście, ponieważ udało nam się złożyć olbrzymie zamówienia na komponenty pod koniec 2021 r., jeszcze przed wzrostem cen. To ratuje nasz bilans.

– Problemy dotyczące niewystarczających dostaw urządzeń IT oraz cyberbezpieczeństwa utrzymywały się w 2022 r. i prawdopodobnie przedłużą się do 2023 r. Chipsety i półprzewodniki były trudne do kupienia, co spowodowało opóźnienia w dostawach, niekiedy nawet o ponad 400 dni. Było też wiele innych kwestii, np. ograniczenie pracy chińskich firm. Z powodu problemów logistycznych wzrosły ceny frachtu, powodując, że producenci podnieśli cenę rynkową – podkreślił Amit Kulkarni. – Wygląda na to, że sytuacja będzie się stopniowo poprawiać, ale nadal pozostaje mnóstwo zaległości z poprzednich zamówień, których realizacja może zająć nawet 8–10 miesięcy.

Dominuje optymizm

Jeśli chodzi o rok 2023, rynek security w Azji jest postrzegany z optymizmem.

– Spodziewam się wzrostu w branży zabezpieczeń w całej Azji Południowo-Wschodniej i Indiach, ponieważ na tych rynkach

klienci korporacyjni nadal inwestują i się rozwijają. Oceania i Japonia również odnotują wzrost – powiedział Tony Wang. – Na rynku zabezpieczeń w regionie APAC w 2023 r. przewiduję ogólną średnią stopę wzrostu na poziomie 20–25%, ale będzie się ona znacznie różnić na poszczególnych rynkach wertykalnych. Wzrost będzie wynikiem popytu, inwestycji w duże projekty infrastruktury krytycznej i nadrobienia zaległości w projektach odłożonych lub opóźnionych z powodu pandemii.

– Szybki wzrost, którego obecnie doświadcza branża security, będzie kontynuowany w najbliższej przyszłości. Dzięki szerszemu wykorzystaniu systemów i zwiększonemu popytowi w segmencie konsumenckim oraz dużym inwestycjom w infrastrukturę będziemy mogli utrzymać prognozowane tempo wzrostu branży na poziomie 20% – zauważył Aditya Khemka. – Na całym rynku malezyjskim tak długo, jak będą otwierane nowe firmy, będzie istniał popyt na produkty security. Wraz z wprowadzeniem technologii 5G w Malezji obserwujemy wzrost zapotrzebowania na systemy o wyższej specyfikacji. Ale nadal potrzebujemy młodego pokolenia użytkowników, które zaakceptuje wszystkie nowe gadżety technologiczne, ponieważ stanowią one nowy rynek – zauważył Ian Foo. 🌐

PRASANTH ABY THOMAS

asmag.com

50²⁰²²
SECURITY

Kontrola dostępu i telewizja dozorowa

Kondycja globalnego rynku w 2022 roku

Firmy na całym świecie powoli podnoszą się po pandemii. Pomimo poważnych napięć geopolitycznych i ograniczeń w łańcuchu dostaw rok 2022 należy uznać za udany – klienci ponownie uruchomili projekty i wznowili zakupy.

Kontrola dostępu w 2022 r. – trendy będą się utrzymywać



Pandemia COVID-19 w latach 2020–21 nadwerżyła kondycję przedsiębiorstw. Choć udało się złagodzić kryzys spowodowany obostrzeniami sanitarnymi, to pojawiły się kolejne problemy, m.in. zaburzenia w łańcuchu dostaw, niedobór chipów i poważne napięcia geopolityczne, które sprawiły, że rynki stały się niestabilne.

– *Ameryka Północna poniosła ogromne straty w szczycie – Dormakaba działała w trudnym środowisku biznesowym w roku finansowym 2021/22 – powiedział Mirko Meier-Rentrop, Deputy VP ds. komunikacji zewnętrznej grupy w firmie Dormakaba. – Pozytywną stroną był niespodziewanie wysoki popyt we wszystkich regionach, dzięki czemu firma zamknęła rok ze wzrostem zamówień i nadrobieniem zaległości. Znalazło to odzwierciedlenie w silnym wzroście o 7,7%.*

Niestabilność na świecie

Mirko Meier-Rentrop wskazał kilka czynników, które nadal oddziałują na środowisko makroekonomiczne. Utrzymujące się w kilku krajach blokady związane z pandemią uderzyły szczególnie w Chiny ze względu na ich strategię zero-COVID. Problemy z łańcuchem dostaw miały wpływ na produkty elektroniczne z wysoką marżą, na które zamówienia nie mogły być realizowane z powodu braku komponentów. Z kolei niedobór siły roboczej zaszkodził projektom budowlanym.

– *Zakłócenia w łańcuchu dostaw i tendencje inflacyjne niespodziewanie nasiliły się od marca br., po wybuchu wojny w Ukrainie – stwierdził Mirko Meier-Rentrop. – Dormakaba zareagowała dość szybko, zwiększając ceny, aby zrównoważyć inflację. Jednak zawsze pojawia się luka pomiędzy gwałtownie rosnącymi kosztami produkcji a ceną sprzedaży, co może mieć wpływ na wynik.*

Skutki wojny w Ukrainie i przyspieszonej inflacji widać również w wielkości PKB. Według OECD (Organizacji Współpracy Gospodarczej i Rozwoju) w pierwszym i drugim kwartale roku finansowego 2021/22 produkt krajowy brutto w krajach G20 zanotował wzrost kwartał do kwartału odpowiednio o 1,9 i 1,3%. W trzecim kwartale stał się widoczny wpływ napięć geopolitycznych, wartość PKB w głównych gospodarkach rozwiniętych i wschodzących zmniejszyła się do 0,7%.

Niedobór chipów i niepewność łańcucha dostaw

Na całym świecie notuje się niedobór mikrochipów. Hanchul Kim, dyrektor generalny firmy Suprema, zauważył, że w związku z eksportem produktów i usług do ponad 140 krajów wyzwaniem dla firmy jest radzenie sobie z zaburzeniami w łańcuchu dostaw i zwiększonymi kosztami surowców.

Kierownictwo innych firm potwierdza tę opinię, ale jednocześnie wskazuje, że nowe okoliczności stworzyły również inne możliwości dla przedsiębiorstw.

– *Globalny niedobór chipów w 2022 r. był głównym wyzwaniem dla wielu branż, w tym naszej – stwierdził Devin Love, starszy dyrektor ds. produktów software'owych w firmie Allegion. – Pojawiają się też nowe możliwości, np. firmy i właściciele bu-*

dyneków rekonfigurują sposób wykorzystania swoich przestrzeni, aby zachować prywatność zapewnianą podczas pracy z domu, a jednocześnie zaoferować przestrzeń do współpracy w biurach i spotkań face to face, których ludzie oczekują.

Wyzwania dla użytkowników końcowych

W ciągu ostatniej dekady sektor kontroli dostępu fizycznego i mobilnego rozwinął się w szybkim tempie, zwłaszcza w okresie pandemii. Prabhuraj Patil, dyrektor handlowy ds. rozwiązań KD w Azji Południowej w firmie HID Global, wskazał, że z punktu widzenia klienta wyzwania dotyczą podatności na zagrożenia i dostosowania się do życia po pandemii. Niektóre z tych zmian na rynku i nowe możliwości zostały uwzględnione w ostatnim badaniu *HID New State of Access Control Report Underscores Growing Demand for Future-Proof Mobile Solutions*.

– *Na bezpieczeństwo i wygodę wskazywało ponad 1000 respondentów na świecie – powiedział Prabhuraj Patil. – W tym samym badaniu 40% ankietowanych stwierdziło, że największym wyzwaniem jest ochrona przed lukami w zabezpieczeniach, natomiast możliwość sprawnego wydawania i cofania poświadczeń tożsamości wybrało 37%. Ponadto problemem, przed jakim staje wiele firm w wyniku hybrydowego modelu pracy i zespołów zdalnych, jest kwestia administrowania poświadczeniami kontroli dostępu.*

Tendencje w popycie konsumenckim

Pandemia COVID-19 jeszcze się nie skończyła, ale ryzyko zachorowania znacznie się zmniejszyło. Światowa Organizacja Zdrowia zasugerowała jej bliski koniec. Choć konsumenci mogą to uznać za sygnał oznaczający powrót do normalnego życia i pracy, ich podejście do funkcjonowania rynku znacznie się zmieniło.

Popyt na rozwiązania bezkontaktowe trwa mimo osłabienia pandemii

Rynek wydaje się podnosić i akceptować wiele zmian, jakie wprowadzono wraz z pandemią. Przykładowo w ciągu ostatnich dwóch lat normą stało się stosowanie rozwiązań bezdotykowych. Obecnie rynek nie wykazuje chęci powrotu do starszych technologii, np. identyfikacji za pomocą odcisków palców.

– *Wszystkie regiony odzyskują siły po pandemii, więc biznes wraca na właściwe tory. W sektorze kontroli dostępu podczas COVID-19 popularnością cieszyły się rozwiązania bezdotykowe. Gdy weszliśmy w erę postcovidową, zapotrzebowanie wzrosło, ponieważ uwidoczniły się ich niezaprzeczalne zalety. Bezkontaktowa KD obejmująca rozpoznawanie twarzy, kody QR, kody kreskowe i technologie dostępu mobilnego jest wygodniejsza, dokładniejsza i szybsza, a ponadto zapewnia higienę – stwierdził Hanchul Kim.*

Świadomość nowych technologii

Z chwilą ożywienia na rynku zostały wznowione duże projekty, które firmy wstrzymały podczas pandemii. Klienci byli zainteresowani rozwiązaniami biometrycznymi i bezdotykowymi, zwłaszcza rozpoznawaniem twarzy.

– *Popyt na dostęp mobilny rośnie w regionach znanych z tego, że szybko przyjmują nowe technologie. Zwięk-*



szonemu zapotrzebowaniu nasza firma mogła sprostać dzięki doświadczeniu w dostosowywaniu się do szybko zmieniających się rynków i potrzeb klientów w połączeniu z reputacją producenta najbardziej zaawansowanych rozwiązań biometrycznych i dostępu mobilnego – wyjaśnił H. Kim z Supremy.

– Rynek kontroli dostępu przeżywa ożywienie. Coraz większą wartość mają informacje o tym, jak są wykorzystywane oferowane przestrzenie i jak skonfigurować bezproblemowy dostęp dla wszystkich mieszkańców, najemców i pracowników – stwierdził Devin Love.

Klienci stają się bardziej świadomi dobrych praktyk w kontroli dostępu i tego, jak w pełni wykorzystać bogactwo oferowanych możliwości nowych technologii. Devin Love zwrócił uwagę na rosnące zainteresowanie rozwiązaniami dostępu mobilnego.

– Większym zainteresowaniem cieszy się mobilne poświadczanie tożsamości, choć branża dopiero poznaje potencjał, jaki technologia ta może zaoferować, np. w celu optymalnego wykorzystania przestrzeni – powiedział.

Z kolei Prabhuraj Patil zauważył, że mimo wielu wyzwań rynek stopniowo przenosi swoje zainteresowanie na nowe technologie, które pomagają złagodzić ryzyka i zapewnić bezpieczne miejsca pracy.

– To stwarza wielką szansę dla graczy takich jak my. W świetle tego zapotrzebowania mieliśmy pozytywny odzew ze strony naszych lokalnych klientów na kluczowe innowacje, takie jak HID Mobile Access, czytniki następnej generacji HID Signo, kontrolery HID Aero i technologia Seos Credential – ocenił.

Czynniki wpływające na popyt

Według Hanchula Kima wraz z ożywieniem gospodarki po pandemii COVID-19 rynki ponownie się otwierają, wzrosło zapotrzebowanie na nowe standardy bezpieczeństwa, takie jak zblizeniowe potwierdzanie tożsamości, a także na wzmocnienie bezpieczeństwa rozwijających się firm oraz wymianę przestarzałych systemów.

Podobne spostrzeżenia ma Mirko Meier-Rentrop z firmy Dormakaba, która nie narzeka na popyt na większości swoich rynków. W roku finansowym 2021/22 miała wiele zamówień.

– Niestabilna sytuacja geopolityczna nie powinna przestąpić fundamentalnych trendów w branży, które pozostają niezmienione w stosunku do okresu sprzed pandemii COVID-19 i nadal będą stymulować rozwój techniczny i handlowy dormakaby – stwierdził Mirko Meier-Rentrop, wymieniając pięć głównych czynników, które jego zdaniem dynamizują popyt.

1. WZROST POZIOMU DOBROBYTU

Potrzeba bezpieczeństwa i ochrony charakteryzująca klasę średnią w krajach rozwiniętych stanie się normą w większej liczbie miejsc na świecie.

2. ZMIANY DEMOGRAFICZNE

Średnia długość życia rośnie, co oznacza, że instytucje i domy prywatne coraz częściej potrzebują rozwiązań „bez barier”, które nie utrudnią seniorom przemieszczania się.

3. GLOBALIZACJA

Większość ludzi na świecie żyje w miastach, a infrastruktura staje się bardziej złożona, co wymaga zaawansowanych rozwiązań wspierających płynny przepływ ludzi.

4. POTRZEBA BEZPIECZEŃSTWA

Budynki i tereny powinny być zarówno łatwo dostępne, jak i zabezpieczone przed zagrożeniami. Spełnienie tych połączonych potrzeb w sposób skuteczny i wygodny wymaga kompleksowego rozwiązania w zakresie kontroli dostępu.

5. TECHNOLOGIA

Technologia wpływa na każdy aspekt rynku zabezpieczeń, od cyfryzacji i kanałów dystrybucji po łączenie produktów w sieć w ramach Internetu rzeczy. Klienci oczekują, że ich doświadczenia zawodowe związane z kontro-

lą dostępu powinny się płynnie integrować z ich osobistymi środowiskami/urządzeniami cyfrowymi (np. smartfonami).

– Tych pięć trendów wpływa na wszystko, co robi Dormakaba – od strategii, przez rozwój produktów, po marketing i sprzedaż. Oczekujemy, że kontrola dostępu i uwierzytelnianie na wszystkich rynkach wertykalnych zostaną wzmocnione z uwzględnieniem adaptacyjności, wszechstronności i ochrony zdrowia – powiedział M. Meier-Rentrop.

Główne sektory zwiększające popyt na kontrolę dostępu

Specyfika rynku postcovidowego sprawiła, że w 2022 r. niemal wszystkie sektory gospodarki zaczęły notować wzrost. Firmy ponownie uruchomiły projekty komercyjne, które były wstrzymane przez prawie dwa lata, natomiast rządy zaczęły inwestować w rozwój infrastruktury w celu pobudzenia gospodarek i oferowania udogodnień technicznych.

Projekty komercyjne

Wzrost popytu w segmencie budownictwa komercyjnego i ekspansja w sektorze przemysłowym pomogły firmom odzyskać pozycję na rynku. Wraz ze stabilizacją działalności branży turystycznej odżyły inne powiązane z nią sektory, takie jak hotelarstwo.

– Wzrost w obu Amerykach wiąże się z ożywieniem na rynku budownictwa komercyjnego w USA (szczególnie w zakresie renowacji i modernizacji) oraz odpornością krajów Ameryki Łacińskiej – ocenił M. Meier-Rentrop. – W regionie Azji i Pacyfiku dynamiczny wzrost zanotowano w największych jego państwach. Dużym zainteresowaniem cieszyły się rozwiązania dostępu bezdotykowego. Ich sprzedaż np. w Hongkongu w okresie 2021/22 zwiększyła się o ok. 50% w porównaniu z rokiem poprzednim. Odnotowano dwucyfrowy wzrost w zakresie oku drzwiowych, systemów wejściowych, systemów noclegowych i systemów kluczy mechanicznych.

W Chinach większa liczba projektów komercyjnych, takich jak lokale na wynajem, z nadwyżką zrekompensowała negatywne skutki lockdownów i inne problemy na rynku mieszkaniowym. Na świecie dostrzeżono duże znaczenie centrów danych, co pobudziło zapotrzebowanie na wyż-

szej klasy, skuteczne systemy zabezpieczeń na potrzeby tego sektora.

– Ilość przesyłanych i przechowywanych danych podczas pandemii COVID-19 znacznie się zwiększyła, gdyż z powodu lockdownu działano głównie online – podkreślił Hanchul Kim. – Sytuacja wymagała zatem zwrócenia większej uwagi na odpowiednie zabezpieczenie centrów danych, w związku z czym firmy zabezpieczające je zaczęły wdrażać więcej terminali kontroli dostępu Supremy.

Budownictwo mieszkaniowe i edukacja

Sytuacja ekonomiczna sprawia, że rośnie zainteresowanie rozwiązaniami kontroli dostępu także w budownictwie mieszkaniowym. Devin Love zwrócił uwagę, że popyt w tym sektorze pobudza m.in. niedobór przystępnych cenowo mieszkań. Z kolei fundusze rządowe pozwoliły szkolnictwu wyższemu i innym organizacjom instytucjonalnym na inwestycje w infrastrukturę

– W ujęciu ogólnym czynniki długoterminowe, z możliwością rekonfiguracji wynajmowanej przestrzeni włącznie, podtrzymują popyt komercyjny, a elektroniczna kontrola dostępu zyskuje akceptację nie tylko w ochronie perymetrycznej obiektów – dodał Devin Love.

Edukacja jest obszarem, gdzie zapotrzebowanie na rozwiązania dostępu mobilnego rośnie.

– Większość studentów korzysta ze smartfonów. Dostęp mobilny z potwierdzeniem tożsamości za pomocą smartfonu ułatwia im dostęp do obiektów na terenie kampusu. – Kim Hanchul potwierdził opinię D. Love'a.

Lotniska i infrastruktura krytyczna

Według Mirko Meiera-Rentropa wzrost w Europie i Afryce będzie kontynuowany dzięki silnemu portfelowi zamówień i rosnącej liczbie projektów na głównych rynkach. Do takich należą m.in. duże kontrakty Dormakaba z Avinor na dostawę bramek samoobsługowych, korytarzy jednokierunkowych i powiązanych usług dla wszystkich norweskich portów lotniczych, a także z REWE Group w Austrii, krajowej sieci supermarketów. Hanchul Kim stwierdził, że firmy z branży naftowej i gazowej również wykazały duże zainteresowanie systema-

mi kontroli dostępu w celu poprawy bezpieczeństwa. Może to być spowodowane problemami z dostawami z Rosji.

David Thean, dyrektor generalny na Azję w Gallagher Security, dodał, że obserwuje wzrost liczby nowych projektów budowlanych w porównaniu z trzema ostatnimi latami, aczkolwiek nieco poniżej oczekiwań, przypuszczalnie z powodu obaw o możliwą globalną recesję.

– Największy popyt odnotował sektor rządowy ze względu na modernizację infrastruktury i szybszą urbanizację – powiedział D. Thean.

Rynek integracji systemów w 2022 r.

Mirko Meier-Rentrop ocenił, że integracja systemów jest znacznie łatwiejsza ze względu na nowoczesne API. Nadal istnieje duże zapotrzebowanie na wdrażanie rozwiązań dla klientów i utrzymanie ich przez cały okres użytkowania.

– Z tego powodu, zwłaszcza w przypadku ograniczeń COVID-19, większą uwagę zwraca się na rozwiązania pozwalające na zdalne podejmowanie interwencji, wykonywanie czynności serwisowych oraz nadzór. Wraz z coraz bardziej odczuwalnym brakiem specjalistów poszukiwane są rozwiązania ułatwiające pracę. Integratorzy są więc zainteresowani rozwiązaniami najbardziej efektywnymi, łatwymi we wdrażaniu i umożliwiającymi zdalną obsługę – powiedział M. Meier-Rentrop.

Hanchul Kim stwierdził, że usługi dostosowane do potrzeb klienta są obecnie głównym trendem wśród integratorów systemów.

– Ponieważ korporacyjne systemy IT konsoliduje się w celu uzyskania efektywności, wymagają one integracji dostosowanej do konkretnych potrzeb. Suprema stale rozszerza partnerstwo z innymi firmami, takimi jak Genetec, aby zapewnić zintegrowane usługi.

Zakłócenia łańcucha dostaw i zwiększone zapotrzebowanie na systemy zintegrowane miały wpływ również na firmy zajmujące się integracją. Systemy IT stają się coraz bardziej przystępne, a integratorzy bardziej obeznani z informatyką. Lista interesariuszy rośnie, ponieważ cyberbezpieczeństwo lokuje się na szczycie wymagań klientów. Branża spełnia wymagania dotyczące bezpieczeństwa zarówno fizycznego, jak i logicznego.

– Niedobory dostaw wpłynęły na integratorów, skłaniając ich do przyjęcia nowej technologii i znalezienia innych sposobów na wykonanie zadania – powiedział Prabhuraj Patil. – Konwergencja bezpieczeństwa fizycznego i logicznego w dalszym ciągu należy do ważnych kierunków rozwoju, a większa elastyczność w świadczeniu pracy, czyli praca w sposób rozproszony, uwypukliła potrzebę zarządzania ludźmi i miejscem.

David Thean podkreślił, że wielu integratorów próbuje nadrobić dwuletnie zaległości w podróżach do klientów i działaniach face to face. Są w stanie wrócić do prowadzenia działalności poprzez kontakty osobiste, co jest jedynym trwałym sposobem budowania relacji biznesowych.

– Spora grupa integratorów inwestuje w marketing i uczestniczy w targach i wystawach w Azji – ocenił.

Branża odbija się od dna

Pomimo wyzwań branża kontroli dostępu jest na drodze do odzyskania równowagi. Dla większości dostawców rozwiązań i integratorów priorytetem jest powrót do działalności sprzed pandemii, kiedy klienci interesowali się nowymi rozwiązaniami.





50²⁰²²
SECURITY

Telewizja dozorowa w 2022 r. – popyt i wyzwania rosną

Po około 24-miesięcznej przerwie spowodowanej pandemią rok 2022 był pracowity dla firm zajmujących się telewizją dozorową. Uruchomiono wiele projektów wstrzymanych z powodu obaw o zdrowie i życie, klienci wznowili inwestycje, co pobudziło popyt na rynku.

– Odnotowaliśmy wzrost wywołany wzmożonym zapotrzebowaniem na rynku – powiedział Ray Mauritsson, prezes Axis Communications. – Ożywienie po pandemii jest tu kluczowym czynnikiem.

Ale pandemia nie była jedynym tego powodem. Na popyt wpłynął również rozwój technologiczny, zapewniający klientom większe poczucie bezpieczeństwa i wygodę.

– Sektor monitoringu wizyjnego kontynuował wzrost w roku 2022 – stwierdził Charles Pitman, Product Marketing Manager w firmie Genetec. – Klienci są zadowoleni z posiadania urządzeń i systemów połączonych w sieć, coraz częściej szukają sposobów na uproszczenie konserwacji systemu, mając jednocześnie zdalny dostęp do danych.

Wyzwania do pokonania

Zwiększony popyt nie oznacza jednak braku wyzwań. Większość firm z obszaru dozoru wizyjnego nadal musi sobie radzić z różnymi problemami, w tym z zaburzeniami w łańcuchu dostaw, niedoborami układów scalonych i innymi wiążącymi się z tym niedogodnościami.

Brak komponentów

Zakłócenia w łańcuchu dostaw i niedostępność komponentów były jednym z największych wyzwań, z jakimi w 2022 r. musiały się zmierzyć firmy na świecie. Chociaż niedobór chipów wydaje się obecnie ustępować, branża nadal zмага się z zaległościami.

– Podobnie jak wiele innych organizacji, wciąż stoimy przed wyzwaniami spowodowanymi utrzymującymi się skutkami pandemii, czyli z globalnymi niedoborami komponentów i zakłóceniami w łańcuchu dostaw. Chociaż ta sytuacja nie jest wyjątkowa dla Axis, uświadomiła nam problemy, z jakimi musieliśmy sobie poradzić – wyjaśnił Ray Mauritsson. – Zrewidowaliśmy podejście do projektowania i wytwarzania naszych produktów, a w miarę ożywienia na rynkach i poprawy w łańcuchach dostaw obserwujemy systematyczny wzrost.

Wychodzenie z blokad

Proces wychodzenia z pandemii nie przebiegał jednakowo na wszystkich rynkach. W wielu częściach świata ograniczenia w podróżowaniu i przywracanie działalności handlowej przebiegały w różnym tempie. Niektóre kraje, np. Chiny, nadal zachowują reżim, co powoduje, że firmy podejmują działania z opóźnieniem.

– Niestabilność rynku, problemy z łańcuchem dostaw i niedobory siły roboczej sprawiły, że w niepewnej sytuacji znalazły się inwestycje w infrastrukturę w zakresie systemów zabezpieczeń – ocenił Charles Pitman. – A wolniejszy niż oczekiwano powrót do biura spowolnił duże projekty i nowe budowy.

Czynniki pobudzające popyt

Pandemia, która zmusiła ludzi do pozostania w domach, pozwoliła z innej perspektywy spojrzeć na korzyści płynące z technologii operujących na danych wizyjnych, zwłaszcza w połączeniu z AI i analityką. Wykorzystanie systemów VSS do celów wykarczających poza zabezpieczenia jest obecnie bardziej popularne.

Korzyści z AI i analityki

Więcej klientów jest obecnie świadomych mocy analityki i tego, jak jej wykorzystanie może pomóc ich firmom. Niższe koszty, zwiększona wydajność i lepsza ochrona oferowane przez algorytmy przemawiają do nich bardziej niż reaktywne urządzenia zabezpieczające z poprzedniej epoki.

– W minionym roku wprowadzano różne projekty prywatne i publiczne, z założeniami wymagające dozoru – powiedział Charles Pitman. – Wiele firm zwraca się ku rozwiązaniom analityki wizji, żeby wzmocnić bezpieczeństwo obiektu, uzyskać nowe dane czy rozwiązać nietypowe problemy. Wiele projektów wdrożeniowych przeprowadzono w związku z udostępnieniem takich technologii, jak uczenie maszynowe i głębokie uczenie, o dużym potencjale do automatyzacji procesów, które jednocześnie dostarczają operatorom informacji biznesowych.

Wykorzystanie analityki do analizy danych wizyjnych przyczyniło się do jej rozwoju w kierunku ułatwienia i ekonomicznego wdrożenia na szeroką skalę. Stało się to możliwe dzięki dostawcom, którzy skupiają się na wydajności zasobów sprzętowych i oferują bardziej precyzyjne sterowanie przebiegiem analiz w ustalonych odstępach czasu lub harmonogramach zamiast w sposób ciągły.

Nieodłączny popyt

Ray Mauritsson uważa, że zwiększone zapotrzebowanie to naturalna kolej rzeczy, ponieważ klienci stają się bardziej świadomi zagrożeń i sposobów radzenia sobie z nimi. Interesują się zaawansowanymi rozwiązaniami monitoringu wizyjnego, które zapewniają lepszą ochronę i większe poczucie bezpieczeństwa.

– Po pierwsze, na naszym rynku od lat utrzymuje się wzrost popytu stymulowany głównie przez zwiększone zainteresowanie technologiami zabezpieczeń we wszystkich sektorach. Nie miała na niego wpływu pandemia, chociaż blokady i problemy z łańcuchem dostaw na krótko zaburzyły sprzedaż Axis – powiedział Ray Mauritsson. – Po drugie, istnieje coraz większe zapotrzebowanie na technologie innowacyjne. Zawsze szczyliciliśmy się tym, że jesteśmy w czołówce innowacji technologicznych, a wraz z tym przychodzi zwiększone zapotrzebowanie na nasze produkty.

Główne branże pobudzające popyt

Niełatwo wskazać branże, które obecnie rozwijają się szybciej niż inne. Firmy realizują nowe i stare projekty we wszystkich sektorach.

– Trudno wskazać jeden sektor z największym popytem i wzrostem, ponieważ tak wiele z tego, co oferujemy, może być szeroko stosowane w wielu inwestycjach – podkreślił Ray Mauritsson. – Obserwujemy wzrost we wszystkich głównych sektorach.

Charles Pitman powiedział, że Genetec obserwuje wzrost w wielu sektorach, szczególnie w transporcie publicznym i przemyśle. Raport KPMG wskazuje, że 2022 zapowiada się jako rok możliwości, ponieważ świat uczy się na doświadczeniach i dąży do odbudowy odporności, wytrzymałości i równowagi. Ponieważ COVID-19 znacząco wpłynął na życie ludzi, zachowania konsumenckie również się zmieniają.

– To będzie również rok niepewności, gdyż pojawiają się nowe wyzwania, a oczekiwania społeczne nadal się zmieniają, gdy uczymy się żyć w świecie z (nie po) COVID-19. Liderzy infrastruktury mają okazję fundamentalnie zmienić naszą wspólną ścieżkę rozwoju w zakresie polityki klimatycznej, społecznej i zarządzania – podano w raporcie KPMG.

Zmiany dla integratorów w 2022 r.

Pandemia przemodelowała sposób działania wielu firm. Integratorzy systemów nie mogli wówczas pracować w terenie z powodu ograniczeń. Obecnie natomiast już nie muszą, ponieważ wraz ze zmianami preferencji klientów zmienił się też charakter ich pracy.

Urządzenia połączone w sieci

Pojawienie się Internetu rzeczy (IoT) i lepsza integracja zapewniły większy zwrot z inwestycji. Pandemia sprawiła, że klienci stali się bardziej świadomi korzyści płynących z takich funkcji, jak zdalne monitorowanie.

– Dążenie do przyłączenia do sieci nigdy nie było bardziej odczuwalne – zauważył Ch. Pitman. – Znalezione sposobów na ograniczenie do minimum prac konserwacyjnych wykonywanych na miejscu i zmniejszenie obciążenia pracowników spowodowały, że klienci poszukują ścieżek do chmury zarówno bezpośrednio, jak i za pomocą zarządzanych urządzeń, co pozwala zdjąć część obowiązków z wewnętrznych zespołów IT.

Efektywność kosztowa

Klienci stają się coraz bardziej wrażliwi na koszty i poszukują sposobów na zdalne monitorowanie lub konfigurowanie syste-

mów oraz ograniczenie zarówno przemieszczania się, jak i wyjazdów z domu z powodu ograniczenia z pracami serwisowymi wykonywanymi na miejscu. Od integratorów systemów oczekują, że skupią się na usługach o wartości dodanej, a nie na podstawowej instalacji i konserwacji. Rozwój oprogramowania i algorytmów pozwala integratorom sprostać tym wymaganiom.

Bezpieczeństwo cybernetyczne i analityka to priorytet

Ray Mauritsson zwrócił uwagę, że zainteresowanie klientów analityką i lepszym zabezpieczeniem przed cyberatakami ma znaczący wpływ na działalność integratorów.

– Funkcjonalność AI poprawiająca wydajność analityki jest czynnikiem pobudzającym popyt. Również, choć nie jest to nowy trend, rośnie zapotrzebowanie na silniejsze i bardziej zaawansowane poziomy cyberochrony. Możliwość oferowania produktów i rozwiązań o najwyższych standardach cyberbezpieczeństwa staje się kluczowym czynnikiem dla nas i dla naszych partnerów – podkreślił.

Wyzwania po pandemii

Podczas gdy obawy o ograniczenia w łańcuchu dostaw i niedobór chipów nękały branżę w 2022 r., firmy z obszaru telewizji dozorowej większości wracają do stanu sprzed pandemii. Po trwającej około dwóch lat przerwie klienci dokonują zakupów, stymulując popyt na rynku.

Przed branżą wciąż stoi sporo wyzwań z perspektywy zarówno dostawcy, jak i integratora. Firmy będą musiały sprostać wymaganiom klientów, oferując rozwiązania innowacyjne i usługi dostosowane do potrzeb. Powinny też zapewnić większy zwrot z inwestycji. ●

R E K L A M A



DYSTRYBUCJA • PROJEKTY • SZKOLENIA

VIVOTEK
A Delta Group Company

BOSCH

UNV

ADVANTECH

suma.solutions

tel. +48 32 757 98 55
email biuro@ipsuma.pl
www.suma.solutions



Badania rynku i komentarze branży

Najnowsze statystyki, analizy trendów i prognozy rynkowe firm badawczych i stowarzyszeń

Główne trendy na rynku zabezpieczeń technicznych w 2023 r.

OWEN KELL

MEMOORI



Swoimi spostrzeżeniami na temat trendów, które będą kształtować branżę zabezpieczeń technicznych w nadchodzącym roku, dzieli się Owen Kell, Senior IoT & Security Analyst w firmie badawczej Memoori.

Napięcia geopolityczne i handlowe

Czołowi chińscy giganci z sektora dozoru wizyjnego stają się coraz bardziej zależni od rynków zagranicznych. Hikvision i Dahua Technology pod względem ogólnych przychodów utrzymali dominującą pozycję z silnym wzrostem sprzedaży zagranicznej w pierwszej połowie 2022 r. i przychodami w wysokości ponad 16,7 mld USD w 2021 r.

Ich potencjalny wzrost jest jednak zagrożony przez słaby popyt wewnętrzny (w dużej mierze ze względu na efekt domina z powodu coraz bardziej kontrowersyjnego podejścia rządu chińskiego zero-COVID i wynikające z tego blokady głównych miast), w połączeniu z utrzymującymi się napięciami handlowymi między Chinami a Zachodem oraz słabnącymi globalnymi perspektywami gospodarczymi.

Napięcia związane z łamaniem praw człowieka oraz wojna handlowa między Chinami a Stanami Zjednoczonymi są powodem zmian legislacyjnych, kolejnych sankcji i barier handlowych, które w znacznym stopniu zakłóciły przepływy zarówno urzędów, jak i kluczowych podzespołów niezbędnych do wprowadzania rozwiązań innowacyjnych, a także zdolność ich producentów do sprzedaży swoich wyrobów.

Ponadto ogłoszone niedawno przez rząd USA restrykcje eksportowe nałożone na czołowych projektantów układów scalonych – firmy NVIDIA i AMD – ograniczą Chinom możliwość stosowania opłacalnych zaawansowanych rozwiązań o dużej mocy obliczeniowej, niezbędnych do zachowania konkurencyjności w dziedzinie technologii widzenia komputerowego (computer vision) i przetwarzania AI.

Restrykcje dotyczące sprzedaży chińskich produktów na określonych segmentach rynku (lub wręcz całkowity zakaz sprzedaży technologii danej firmy) obejmują większy zasięg nie tylko w USA, ale także w krajach zachodnich. Napięcia geopolityczne i handlowe zapewne będą się pogłębiać.

Producenci układów scalonych w Państwie Środka nie są w stanie osiągnąć wydajności zaawansowanych układów NVIDIA i AMD, toteż w celu odtworzenia mocy obliczeniowej chińscy badacze AI mogą być zmuszeni do powrotu do stosowania wielu układów z niższej półki.

AI staje się głównym nurtem

Po kilku latach obietnic i szumu wokół AI stosowanie rozwiązań opartych na sztucznej inteligencji staje się coraz bardziej opłacalne. Tempo zmian w ciągu ostatnich 12 miesięcy było nadzwyczaj szybkie. Poza tym wciąż są prowadzone prace badawcze.

Nastąpiła duża poprawa pod względem szybkości i dokładności rozwiązań uczenia maszynowego w praktycznych zastosowaniach w dziedzinach związanych z bezpieczeństwem, m.in. w wieloelementowym rozpoznawaniu twarzy, przetwarzaniu na krawędzi sieci obrazów z kamer dozоровych, analityce dźwięku oraz robotyce/dronach. To spowodowało, że obecnie silne algorytmy AI w kilku obszarach znacznie przewyższają możliwości człowieka.

Wysoko zaawansowana AI wymaga wprawdzie znacznej mocy obliczeniowej i zdolności przetwarzania, jednak połączenie możliwości przetwarzania w urządzeniu na brzegu sieci i elastycznego dostępu do coraz większych zasobów obliczeniowych w chmurze sprawia, że jej jest łatwiej dostępna.

Trwa wyścig pomiędzy dostawcami w zakresie integracji funkcjonalności nowej generacji, które są oparte na sztucznej inteligencji, z aplikacjami przeznaczonymi dla użytkowników końcowych w sposób ułatwiający dostępność, zwiększający użyteczność i ułatwiający stosowanie w codziennych scenariuszach bezpieczeństwa. Sztuczna inteligencja w coraz większym stopniu zastępuje operatora systemu bezpieczeństwa w wykonywaniu pewnych zadań, a interpretację danych, która wcześniej wymagała udziału człowieka, obecnie obsługują algorytmy. Dzięki automatyzacji procesów zarządzanie bezpieczeństwem jest łatwiejsze. W przypadku pracowników ochrony/operatorów stacji monitorowania pozwoli to na skrócenie czasu poświęcanego na monitorowanie zdarzeń/ekranów lub pilnowanie powiadomień alarmowych na rzecz zwiększenia czasu przeznaczonego na wykonywanie ważniejszych zadań. Sztuczna inteligencja odciąży ich w analizowaniu, ocenie i nadawaniu priorytetów zdarzeniom alarmowym, a następnie zapewni priorytetyzację w czasie rzeczywistym i rekomendacje dotyczące zdarzeń wymagających uwagi pracownika ochrony.

Udostępnienie tego rodzaju funkcji AI specjalistom ds. bezpieczeństwa będzie wymagało również integracji narzędzi AI/ML z istniejącym oprogramowaniem i platformami w sposób minimalizujący potrzebę kodowania lub wiedzy technicznej niezbędnej do ich obsługi, a także zapewnienia dostępności za pośrednictwem wielu mediów, w tym urządzeń mobilnych.

Pozostaną obawy dotyczące kwestii etycznego wykorzystania sztucznej inteligencji czy stronniczości algorytmów, ale rosnący poziom zastosowań technologii AI we wszelkiego rodzaju świadczonych codziennie usługach i rozwiązaniach (w szczególności w mediach społecznościowych) doprowadzi do coraz szerszej akceptacji tej technologii przez społeczeństwo.



Klienci bardziej świadomi

Inteligentne budynki wyposaża się w olbrzymią liczbę urządzeń IoT, zauważalny jest także wyższy poziom konwergencji między sieciami IT a OT. Czynniki te, w połączeniu z coraz większym wyrażaniem złośliwych wirusów i rosnącym uzależnieniem od usług w chmurze, powodują, że inteligentne budynki są coraz bardziej podatne na cyberataki.

W ostatnich 18 miesiącach na świecie odnotowano duży wzrost liczby ataków typu ransomware i strat wywołanych przez te nie². Zbyt często systemy automatyki budynkowej lub systemy zabezpieczeń technicznych oparte na technologii IoT stanowiły słaby punkt organizacyjnej cyberobrony, a liczne głośne przypadki naruszenia bezpieczeństwa służyły podkreśleniu ryzyka i podatności na zagrożenia.

Wśród klientów rośnie świadomość ryzyka cybernetycznego, konsekwencji kosztowych, a nawet negatywnego wpływu na zdolność właścicieli/operatorów do skutecznego ubezpieczenia budynków. W ostatnim roku na przyjęcie rygorystycznych warunków polis w zakresie cyberochrony decydują się bardziej doświadczeni klienci, by złagodzić skutki zagrożenia, przy czym wiele firm wdraża podejście Zero Trust do struktur sieciowych, ich ciągłą weryfikację, a także inwestycje w „utwardzanie” systemów.

Sztuczna inteligencja będzie odgrywać coraz większą rolę w obszarze bezpieczeństwa teleinformatycznego – w odniesieniu zarówno do cyberataków, jak i w ochronie przed nimi.

W ostatnim raporcie Memoori dotyczącym sztucznej inteligencji i uczenia maszynowego w inteligentnych budynkach (*AI & Machine Learning in Smart Buildings*) podano,

¹ Technologia operacyjna (OT – *operational technology*) – według definicji Gartnera, to sprzęt i oprogramowanie, które wykrywa lub powoduje zmianę poprzez bezpośrednie monitorowanie i/lub kontrolę fizycznych urządzeń, procesów i zdarzeń w przedsiębiorstwie.
² <https://www.ibm.com/security/data-breach>

że rozwiązania AI były wykorzystywane do przeprowadzania ofensywnych cyberataków. Kilka zidentyfikowanych incydentów wskazuje, że były też stosowane do szybszego uzyskania dostępu do systemu. Jeśli zaś chodzi o ochronę przed zagrożeniem, sztuczna inteligencja dostarcza pogłębione analizy ryzyka ataku cybernetycznego, przewiduje je z dużym prawdopodobieństwem ich wystąpienia, a także szybciej wykrywa, podnosząc poziom bezpieczeństwa i odporność organizacji.

Możliwości AI w zakresie bezpieczeństwa cybernetycznego przestają być dodatkiem, a stają się koniecznością w ocenie klientów świadomych zagrożeń cyfrowego świata. Dostawcy rozwiązań security, którzy chcą się wyróżnić na rynku, będą musieli inwestować w zabezpieczenia już w fazie projektowania, by uzyskać certyfikaty cybernetyczne, wykazać zgodność ze standardami cybernetycznymi oraz niezależnie testować i walidować swoje produkty.

Inne trendy, na które warto zwrócić uwagę w 2023 r.

Zdaniem ekspertów na rynek zabezpieczeń technicznych nadal będą miały znaczący wpływ:

- Utrzymujące się problemy globalnego łańcucha dostaw, oddziałujące na poziom zapasów, inflację i ceny oraz dostępność komponentów.
- Zacieranie się granic pomiędzy chmurą a wdrożeniami fizycznymi, gdyż coraz większa liczba użytkowników końcowych wybiera hybrydowe modele wdrażania w odniesieniu do przynajmniej części swoich rozwiązań security.
- Rosnące zapotrzebowanie na integrację i interoperacyjność systemów zabezpieczeń w celu lepszego raportowania i kontroli innych funkcji budynku/biznesu, obejmujące analizę zajętości, efektywność energetyczną i poprawę doświadczenia pracowników lub najemców.

Wskazane tu trendy zostały opracowane na podstawie raportów firmy Memoori dotyczących cyberbezpieczeństwa, potencjału IoT oraz aplikacji AI dla inteligentnych budynków. Będą one wzięte pod uwagę podczas corocznych badań dotyczących rynku zabezpieczeń technicznych, których wyniki zostaną opublikowane w grudniu 2022 r.

to, że 2021 był pierwszym rokiem, w którym ceny rosty, a nie spadały. Głównym powodem tendencji wzrostowej był niedobór podzespołów używanych do produkcji urządzeń do dozoru wizyjnego. Spowodowało to, że firmy, które nie były w stanie udźwignąć tak dużego zwiększenia kosztów, podniosły ceny produkowanych przez siebie urządzeń.

Dostawcy stanęli w obliczu niedoboru głównie półprzewodników, które są podstawą do wytwarzania przetworników obrazu i SoC, kluczowych elementów w kamerach IP.

Ustawa *CHIP Act* może nieco pomóc, ale nie od razu

- Szczególnie problematyczny był niedobór półprzewodników. Brakowało również rezystorów oraz niektórych tworzyw sztucznych i metali – powiedzieli Josh Woodhouse i Jon Cropley, dodając, że podpisana niedawno w Stanach Zjednoczonych ustawa *CHIP Act* może nieco poprawić sytuację związaną z niedoborem układów scalonych.
- Jest prawdopodobne, że w dłuższej perspektywie ustawa doprowadzi do zwiększenia produkcji półprzewodników w USA. Potrzeba jednak lat, aby powstały nowe zakłady produkcyjne i wielkość produkcji wzrosła. Dlatego wpływ ustawy *CHIP* prawdopodobnie zacznie być odczuwalny dopiero pod koniec okresu prognoz zawartych w naszym raporcie, sięgających do 2026 r. – stwierdzili Josh Woodhouse i Jon Cropley.

Według obu ekspertów presja inflacyjna zmusi dostawców do dalszego podnoszenia cen w latach 2022 i 2023, co będzie wpływać na rynek dozoru wizyjnego.

- Dystrybutorzy i użytkownicy końcowi będą kupować mniej kamer, a to oznacza, że w roku 2022 wzrost frachtu tych urządzeń będzie mniejszy niż w roku 2021, tendencja zniżkowa utrzyma się też w 2023 r. – podkreślili analitycy Novaira

Insights. – Średnie ceny kamery sieciowej i kamery analogowej powinny ponownie spaść w 2024 r., chyba że okres wysokiej inflacji będzie długotrwały.

Z kolei globalny rynek telewizji dozorowej (urządzenia i oprogramowanie) powinien do końca 2022 r. wzrosnąć o 11,7% i osiągnąć szacunkowo 28,2 mld dolarów. Jednak J. Woodhouse i J. Cropley prognozują znacznie niższy jego wzrost w 2023 r., natomiast stopniowe ożywienie z tendencją wzrostową powinno się zacząć od roku 2024.

Większe zainteresowanie rozwiązaniami w chmurze, szczególnie w USA

Pod względem technologicznym stopniowy trend do korzystania z rozwiązań monitoringu wizyjnego w chmurze utrzymywał się również w 2021 r., szczególnie w obu Amerykach, gdzie rynek oprogramowania zarządzającego materiałem wizyjnym w chmurze przekroczył 150 mln dolarów. W raporcie prognozuje się, że w latach 2021–2026 liczba kamer dozorowych podłączonych do chmury w tym regionie będzie rosła średnio dwukrotnie szybciej niż do staw kamer sieciowych.

Stosowanie rozwiązań do dozoru wizyjnego w chmurze w Stanach Zjednoczonych nastąpiło szybciej niż w większości krajów na świecie.

- To efekt wpływu wielu czynników. Głównym jest to, że w USA jest wiele przedsiębiorstw z rozproszonymi lokalizacjami, a każda z nich ma niewielką liczbę kamer. Co więcej, firmy te działają na dużym obszarze, używając wspólnego języka i wspólnego zestawu zasad dotyczących miejsca przechowywania danych, prywatności itp. Dostępność i koszt pasma były również bardziej korzystne niż w niektórych krajach – wyjaśniają J. Woodhouse i J. Cropley.



Novaira Insights: Rynek dozoru wizyjnego rośnie, a wraz z nim rosną ceny

WILLIAM PAO

asmag.com



Monitoring wizyjny jest kluczowym systemem zabezpieczeń elektronicznych. Josh Woodhouse, główny analityk i założyciel Novaira Insights, oraz Jon Cropley, analityk, zbadali, jak firmy z sektora VSS radziły sobie na tym polu w ostatnim czasie. Przedstawiają również prognozy na najbliższe lata.

Według raportu *The world market for video surveillance hardware and software*, opublikowanego przez Novaira Insights, światowy rynek urządzeń i oprogramowania do dozoru wizyjnego w 2021 r. wzrósł o 16,4%. Wśród kluczowych czynników wymienia się złagodzenie ograniczeń w przemieszczaniu się oraz zwiększony popyt po pandemii COVID-19 spowodowany wznowieniem projektów i boorem budowlanym w różnych częściach świata.

Wzrost cen spowodowany brakiem dostaw

W raporcie podano, że średnia cena kamery sieciowej na świecie wzrosła w ub. roku o ponad 7%, co sprawi-

³ Prezydent USA Joe Biden w sierpniu 2022 r. podpisał ustawę *Chips and Science Act*. Umożliwia ona m.in. uruchomienie subsydiów i ulg podatkowych na produkcję czipów oraz B&R. Nowe inwestycje w Stanach Zjednoczonych mają zwiększyć produkcję układów scalonych, jest więc szansa na ograniczenie problemu niedoborów.





OSSA: Nadzór nad przepływem danych cyfrowych

GIJS VAN DEN HEUVEL

Chair of Marketing Open Security & Safety Alliance (OSSA) oraz menedżer ds. strategii i współpracy z partnerami w Bosch Security Systems



Open Security & Safety Alliance (OSSA) to inicjatywa skupiająca się na tworzeniu ram dla standardów i specyfikacji z zakresu zabezpieczeń technicznych, ochrony fizycznej i automatyki budynkowej. Gijs van den Heuvel dzieli się swoimi przemyśleniami dotyczącymi trendów, które wpłyną na branżę zabezpieczeń w nadchodzącym roku.

Jako stowarzyszenie branżowe doskonale wiemy, co planują nasi członkowie, jeśli chodzi o wprowadzanie innowacji w ważnych obszarach zabezpieczeń i ochrony, ale nie tylko. Przedstawiciele OSSA są reprezentantami najbardziej wpływowych firm tego sektora, takich jak Bosch, Hanwha Techwin, Milestone Systems i Vivotek. Wspólnie kontynuujemy wprowadzanie otwartego ekosystemu opartego na danych.

IoT łączy urządzenia, czyniąc życie łatwiejszym, bardziej inteligentnym, bardziej intuicyjnym i bardziej produktywnym. Grupy robocze OSSA realizują projekty, których celem jest ujednolicenie i podniesienie poziomu rynku jako całości, co zapewni rozwój wszystkim uczestnikom. Organizacja OSSA określiła już warunki sprzętowe i programowe, które pozwalają na bezpieczne uruchamianie aplikacji analitycznych (wspieranych przez AI) innych firm na istniejących, niezależnie od marki, urządzeniach sieciowych (począwszy od kamer). Grupa opracowała kilka specyfikacji dotyczących tworzenia wspólnych elementów (np. w zakresie podstawowych wymagań systemowych, wskazówek dotyczących bezpieczeństwa cybernetycznego i interfejsów API), z których mogą wszyscy korzystać.

Wartym uwagi projektem, w który członkowie OSSA wnoszą swój wkład i wiedzę, jest wprowadzenie nowych poziomów wymiany danych i informacji z inteligentnych kamer i urządzeń IoT. W jaki sposób można osiągnąć kolejny poziom rozpowszechniania niezwykle wartościowych danych wykrywanych przez urządzenia gromadzące je w silosach charakterystycznych dla danej marki? Jak ustanowić otwarte, ale bezpieczne ścieżki łatwego dzielenia się danymi i jednolitej ich interpretacji, aby połączyć urządzenia dozorowe z urządzeniami edge computing?

Miliony rzeczy generują, gromadzą i przechowują mnóstwo informacji, które niestety zbyt często są niewykorzystywane i pozostają w archiwach. Po ich zebraniu, połączeniu i obróbkę, z opcjonalnym zastosowaniem AI, informacje te dają

szerszy obraz tego, co wykrył np. system dozoru wizyjnego. Zbieranie obrazów z różnych urządzeń IoT i budowanie relacji między nimi w celu stworzenia spójnego przepływu danych otwiera szerokie możliwości. Dostarczanie spójnych danych z jednego źródła do innego, które łatwo je zinterpretuje, ma ogromną wartość.

Wyobraźmy sobie wykorzystanie materiału wizyjnego z kamery dozorowej z aplikacją do odczytu tablic rejestracyjnych. Auto przejeżdża przed budynkiem, a kilka minut później inna kamera po drugiej stronie obiektu rejestruje osobę wspinającą się na ogrodzenie w pobliżu miejsca, gdzie wykryto samochód. Wreszcie trzecia kamera po przeciwnej stronie budynku rejestruje osobę przebywającą w niedozwolonym miejscu, a aplikacja otwartej platformy wykrywa broń w ręku. System natychmiast alarmuje pracowników ochrony o potencjalnym zagrożeniu. Powiązanie tych kluczowych informacji w sposób płynny, poprzez naturalną ścieżkę przepływu danych z urządzeń security i safety, wprowadza na nowy poziom, dostarczając nie tylko to, co widać, ale przede wszystkim to, co można przeczuć instynktownie. To jest przyszłość, o ile producenci urządzeń i inni interesariusze będą chcieli uczestniczyć w ekosystemie inicjowanym przez przemysł.

Członkowie organizacji pracują nad zestawem ogólnych, neutralnych dla producentów interfejsów programowania aplikacji (API), umożliwiających jednolitą interpretację danych w kamerach lub urządzeniach sieciowych zgodnie ze standardami OSSA. Interfejs może być również zastosowany w innego typu urządzeniach IoT z zakresu zabezpieczeń i ochrony, zapewniając łatwe sprzężenie między dowolną parą aplikacji wysyłających i odbierających, które gromadzą, przetwarzają i interpretują dane. Umożliwienie interpretowania treści pochodzących z urządzeń różnych marek i typów na otwartym forum wprowadza nowy poziom interpretacji zdarzeń związanych z bezpieczeństwem.

OSSA podejmuje współpracę na wielu poziomach, ułatwia integrację zewnętrznych aplikacji analitycznych AI w kamerach wideo i sieciach komputerowych. Organizacja jest zainteresowana wspólnymi działaniami wprowadzającymi branżę na wyższy poziom innowacji i interoperacyjności, by na tych polach osiągać sukcesy. 



ZINTEGROWANA PLATFORMA BRIVO DO KONTROLI DOSTĘPU

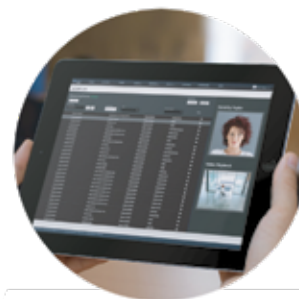
ŚWIATOWY LIDER I PIONIER W ZAKRESIE KONTROLI DOSTĘPU
I PLATFORM OCHRONY OPARTYCH W CHMURZE



Kontrola dostępu
Zautomatyzuj kontrolę dostępu
budynku oraz raportowanie



Monitoring wizyjny
Wyświetlaj obrazy w czasie
rzeczywistym i przeglądaj zapisy



Zdalne zarządzanie
Zarządzaj zabezpieczeniami
z dowolnego urządzenia mobilnego



Zarządzanie użytkownikami
Nadawaj uprawnienia
użytkownikom w systemie



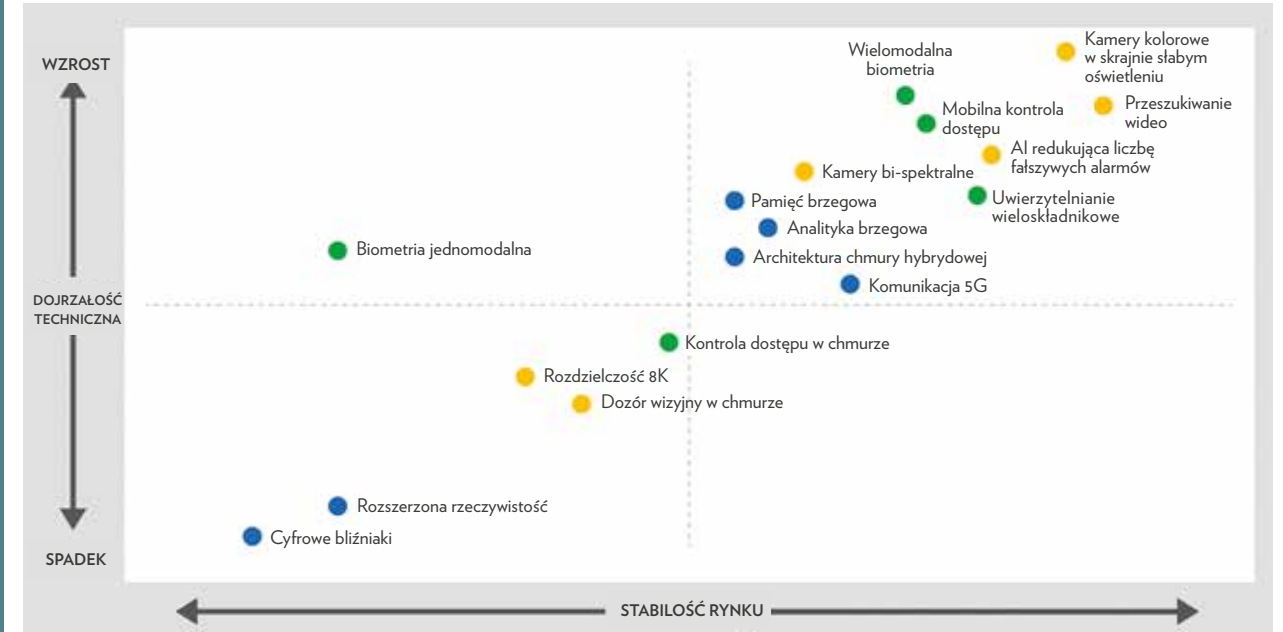
Kontrola odwiedzających
Bezpieczne warunki dla
odwiedzających i pracowników



Analiza danych
Przetwarzaj informacje na temat
bezpieczeństwa fizycznego

Główne trendy na rynku zabezpieczeń technicznych w roku 2022

W roku 2022 cyfrowa transformacja zabezpieczeń technicznych nabrała tempa. Następuje przekształcanie systemów z reaktywnych w proaktywne, pojawiają się nowe zastosowania, a organizacja staje się zoptymalizowana, wydajniejsza i bezpieczniejsza.



W tegorocznej ankiecie badającej dojrzałość i przydatność technologii stosowanych obecnie na rynku, przeprowadzonej przez asmag.com, wzięło udział 323 uczestników. Pozwoliło to wskazać te technologie, które są już dostępne, oraz te, które wchodzą do rozwiązań telewizji dozorowej i kontroli dostępu.

Bieżące i pojawiające się trendy



Wśród technologii dojrzałych i odpowiednich znalazły się: pamięć brzegowa (*edge storage*) (3), analityka brzegowa (*edge analytics*) (4), architektura chmury hybrydowej (*hybrid-cloud architecture*) (5) i komunikacja 5G (*5G wireless communication*) (6). Za niezbyt dojrzałe i nieodpowiednie uznano: cyfrowe bliźniaki (*digital twins*) (1) i rozszerzoną rzeczywistość (*augmented reality*) (2).

5G i przetwarzanie w urządzeniu brzegowym sieci (*edge computing*) to dwie technologie, których udział w rynku szybko rośnie, choć 5G w zeszłym roku uznano za niedojrzałe, natomiast

przetwarzanie na brzegu sieci nadrobiło opóźnienia. Użytkownicy opowiadają się za przetwarzaniem w urządzeniach końcowych, co ułatwia postępowanie w analityce brzegowej i pamięci masowej. Cyfrowe bliźniaki i rozszerzona rzeczywistość wciąż jeszcze mają przed sobą pole do rozwoju, ale ich potencjał w optymalizacji aplikacji bezpieczeństwa wydaje się obiecujący.

Kontrola dostępu



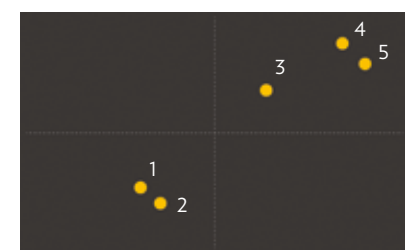
Technologie dojrzałe i odpowiednie: wielomodalna biometria (3), mobilna kontrola dostępu (4) i uwierzytelnianie wieloskładnikowe (5). Niezbyt dojrzałe ani odpowiednie: kontrola dostępu w chmurze (2). Za dojrzałe, ale nie tak odpowiednie uznano biometrię jednomodalną (1).

Dzięki wszechobecny smartfonom oraz uwierzytelnianiu bezdotykowemu mobilna kontrola dostępu w chmurze staje się coraz bardziej popularna i wciąż ma potencjał na rozwój. Uwierzytelnianie wieloskładnikowe przeważało nad biometrią jednomodalną, ponieważ

użytkownicy chcą korzystać z rozwiązań bardziej dokładnych i szybszych.

Telewizji dozorowa

Jako technologie dojrzałe i odpowiednie wskazano: kamery kolorowe działające przy skrajnie słabym oświetleniu (4), wspierane AI przeszukiwanie wideo (5), kamery bi-spektralne: termowizyjna + światła widzialnego (3). Za niezbyt dojrzałe uznano: rozdzielczość 8K (1), dozór wizyjny w chmurze (2).



Postęp w technologii odwzorowania kolorów na obrazie z kamery uzyskanym przy skrajnie słabym oświetleniu sceny przyczynił się do zwiększenia popularności kamer z taką funkcjonalnością w porównaniu z kamerami bi-spektralnymi. Spośród wszystkich funkcji sztucznej inteligencji jako najbardziej dojrzałe i odpowiednie wskazano wyszukiwanie osób/pojazdów. Tempo przechodzenia systemów monitoringu wizyjnego do chmury jest nadal powolne, ale powinno wzrosnąć wraz z ich rozwojem, natomiast rozdzielczość 8K może napotkać problemy związane z ceną i dystrybucją.

50²⁰²²
SECURITY

Badanie dojrzałości i przydatności technologii w 2022 r.



Kontrola dostępu w 2022 r. – rośnie popularność urządzeń mobilnych, chmura pozostaje stabilna

PRASANTH ABY THOMAS

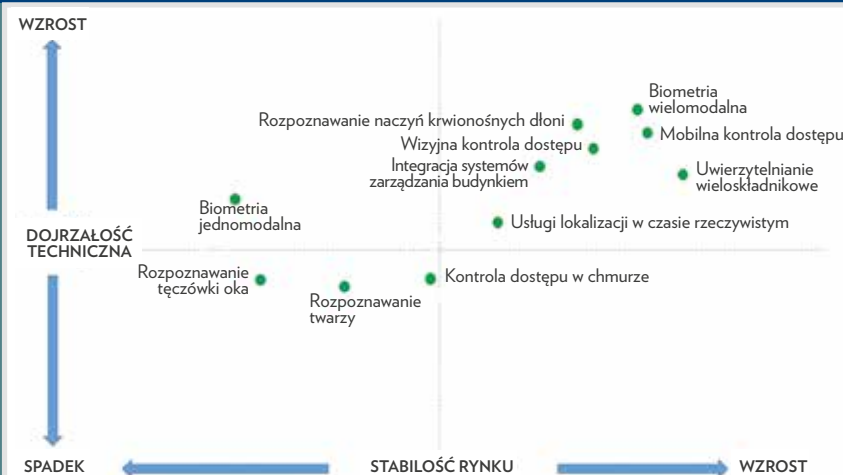
asmag.com

Badanie dotyczące kontroli dostępu w 2022 r. przeprowadzone przez asmag.com wśród integratorów, dystrybutorów i użytkowników końcowych wykazało, że biometria wielomodalna, uwierzytelnianie wieloskładnikowe, mobilna kontrola dostępu i rozpoznawanie linii papilarnych to jedne z najbardziej dojrzałych i wciąż rozwijających się technologii. Spośród nich biometria wielomodalna znalazła się na szczycie rankingu dojrzałości, podczas gdy wieloskładnikowe potwierdzanie tożsamości zostało uznane za najbardziej zrównoważone.

Większość dostawców, którzy wyrazili swoją opinię na analizowany temat, zgodziła się z wynikami badania. Niektórzy przedstawili czynniki wpływające na wybory dokonywane przez konsumentów i ich znaczenie w dłuższej perspektywie.

Wzrost popularności mobilnej kontroli dostępu

Hanchul Kim, prezes firmy Suprema, zwrócił uwagę na rosnącą popularność mobilnej kontroli dostępu ze względu na jej wygodę, łatwość i szybkość w użyciu. Wystarczy, że uprawniony użytkownik stuknie w swój smartfon, by przejść przez drzwi. Zarządzanie uwierzytelnianiem gości, a nawet obecnością pracowników jest bardziej opłacalne, ponieważ nie ma już potrzeby wydawania, gromadzenia i usuwania nieaktualnych fizycznych kart dostępu.



– Mobilna kontrola dostępu jest bezpieczna: karty dostępu mogą zostać zgubione, skradzione lub użyte przez nieuprawnionych użytkowników, natomiast mobilne dane potwierdzające tożsamość są zapisywane w smartfonie użytkownika, który ma określone uprawnienia – powiedział Hanchul Kim. – Mobilne poświadczenia są również w pełni zarządzane w chmurze, co ułatwia ich zdalną dezaktywację w przypadku zgubienia lub kradzieży smartfonu. Rozwiązania dostępu mobilnego Suprema zapewniają wszystkie powyższe cechy, które zwiększają wygodę użytkowników.

Podobnymi przemyśleniami podzielił się Devin Love, Senior Director for Software Products w firmie Allegion. Jak zauważył, poświadczenia tożsamości przechowywane w telefonie użytkownika i stosowane jako poświadczenia mobilne będą nadal jedną z popularniejszych technologii, ponieważ współpracują z przyzwyczajeniami człowieka.

– Zabezpieczając telefon biometrycznie, wiemy, gdzie te informacje są przechowywane i jak są wykorzystywane. Z tego procesu użytkownik prawdopodobnie już kiedyś korzystał. Równie ważne jest to, że szybkie tempo zmian w tym obszarze wymaga częstych aktualizacji, które można przeprowadzić poprzez stosunkowo szybki cykl aktualizacji telefonów komórkowych. Nadal wprawdzie nie będzie jednej uniwersalnej technologii, która zarządziłaby wszystkim, ale można oczekiwać, że uwierzytelnianie za pomocą telefonu, jako jedna z metod, będzie rozwijane i szybciej wdrażane niż inne – powiedział Devin Love.

Potencjał rozwiązań w chmurze

Rozwiązania oparte na chmurze zyskują na popularności. W badaniu asmag.com wykazano, że większość respondentów wystawiła kontroli dostępu w chmurze ocenę średnią pod względem dojrzałości i trwałości. Jedną z firm, która skupiła się na tych rozwiązaniach i opowiada się za chmurą hybrydową jako najlepszym sposobem na przyszłość, jest Gallagher.

– Chmura hybrydowa znacznie ułatwia wdrażanie szeregu usług – ocenił Steve Bell, kierownik ds. technologii w Gallagher Security. – Pozwala sprzedawcy kontrolować aktualizacje oprogramowania, aby mieć pewność, że te usługi są zawsze zabezpieczone przed najnowszymi zagrożeniami cybernetycznymi. Wdrożenie bezpiecznego połączenia do naszej chmury Gallagher z serwera on-premise jest najważniejsze. Zawsze zlecamy podłączenie urządzeń pracujących w sieci lokalnej do chmury Gallagher, ponieważ dzięki temu dział IT klienta może łatwo zabezpieczyć połączenie, a firma Gallagher zabezpiecza je po stronie chmury.

Command Center Web firmy Gallagher to nowy interfejs użytkownika, który wykorzystuje podejście hybrydowe, aby umożliwić bezpieczne uruchamianie stacji roboczej na dowolnym urządzeniu z przeglądarką internetową. Użytkownicy mogą dodawać nowe funkcje do tej aplikacji bez aktualizacji na miejscu, a klienci zawsze będą dysponować najnowszą jej wersją. Według S. Bella to najlepsza opcja dostępna dzięki obu rozwiązaniom.

Rozwiązania do wielu zastosowań

Istnieje kilka technologii kontroli dostępu, ale wielu użytkowników zastanawia się nad tym, czy są one na tyle dopracowane, by móc je stosować na szeroką skalę. Hanchul Kim uważa, że mobilnej kontroli dostępu można bezpiecznie używać w wielu zastosowaniach, zwłaszcza że KD oparta na technologii UWB (Ultra-WideBand) wkrótce zostanie skomercjalizowana. UWB to technologia RF, która może dokładnie mierzyć odległości z błędem 5–10 cm.

– Na rynku pojawiają się smartfony z UWB, m.in. iPhone i Samsung Galaxy – zaznaczył H. Kim. – Im więcej takich smartfonów będzie w użyciu, tym bardziej wzrośnie zapotrzebowanie na mobilną kontrolę dostępu opartą na UWB. Użytkownik zbliżający się do drzwi zostanie rozpoznany, o ile będzie miał przy sobie smartfon, a drzwi otworzą się automatycznie, bez konieczności dalszego uwierzytelniania. Suprema dołączyła do FiRa Consortium, organu doradczego, który ustala standardy dla technologii UWB, aby przyspieszyć rozwój tych rozwiązań i zapewnić wygodniejsze oraz bezpieczniejsze korzystanie z nich.

Inni z kolei sugerują, że potencjał mobilnej kontroli dostępu ogranicza kilka zmiennych. Steve Bell zwrócił uwagę, że chociaż te rozwiązania są dostępne już od co najmniej pięciu lat, doświadczenie użytkownika w dużej mierze zależy od tego, czy korzysta z usług niezawodnego i zaufanego dostawcy. Poświadczenia tożsamości ze smartfonu poprawią wydajność, umożliwiając wykorzystanie technologii NFC zarówno na urządzeniach Apple'a, jak i z systemem Android. Zgodnie z wynikami ankiety S. Bell też uważa autoryzację wieloelementową za opcję dojrzałą, choć to zależy od zastosowanych technologii.

– Uwierzytelnianie wieloskładnikowe powinno być stosowane przez większą liczbę klientów. Podążając za przykładem sieci komputerowej i uwierzytelniania internetowego, ważne jest zapewnienie ochrony cybernetycznej, którą wieloskładnikowość gwarantuje – zauważył Steve Bell. – Łatwo sklonować większość starszych technologii poświadczeń tożsamości. Nadal można ukraść dane identyfikacyjne lub przechwycić kartę, którą ktoś zgubił. Uwierzytelnianie wieloelementowe, np. karta oraz kod PIN lub karta plus dane biometryczne, może chronić przed nieuprawnionym dostępem. Przykładowo, karta rządu

USA w standardzie FIPS201 (PIV) ma możliwość 3-elementowego uwierzytelniania za pomocą karty/PIN/biometrii, ale w praktyce nie jest zbyt często stosowana.

Wniosek

Odpowiedzi czytelników asmag.com i wywiady z dostawcami nie dają jasnego obrazu rynku. Analiza wyników badania pozwala jednak wskazać kilka trendów. Przykładowo wzrost zastosowania mobilnych rozwiązań kontroli dostępu jest powszechnie postrzegany jako wielki krok naprzód w systemach KD, ponieważ oferowane przez nie wygodę i bezpieczeństwo przewyższają te, które są dostępne w innych rozwiązaniach. Wykorzystanie chmury ma potencjał, ale jej powolny wzrost pokazują zarówno badania, jak i wywiady z producentami. Jednak w perspektywie może się okazać integralną częścią systemów kontroli dostępu.

Identyfikacja wieloskładnikowa jest prawdopodobnie najbardziej dopracowanym i popularnym rozwiązaniem na wszystkich rynkach. Może to stanowić podstawę do płynnego przejścia do rozwiązań opartych na urządzeniach mobilnych, ponieważ urządzenia te mogą zapewniać kilka trybów uwierzytelniania.

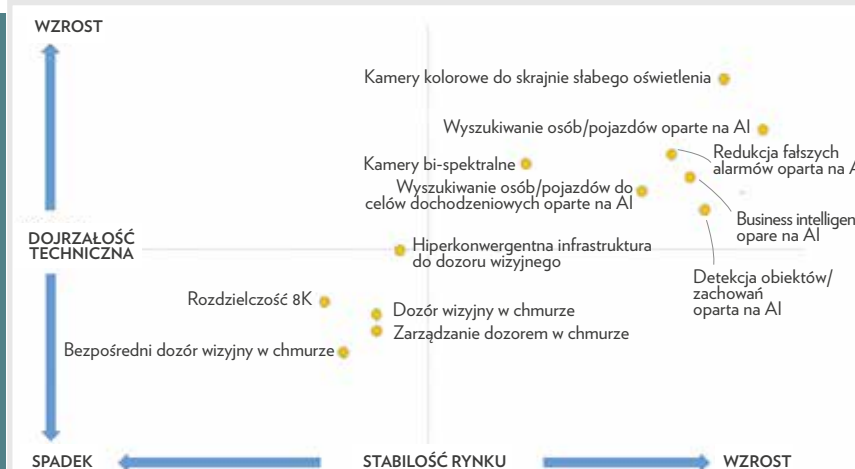
Telewizja dozorowa: w 2022 r. najpopularniejsza jest AI

Tegoroczna ankieta przeprowadzona wśród integratorów, dystrybutorów i użytkowników końcowych ukazuje się w trudnym momencie, gdy firmy na całym świecie wracają do normalnego funkcjonowania po dwóch latach przerwy, a jednocześnie pojawiają się skutki wojny w Ukrainie. Pandemia miała duży wpływ na branżę i konsumentów, otwierając nowe perspektywy na technologie i rozwiązania. Co ważne, firmy zdały sobie sprawę ze znaczenia usług zdalnych i analityki wspieranej sztuczną inteligencją, które mogą zwiększyć wygodę i bezpieczeństwo.

PRASANTH ABY THOMAS

asmag.com

Kamery kolorowe działające w skrajnie słabym oświetleniu, zaimplementowanymi algorytmami sztucznej inteligencji – wspierane AI przeszukiwanie wideo, redukcja fałszywych alarmów i analizy biznesowe – to wg tegorocznych respondentów cztery główne trendy w monitoringu wizyjnym. Większość biorących udział w ankiecie jako najbardziej dojrzałe i zrównoważone





ne rozwiązania wskazała kamery kolorowe działające w skrajnie słabym oświetleniu oraz wspierane AI przeszukiwanie wideo.

Wzrost znaczenia AI

To, że trzy z czterech najpopularniejszych trendów są związane z AI, pokazuje jej znaczenie w monitoringu wizyjnym. Algorytmy w ciągu ostatnich kilku lat radykalnie się poprawiły, dostarczając klientom bezprecedensową wartość w postaci alertów w czasie rzeczywistym, analiz biznesowych czy łatwego zarządzania materiałem wizyjnym z lepszą dokładnością. Według Adama Ringa, Sr. Manager, Tech Services and Sales Engineering w i-PRO Americas, technologia oparta na AI stanowi ewolucję technologiczną, która pobudza do innowacji. W przypadku monitoringu wizyjnego detekcja obiektów wsparta sztuczną inteligencją umożliwia zintegrowane wyszukiwanie osób i pojazdów do celów dochodzeniowych oraz dostarcza danych do analizy biznesowej.

– Kamery i-PRO niezawodnie wykrywają obiekty i rejestrują około 60 unikalnych atrybutów związanych z nimi – powiedział Adam Ring. – Dzięki temu operatorzy mogą szybko i wydajnie wyszukiwać obiekty, a także powiadamiać o zdarzeniach w czasie rzeczywistym, przy maksymalnym ograniczeniu fałszywych alarmów. Nasze oprogramowanie Active Guard prezentuje metadane AI w łatwym w użyciu interfejsie najpopularniejszych systemów VMS, np. oferowanych przez Genetec czy Milestone.

Zespoły ds. bezpieczeństwa i operatorzy mogą teraz zmienić swoją postawę z reaktywnej na proaktywną, aby reagować na zdarzenia, mając na celu przede wszystkim zapobieganie występowaniu incydentów. Kamery z AI mogą również dostarczać cenne informacje z zakresu analizy biznesowej zespołom zarówno marketingowym, jak i operacyjnym – dane o liczbie klientów w godzinach szczytu, czasie przebywania klienta w poszczególnych strefach, długości kolejek i wiele innych. Technologia jest sprawdzona, dojrzała i w sposób zasadniczy zmienia wartość systemów monitoringu wizyjnego.

– Spodziewamy się, że coraz więcej takich technologii, jak sztuczna inteligencja i uczenie maszynowe, będzie zyskiwać na popularności – wyjaśnił Vijay Dhamija, globalny lider inżynierii wideo w Honeywell Building Technologies. – Duży nacisk kładzie się na opracowywanie dopracowanych modeli sztucznej inteligencji z zaawansowanym wykrywaniem osób. To szczególnie ważne narzędzie, ponieważ coraz częściej nasze przestrzenie publiczne przywraca się do ich przeznaczenia sprzed pandemii.

Edge dodaje więcej wartości do analizy

Analityka przynosi klientom wiele korzyści, a dodatkowe atuty rozwiązań na brzegu sieci zapewniają jeszcze większą wartość. W miarę jak urządzenia brzegowe stają się coraz bardziej wydajne, przetwarzanie informacji na krawędzi sieci to trend widoczny we wszystkich dziedzinach.

– Redukcja kosztów w porównaniu z wdrażaniem serwerów do tych samych zadań jest znacząca. Analityka brzegowa, w szczególności wspomagana przez AI i uczenie maszynowe, zmienia zasady gry dla specjalistów ds. bezpieczeństwa, którzy mogą zrobić więcej, gdy są odciążeni od nużącej pracy. Przy monitorowaniu obrazów z tak wielu kamer mogą polegać na analizie, która powiadamia ich o zdarzeniach wymagających uwagi – powiedział Adam Ring. – Uważamy, że otwarta architektura staje się wymogiem w branży zabezpieczeń, ponieważ przyszłość musi być budowana na platformach, które bezproblemowo współdziałają z wieloma systemami i różnymi technologiami. Ponieważ żadna pojedyncza firma nie jest w stanie zapewnić najlepszych rozwiązań do każdego scenariusza, ważne, aby klienci mogli wybierać najlepsze w swojej klasie narzędzia, które pasują do ich potrzeb i wymagań, i móc je bez problemu zintegrować.

Firmy, które nie oferują otwartych systemów, są czasem traktowane podobnie jak platformy typu „usługa jako zakładnik”, ponieważ zmuszają użytkowników do korzystania z kamer, narzędzi i infrastruktury, stanowiących zazwyczaj kompromis w stosunku do oferty dostępnej na rynku. Największe szanse na wygranie przetargu mają dostawcy, którzy oferują niestandardowe rozwiązania dokładnie odpowiadające potrzebom użytkownika końcowego.

Więcej do chmury

Wraz z zainteresowaniem rozwiązaniami na brzegu sieci widać wzmożoną migrację do rozwiązań opartych na chmurze. Interesujące może być to, w jaki sposób firmy starają się zrównoważyć wykorzystanie chmury i rozwiązań brzegowych w przyszłości. Vijay Dhamija wyjaśnił, że nadal jest zauważalny wzrost popularności Cloud VSaaS i usługi bezpośredniego monitoringu wizyjnego w chmurze, ponieważ coraz więcej klientów czuje się komfortowo z ideą chmury i zdaje sobie sprawę z jej zalet. Obecnie jest tak dużo danych i tak wiele wymagań dotyczących zgodności, o których należy pamiętać, że przechowywanie

Badanie asmag.com

Ankieta dotycząca trendów technologicznych została przeprowadzona przez asmag.com w październiku 2022 r., a swoje opinie przedstawiło 323 jej uczestników. Respondenci składali się głównie z dystrybutorów (35%), integratorów/installatorów systemów (27%), konsultantów (21%), użytkowników końcowych (9%) oraz producentów (4%). Najbardziej reprezentowane były Azja i Oceania (58%), następnie EMEA (26%) i obie Ameryki (16%).

tych danych na miejscu staje się coraz trudniejsze i bardziej kosztowne.

– System oparty na chmurze łatwiej jest skonfigurować i utrzymać, jest bardziej opłacalny i wydajniejszy w zakresie raportowania oraz zgodności. Ponadto użytkownicy mogą uzyskać dostęp do systemów w chmurze z dowolnego miejsca i w dowolnym czasie – podkreślił Vijay Dhamija.

Trendy w urządzeniach

Mimo że to oprogramowanie jest w centrum uwagi, jeśli chodzi o postęp, daje się zauważyć również specyficzne trendy w zastosowaniu urządzeń. Przykładowo coraz powszechniejsze są kamery bi-spektralne, wykorzystujące termowizję i światło widzialne. Wcześniej mogły to być dwie osobne kamery, teraz ta sama kamera może wykonywać dwa różne zadania. Wykorzystanie niszowych rozwiązań, takich jak radar i LiDAR, również nabiera tempa w popularnych zastosowaniach w dziedzinie zabezpieczeń. Czujniki LiDAR mogą być wdrażane w szerokim zakresie, m.in. w dozorze zewnętrznym i wewnętrznym sektora bezpieczeństwa publicznego, do wykrywania intruzów w kontroli granicznej i ochronie obwodowej oraz kontroli dostępu.

– Dla Honeywell infrastruktura krytyczna stanowi największy rynek odbiorców LiDAR-ów, z głównymi segmentami obejmującymi centra danych, wytworzenie i dystrybucję energii, dystrybucję wody i usług komunalnych, obiekty elektrowni jądrowych oraz przetwórstwa ropy naftowej i gazu – powiedział Vijay Dhamija. – Inne kategorie obejmują budynki komercyjne, magazyny i kontrolę graniczną. W wielu środowiskach LiDAR będzie współistnieć z czujnikami biometrycznymi, oferując pełen zakres funkcji zabezpieczeń, od wczesnego wykrywania z dalekim zasięgiem po rozpoznawanie twarzy. Kamery zaczynają zawierać LiDAR, więc dodają kolejny poziom ochrony z dokładniejszym skanowaniem, zwiększoną percepcją głębi i innymi atutami.

Wnioski

Pojawienie się sztucznej inteligencji zrewolucjonizowało branżę telewizji dozorowej, radykalnie zwiększając jej funkcje i korzyści. Ostatnie badanie podkreśla ten fakt i wskazuje na przyszłość tego sektora z bardziej znaczącym wpływem oprogramowania. Jeśli chodzi o urządzenia, pojawi się więcej rozwiązań realizowanych w urządzeniach na brzegu sieci, ponieważ firmy starają się maksymalnie wykorzystać te możliwości. Połączenie technologii brzegowej, chmury i sztucznej inteligencji to kierunek w branży telewizji dozorowej. ☉

AVIGILON™



MOTOROLA
SOLUTIONS

venom
PSIM PLATFORM

Nowoczesne serwerownie wymagają systemu PSIM klasy High-End

Dowiedz się więcej na www.psim.pl





NAJWIĘKSZE FIRMY
branży security
na świecie

2022 S50	2021 S50	Nazwa firmy		SIEDZIBA	GŁÓWNY OBSZAR DZIAŁANIA	PRZYCHODY W 2021 R. (MLN USD)	PRZYCHODY W 2020 R. (MLN USD)	WZROST PRZYCHODÓW (2021-2020)
1	1	Hikvision Digital Technology		Chiny	różne	10 097,0	8636,2	16,9%
2	2	Dahua Technology		Chiny	różne	5 089,2	4102,0	24,1%
3	3	Assa Aloy (zamki elektromechaniczne i elektroniczne)		Szwecja	kontrola dostępu	3 320,4	3165,3	4,9%
4	4	Axis Communications		Szwecja	różne	1 362,9	1 347,1	1,2%
5	5	Motorola Solutions (telewizja dozorowa i kontrola dostępu)		USA	różne	1 226,0	927,0	32,3%
6	6	Uniview Technologies		Chiny	telewizja dozorowa	941,3	818,4	15,0%
7	7	Tiandy Technologies		Chiny	telewizja dozorowa	825,1	736,7	12,0%
8	8	Allegion (produkty elektroniczne i kontrola dostępu)		USA	kontrola dostępu	602,2	571,2	5,4%
9	10	Hanwha Techwin		Korea Płd.	telewizja dozorowa	593,4	462,8	28,2%
10	11	Alphone		Japonia	Interkomy	473,4	420,2	12,7%
11	17	Dongguan Yutong Optical Technology		Chiny	telewizja dozorowa (obiektywy)	319,6	228,1	40,1%
12	13	ZKTeco		Chiny	różne	303,1	279,2	8,5%
13	16	Intelbras		Brazylia	różne	292,8	207,3	41,2%
14	12	Infinova		Chiny	telewizja dozorowa	245,7	452,7	-45,7%
15	21	CP Plus		Indie	telewizja dozorowa	222,9	151,8	46,9%
16	19	Kedacom (telewizja dozorowa)		Chiny	telewizja dozorowa	201,5	172,5	16,8%
17	18	VIVOTEK		Tajwan	telewizja dozorowa	195,2	198,5	-1,7%
18	22	Milestone Systems		Niemcy	telewizja dozorowa	181,4	161,7	12,2%
19	20	Nedap		Holandia	różne	175,5	164,6	6,6%
20	27	TVT Digital Technology		Chiny	telewizja dozorowa	155,6	122,2	27,3%
21	24	IDIS		Korea Płd.	telewizja dozorowa	151,7	129,4	17,2%
22		Dnake		Chiny	interkomy	136,4	111,7	22,1%
23	23	Raysharp		Chiny	telewizja dozorowa	134,4	145,8	-7,8%
24	28	Optex (czujki)		Japonia	systemy alarmowe	124,3	105,2	18,2%
25	29	Commax		Korea Płd.	automatyka domowa	123,5	113,9	8,5%
26	30	Napco Security Technologies		USA	różne	114,0	101,4	12,5%
27	39	Gallagher		Nowa Zelandia	kontrola dostępu	113,1	87,6	29,0%

28		Jovision		Chiny	telewizja dozorowa	112,2	111,2	0,8%
29	31	BCDVideo		USA	telewizja dozorowa	108,7	101,1	7,5%
30	33	Identiv		USA	kontrola dostępu	103,8	86,9	19,4%
31	35	Zenitel		Norwegia	interkomy	92,4	86,2	7,2%
32	38	Suprema		Korea Płd.	kontrola dostępu	90,3	73,4	23,1%
33	25	Tamron (obiektywy)		Japonia	telewizja dozorowa (obiektywy)	85,2	82,6	3,2%
34	32	KOCOM		Korea Płd.	Home Security & Automation	80,9	103,9	-22,1%
35		EVETAR		Chiny	telewizja dozorowa (obiektywy)	77,7	64,6	20,1%
36	36	Mobotix		Niemcy	telewizja dozorowa	73,8	83,2	-11,3%
37	41	Foctek Photonics		Chiny	telewizja dozorowa (obiektywy)	70,6	56,5	25,0%
38	42	BlueSky Technologies		Chiny	telewizja dozorowa	68,2	54,6	24,9%
39	43	DynaColor		Tajwan	telewizja dozorowa	61,1	42,1	45,1%
40	40	Costar Technologies		USA	telewizja dozorowa	52,9	60,4	-12,3%
41	37	C-PRO Electronics		Korea Płd.	telewizja dozorowa	45,6	74,1	-38,4%
42	44	GeoVision		Tajwan	telewizja dozorowa	44,6	41,4	7,7%
43	48	Senstar Technologies		Izrael	różne	34,9	33,4	4,7%
44	46	Hi Sharp Electronics		Taiwan	telewizja dozorowa	33,4	29,4	13,5%
45	45	Synectics (System Division)		Wlk. Brytania	telewizja dozorowa	28,4	32,5	-12,6%
46	47	ITX AI		Korea Płd.	telewizja dozorowa	27,4	28,1	-2,4%
47	49	Hitron Systems		Korea Płd.	telewizja dozorowa	24,0	23,8	0,7%
48		Evolv Technologies		USA	systemy screeningowe	21,8	3,9	456,0%
49		Ava Group (systemy perymetryczne i kontrola dostępu)		Australia	różne	19,5	16,7	17,1%
50		Webgate		Korea Płd.	telewizja dozorowa	18,8	13,1	43,1%

→ 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 2021, wyróżnia zarówno światowych liderów, jak i nowe podmioty na rynku. Ranking odzwierciedla 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 branżowych, 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, zbadane 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 2020-2021. ➡

50²⁰²²
SECURITYSECURITY
50TOP 10 producentów
z sektora
telewizji dozorowej
i kontroli dostępuGłówne trendy na rynku
zabezpieczeń technicznych w roku 2023

WILLIAM PAO

asmag.com



Rok 2022 przyniósł wprawdzie wyraźny wzrost przychodów dla większości firm z listy Security 50, jednak kończy się dla branży security problemami, które w nadchodzącym roku będą stanowić poważne wyzwania.

Po analizie tegorocznej listy Security 50 należy stwierdzić, że największe firmy utrzymały swoje pozycje z poprzedniego roku. W pierwszej 10 największych producentów w sektorach telewizji dozorowej i kontroli dostępu (na podstawie przychodów ze sprzedaży produktów w 2021 r.) są Hikvision Digital Technology, Dahua Technology, ASSA ABLOY, Axis Communications, Motorola Solutions, Uniview Technologies, Tiandy Technologies, Allegion, Hanwha Techwin i Aiphone. Warto odnotować, że przychody Hikvision w roku finansowym 2021/2022 przekroczyły 10 mld USD, osiągając 10,1 mld USD, co w porównaniu z 8,64 mld USD w 2020/2021 r. oznacza wzrost o 16,9 proc.



Security 50 2022 r. TOP 10 producentów o najwyższych przychodach w sektorze telewizji dozorowej i kontroli dostępu

– Wierzymy, że innowacje technologiczne są kluczowym elementem udanego rozwoju firmy. Nasze innowacyjne produkty i rozwiązania tworzą dodatkową wartość dla klientów, pomagają organizacjom poprawić bezpieczeństwo, zwiększyć wydajność operacyjną i osiągać zrównoważony rozwój. Cieszymy się, że klienci nadal mają do nas zaufanie, to motywuje do rozwoju firmy – powiedział Frank Zhang, wiceprezes Hikvision Digital Technology. – Zarówno w zeszłym, jak i tym roku pojawiło się więcej czynników zewnętrznych, które budzą niepewność, ponieważ inflacja, wzrost stóp procentowych i zmiany kursów walut niekorzystnie wpływają na gospodarkę światową. Dzięki optymalizacji naszych działań z ulepszonymi elastycznymi procesami produkcyjnymi, logistyką i usługami lokalnymi Hikvision z powodzeniem utrzymuje dostawę produktów. Konsekwentnie inwestujemy w badania i rozwój, a wydatki na te cele stanowią ponad 10% całkowitych przychodów w 2021 r. Wyśiłki te zapewniły stały rozwój firmy.

W tym roku do listy Security 50 dołączyło sześć firm: chińskie Dnake (interkom), Jovision (wideo) i EVETAR (obiektywy), a także Evolv, dostawca systemów screeningowych z siedzibą w USA, Ava Group, australijski dostawca rozwiązań do zarządzania ryzykiem, oraz Webgate, koreańska firma zajmująca się systemami monitoringu wizyjnego.

W tegorocznym rankingu Security 50 znalazło się 15 chińskich firm, cztery z nich uplasowały się w pierwszej dziesiątce (Hikvision, Dahua, Uniview i Tiandy). Większość firm z Państwa Środka odnotowała wzrost w 2021 r., co wskazuje, że wpływ sankcji handlowych nałożonych przez USA na chińskie towary był ograniczony.

Warto zauważyć, że w pierwszej połowie roku 2022 wiele chińskich firm odnotowało roczne spadki przychodów. W tym okresie Hikvision uzyskał całkowity zysk netto w wysokości 848,6 mln USD, co oznacza spadek o 11,14% w porównaniu z pierwszą połową 2021 r., chociaż jego przychody w I półroczu 2022 r. wzrosły o 9,9% rok do roku.

Ma to jednak większy związek z pandemią COVID-19 w Chinach i innymi problemami niż z konfliktem handlowym.

– Spadki wynikają z warunków panujących na chińskim rynku krajowym, a nie z ceł i ograniczeń handlowych z USA. W pierwszej połowie 2022 r. w kilku głównych miastach chińskich pojawiły się ograniczenia w poruszaniu się związane z nasileniem pandemii. W związku z tym wydatki rządowe zostały przekierowane z innych obszarów na walkę z COVID-19 i wspieranie gospodarki podczas blokad – skomentowali Josh Woodhouse, główny analityk i założyciel firmy Novaira Insights, oraz Jon Cropley, analityk w tej firmie.

Wszyscy zastanawiają się też, czy na konflikcie pomiędzy USA a Chinami zyskają tajwańscy producenci z branży zabezpieczeń. Może tak się wydawać, ponieważ niektóre tajwańskie firmy, m.in. Dynacolor, Hi Sharp i GeoVision, odnotowały wzrost w 2021 r. Jednak biorąc pod uwagę mniejszą skalę i moce produkcyjne tajwańskich zakładów, dopiero się okaże, czy będą nadal czerpać korzyści z zamówień OEM-owych przeniesionych z Chin. W rzeczywistości większość tajwańskich firm zmieniła strategię, aby tworzyć niszowe rozwiązania z wartością dodaną, np. w inteligentnym transporcie, co było jednym z czynników przyczyniających się do ich sukcesu.

Powrót tendencji wzrostowej

W latach 2021–2022 po złagodzeniu skutków pandemii zanotowano powrót do poziomu sprzed dwóch lat.

– Dzięki większej dostępności szczepionek i metod leczenia COVID-19 wiele firm mogło zmienić swoje strategie biznesowe w kierunku tworzenia bezpiecznego środowiska pracy dla pracowników i klientów powracających do przestrzeni fizycznej, jednocześnie utrzymując (a nawet rozszerzając) rozwiązania zdalne wdrożone w szczytowym okresie pandemii – powiedziała Danielle Van Zandt, starszy analityk branżowy ds. bezpieczeństwa w firmie Frost & Sullivan. – W przypadku wielu rynków wydatki i możliwości inwestycyjne na zabezpieczenia elektroniczne osiągnęły poziom sprzed pandemii, natomiast dzięki upowszechnieniu cyfryzacji wzrosło zainteresowanie niektórymi technologiami.



mi. W tym roku rozwinęły się takie dziedziny, jak biometria, kontrola dostępu, analiza wideo i cyfrowa inteligencja.

Na światowych rynkach obserwuje się zwiększony popyt.

– Jednym z czynników na to wpływających jest ogólne rosnące zainteresowanie systemami sieciowymi. Kolejnym motorem napędowym jest rozwój technologii. Popyt na nasze produkty rośnie, ponieważ opracowujemy nowe innowacyjne produkty i rozwiązania, które spełniają potrzeby klientów – ocenił Ray Mauritsson, dyrektor generalny Axis Communications.

Prognoza na rok 2023: Przed branżą security stoją wyzwania

Gdy wydawało się już, że koszmar pandemii dobiega końca, pojawiły się nowe problemy, które mają wpływ na różne branże, w tym również zabezpieczeń technicznych. Gwałtowny wzrost popytu po COVID-19, a także konflikty regionalne wywołały kryzys w łańcuchach dostaw. Wyzwaniem jest też wymykająca się spod kontroli powszechna inflacja, rosną ceny energii, żywności i produktów konsumpcyjnych. Aby ograniczyć inflację, stopy procentowe zostały podniesione do poziomu najwyższego od lat, a to zapowiada recesję. Rzeczywiście świat, jaki znaliśmy przed COVID-em, zmienił się i mimo wzrostu na rynku security wspomniane wyzwania nie wróżą dobrego nadchodzącego roku.

Problemy z łańcuchem dostaw

Branża zabezpieczeń stoi obecnie w obliczu wyzwań, a jednym z nich, największym od dziesięcioleci, jest kryzys łańcucha dostaw.

– Podobnie jak wiele innych firm, nas też dotknęły problemy związane z ciągłością łańcucha dostaw. Najpoważniejszymi przyczynami zakłóceń były blokady i inne działania spowodowane pandemią. Ważnym czynnikiem był również niedobór komponentów, który pandemia pogłębiła. Przeprojektowanie produktu i zakupy podzespołów na rynku lokalnym to przykłady minimalizacji skutków niedoborów. Dłuższy czas realizacji zamówień doprowadził do wolniejszego niż oczekiwano wzrostu w latach 2020–2021. Ponieważ zaczynamy dostrzegać poprawę w naszym łańcuchu dostaw, spodziewamy się powrotu do dwucyfrowego wzrostu – powiedział Ray Mauritsson.

Dla branży zabezpieczeń elektronicznych, zwłaszcza dla producentów urządzeń, spośród niedoborów wszystkich komponentów szczególnie dotkliwy był brak półprzewodników.

– Ograniczenia pandemiczne w przemieszczaniu się spowodowały zainteresowanie zakupem elektroniki użytkowej. Ludzie potrzebowali laptopów do pracy w domu i do nauki w domu, więcej swoich dochodów przeznaczali też na rozrywkę domową. Ten sprzęt wymaga podzespołów półprzewodnikowych, stąd ogromny wzrost zapotrzebowania na nie. Dostawcy urządzeń do systemów monitoringu wizyjnego stanowili tylko jedną z grup konkurujących o dostawy układów scalonych. Największymi ich odbiorcami i zarazem konkurentami byli producenci samochodów i smartfonów – stwierdzili zgodnie Josh Woodhouse i Jon Cropley.

– Jeśli chodzi o podzespoły, niedobory odczuwano w dostawach chipów do wszelkiego typu procesorów potrzebnych do analityki wizyjnej, przystosowanych do potrzeb AI czy urządzeń brzegowych. Te rozwiązania cieszą się dużym zainteresowaniem klientów, dlatego terminowe zabezpieczanie dostaw podzespołów stało się kluczowym wyróżnikiem projektów, które wygrały w ostatnim roku. Zwycięzcami byli ci dostawcy, którzy potrafili zdywersyfikować swoje łańcuchy dostaw i nie odczuć wpływu logistycznej zmiany tras na całym świecie – powiedziała Danielle VanZandt.

Inflacja

Inflacja uderza w wiele branż, w tym sektor zabezpieczeń.

– Na cenę urządzeń do monitoringu wizyjnego wpływa obecnie presja inflacyjna w całej gospodarce. Ceny mediów, koszty robocizny i surowców szybko rosną. Dostawcy urządzeń będą zmuszeni podnieść ceny swoich produktów. Kamera sieciowa będzie droższa zarówno w 2022, jak i 2023 r. – przewidyują Josh Woodhouse i Jon Cropley.

W obliczu wzrostu cen, firmy z branży security musiały zmienić strategię i zastanowić się nad sposobami zatrzymania klientów.

– Inflacja spowodowała wzrost kosztów we wszystkich dziedzinach, również komponentów do produkcji urządzeń. Aby go zrównoważyć, wielu dostawców i integratorów podniosło ceny. Ponieważ wiele projektów miało dłuższe ramy czasowe niż zwykle, mogą zaoferować klientom bardziej elastyczny model płatności – zauważyła Danielle VanZandt. – Ponadto branża w dużej mierze skupiła się na poprawie ogólnej obsługi klienta, w tym na oferowaniu bardziej spersonalizowanych modeli usług. To podejście nie tylko wpisuje się w ogólne trendy w branży, ale także pomaga dostawcom zapobiegać utracie wielu klientów.

Inne wyzwania

Konflikty geopolityczne w niektórych częściach świata również odbiły się na podmiotach działających na branżowym rynku.

– Bieżące problemy geopolityczne, które uważnie obserwujemy, wywołują niepokój i niepewność. Podobnie jak wiele innych firm, zawiesiliśmy działalność biznesową w Rosji z powodu inwazji na Ukrainę – powiedział Ray Mauritsson.

Na całą branżę zabezpieczeń wpływa również perspektywa potencjalnych nowych przepisów dotyczących ochrony danych osobowych, które różnią się w poszczególnych krajach.

– Z tego powodu dostawcy muszą tworzyć nowe rozwiązania z nieodłącznymi funkcjami ochrony prywatności wymaganymi w danym kraju albo projektować elastyczne rozwiązania, by móc wprowadzać szybkie zmiany w celu spełnienia wszelkich pojawiających się nowych wymagań – stwierdziła Danielle VanZandt.

Niepewne perspektywy wzrostu

Branża zabezpieczeń elektronicznych w tym roku znów odnotowuje wzrosty. Jeśli zaś chodzi o rok przyszły, przewidywania wydają się niepewne.

– W pierwszej połowie roku nasza długoletnia zagraniczna działalność nadal rozwijała się szybko, gdyż była dobrze zakorzeniona. Kontynuowano też promowanie strategii biznesu lokalnego oraz ulepszano ciągłość globalnego łańcucha dostaw, wdrażając różne systemy wspierające. Możliwości biznesowe w regionie Azji i Pacyfiku, Afryce, Ameryce Łacińskiej i na Bliskim Wschodzie są względnie optymistyczne, ale są też regiony o stosunkowo słabym wzroście – powiedział Fu Liquan, prezes Dahua Technology. – Patrząc w przyszłość, firmy zagraniczne będą nadal borykać się z czynnikami regionalnymi, inflacją i innymi wyzwaniami. Ale rynek globalny jest ogromny, ma liczne możliwości, które w dłuższej perspektywie mogą przynieść wzrosty.

Biorąc pod uwagę wspomniane wyzwania, prawdopodobnie nastąpi korekta dotycząca rozwoju rynku.

– Przewiduje się, że światowy rynek urządzeń i oprogramowania do monitoringu wizyjnego wzrośnie w 2022 r.

o 11,7%. Problemy gospodarcze będą miały wpływ zarówno na publiczne, jak i prywatne wydatki na te systemy w 2023 r. Jednocześnie utrzyma się presja inflacyjna. Światowy rynek wzrośnie w tej dziedzinie prawdopodobnie o 6,4% w 2023 r. – stwierdzili Josh Woodhouse i Jon Cropley.

– Nie spodziewam się, by w roku 2023 nastąpił całkowity spadek ogólnych wskaźników wzrostu w branży, ale trzeba się liczyć z korektą rynkową i obniżeniem wskaźników z wysokich dwucyfrowych wartości do bardziej zrównoważonych i znaczących 8–9% rok do roku – oceniła Danielle VanZandt, dodając, że chociaż wyzwania pozostaną, to pojawiają się także nowe możliwości. – Obawy związane z inflacją, wyzwania dotyczące utrzymania ciągłości łańcucha dostaw i niestabilność na światowym rynku energii powodują, że firmy wstrzymują wiele nowych inwestycji w zabezpieczenia, dopóki nie przekonają się, jaki ta sytuacja wpłynie na ich budżety i wyniki finansowe. Dostawcy mogą nawiązać znacznie bliższą współpracę z ich obecnymi klientami w celu określenia sposobów ulepszenia stosowanych przez nich rozwiązań. Dostaną informacje zwrotne, np. jakie potencjalnie nowe funkcje mogą wprowadzić lub zaoferować testowanie nowych możliwości – dodała Danielle VanZandt.

Sekrety sukcesu najlepiej rozwijających się firm



WILLIAM PAO

asmag.com



Na podstawie tegorocznej listy Security 50 można stwierdzić, że branża zabezpieczeń rośnie. W zestawieniu ubiegłorocznym po raz pierwszy od lat więcej było firm, bo aż 28, które odnotowały spadek przychodów. Teraz sytuacja jest już inna: w 2021 r. zdecydowana większość firm osiągnęła wzrost przychodów w ujęciu rok do roku, co potwierdza powrót tendencji sprzed pandemii.

– W II połowie ub. roku nasza firma miała doskonałe wyniki w regionie EMEA, tendencja wzrostowa utrzymuje się też w 2022 r. Wyjście z dwuletniej blokady po pandemii sprawiło nam ulgę. Możliwość bezpośrednich spotkań z partnerami i klientami miała kluczowe znaczenie dla naszej strategii sprzedaży w pierwszej połowie roku – powiedział Jos Beernink, wiceprezes Milestone Systems na region EMEA.

– Wzrost przychodów firmy Identiv przyspiesza, odzwierciedlając naszą stałą pozycję lidera w zakresie specjali-

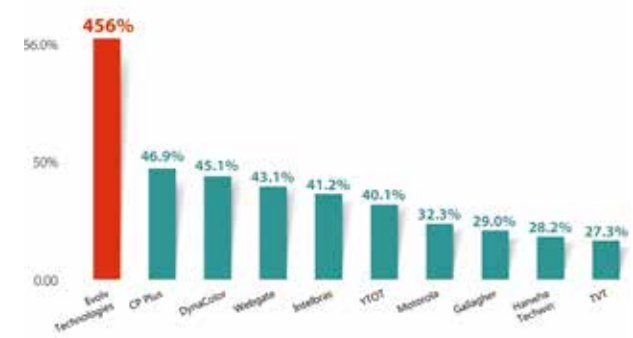
Jeśli chodzi o trendy na przyszły rok, na rynku nadal będą dominować sztuczna inteligencja, przetwarzanie brzegowe, chmura i cyberbezpieczeństwo. Kolejnym zjawiskiem będzie podejście wieloaspektowe.

– Z perspektywy Hikvision podejście wieloaspektowe umożliwi branży security przejście na wyższy poziom. Oprócz obrazowania w świetle widzialnym więcej możliwości da dodawanie do urządzeń security obrazowania termowizyjnego lub radaru, pomiaru temperatury, wilgotności czy detekcji wycieku gazu. Dzięki temu systemy dozoruwe stają się potężniejsze – powiedział Frank Zhang. – Poznawanie środowiska zewnętrznego, identyfikowanie zdarzeń i dostarczanie bardziej szczegółowych informacji stwarza nowe możliwości wykorzystania systemów dozoru w coraz szerszych zastosowaniach. Rozszerzamy nasze technologie percepcji maszynowej na pełne spektrum elektromagnetyczne, opracowaliśmy innowacyjne produkty i aplikacje, które wychwytyją promieniowanie rentgenowskie, promienie podczerwone, milimetrowe fale radarowe i fale dźwiękowe.

stycznych zastosowań RFID dla sektora IoT. Rozwijamy się znacznie szybciej, co oznacza, że przejmujemy udziały innych firm działających w tym segmencie rynku – stwierdził Steve Humphreys, dyrektor generalny Identiv. – W ostatnim kwartale 2021 nasze przychody z RFID wzrosły o 41% rok do roku, o 20% zwiększył się udział w rozwiązaniach dla lokali użytkowych. Zanotowaliśmy przychody o 16% większe rok do roku.

Strategie na rzecz wzrostu

W ubiegłym roku 40 firm z tegorocznego Security 50 odnotowało wzrosty, przy czym 28 osiągnęło wynik dwu-, a nawet trzycyfrowy. Wśród 10 firm z sektorów telewizji dozoruwej i kontroli dostępu o najbardziej dynamicznym wzroście w 2021 r. znalazły się: Evolv Technologies, CP Plus, Dynacolor, Webgate, Intelbras, Dongguan Yutong Optical Technology, Motorola Solutions, Gallagher, Hanwha Techwin i TVT Digital Technology.





Pierwszy w tym zestawieniu Evolv, dostawca systemów do wykrywania broni, w 2021 r. uzyskał przychody w wysokości 21,77 mln USD w porównaniu z 3,92 mln USD w 2020 r. Wzmoczone wysiłki firmy w zakresie pozyskiwania klientów i ekspansja na kluczowe rynki przełożyły się na gigantyczny wzrost o 455,98% w ujęciu rok do roku.

Spryt i szybkość reakcji

Kluczowe znaczenie w obliczu pojawiających się przeciwności losu ma wykazanie się sprytem i szybkością reakcji.

– W ostatnich kilku latach wiele się działo. Najpierw, w 2020 r., radziliśmy sobie z pierwszą fazą pandemii, w 2021 r. z drugą. Na szczęście nasz łańcuch dostaw pomógł nam przetrwać te lata. Udało się nam wyprzedzić zamknięcie i zamówić w przedsprzedaży 4-krotność miesięcznych zamówień dla naszych głównych dostawców, gdy usłyszeliśmy, że eksperci Światowej Organizacji Zdrowia jadą do Wuhan w Chinach. Dwa dni po złożeniu przez nas zamówień nastąpił lockdown. Tak więc zapasy były z pewnością ważnym czynnikiem sukcesu, podobnie jak posiadanie zespołów produkcyjnych chętnych do przebywania w naszej centrali i tworzenia produktów na zamówienia klientów – powiedział Jeff Burgess, założyciel i dyrektor generalny BCDVideo.

Tworzenie wartości biznesowej dla klientów

Kolejnym kluczem do sukcesu jest tworzenie dodanej wartości dla klientów, aby nadal korzystali z rozwiązań od zaufanego dostawcy.

– Wraz z rosnącą zdolnością do umiętnego wdrażania AI i stałym wysiłkiem w odkrywaniu nowych wartości danych zbieranych z elektronicznych systemów zabezpieczeń firma Dahua stopniowo rozszerza swoją działalność w obszarze tradycyjnego security o zarządzanie przedsiębiorstwem. Pomagamy zmniejszać koszty i zwiększać wydajność, dzięki czemu rośnie wartość biznesowa naszych klientów – powiedział Fu Liquan, prezes Dahua Technology.

Według S. Humphreysa zaangażowanie w tworzenie wartości dodanej dla klienta pozwoliło firmie osiągnąć wzrost nawet w warunkach największego od pokoleń globalnego kryzysu łańcucha dostaw.

– Rzeczywistość jest taka, że od 1972 r. nie odczuwaliśmy tak poważnych zaburzeń w łańcuchach dostaw. Branża RFID jest zdominowana głównie przez firmy, które chcą uzyskać prosty projekt, a następnie wyprodukować go w setkach milionów. Z biznesowego punktu widzenia to nie było naszym celem częściowo dlatego, że nie tam są marże – powiedział S. Humphreys. – Wchodząc na rynek, strategię biznesu opieramy na rozwiązaniach oferujących wyższą wartość dodaną. Dobrze czujemy się w długich cyklach sprzedaży. Rozumujemy, że klienci rozpoczynający inwestycję niekoniecznie muszą wiedzieć, co mogą jeszcze osiągnąć. Nasz proces sprzedaży oparty jest na współpracy i know-how.

Zaangażowanie w innowacje technologiczne

Ściśle związana z tworzeniem wartości jest innowacyjność technologiczna, która pozwala firmom dostarczać produkty i rozwiązania dostosowane do indywidualnych potrzeb użytkowników.

– Identiv projektuje i dostarcza produkty nowej generacji, które otwierają drogę rozwiązaniom IoT. Jesteśmy firmą wysoce

techniczną, co pomaga nam zdobyć większy udział w rynku – ocenił S. Humphreys. – Z technologią, która jest rdzeniem naszej działalności, spotykamy się każdego dnia, zwłaszcza w przypadku RFID w obiektach użytkowych. Mamy jednych z najbardziej innowacyjnych i błyskotliwych inżynierów, którzy zajmują się badaniami i rozwojem, chociaż znalezienie talentów jest dużym wyzwaniem w branży zabezpieczeń. Ci inżynierowie sprawiają, że technologia jest głębiej osadzona, efektywniej wykorzystana, staje się wszechobecna, dzięki czemu bezpieczeństwo jest kompleksowe.

Respektowanie lokalnych przepisów

Dla firm prowadzących działalność w skali globalnej przestrzeganie lokalnych przepisów jest kluczem do zapewnienia wzrostu w działalności zagranicznej.

– W obliczu złożonej i zmieniającej się sytuacji polityczno-gospodarczej musimy mieć rozwiązania dostosowane do przepisów prawa i zwyczajów różnych krajów. Aby spełnić wymagania zgodności, Dahua przyjmuje podejście „jeden kraj, jedna polityka” – powiedział Fu Liquan. – Firma nadal wzmacnia strategię zatrudniania pracowników lokalnych, tworząc międzynarodowy zespół marketingu i zarządzania, a także lokalne centra marketingowe i usługowe, aby eksplorować globalny rynek. Globalizacja i działalność na rynkach zagranicznych przyczynią się również do przyszłego wzrostu biznesowego firmy.

Kontynuacja wzrostu

Większość firm wyraziła nadzieję, że tendencja wzrostowa w 2023 r. będzie kontynuowana.

– Jesteśmy optymistami co do rynku zabezpieczeń, ponieważ AI i Machine Learning otwierają zupełnie nową skalę możliwości, rozwiązań i integracji w zakresie bezpieczeństwa i poza nim – powiedział Jos Beernink. – Dostrzegamy to, że nasi klienci z branży transportowej, np. w portach lotniczych, stoją przed ogromnymi wyzwaniami związanymi z utrzymaniem sprawności operacyjnej, a jednocześnie muszą mierzyć się z brakiem pracowników w konfrontacji z olbrzymią liczbą pasażerów. To właśnie powoduje zapotrzebowanie na wsparcie ich inteligentnymi rozwiązaniami VMS w zakresie bezpieczeństwa. Security Managerowie na naszych rynkach mogą zrobić więcej, dysponując mniejszymi zasobami. W Milestone Systems mamy świetne rozwiązania, które spełniają te oczekiwania rynku.

– W ciągu ostatnich dwudziestu lat przeżyliśmy już tsunami w Japonii, pożary fabryk, recesję i wybory prezydenckie. W zasadzie widzieliśmy już tak dużo, że chyba jesteśmy na wszystko przygotowani. Jednak stawiamy sobie kolejne wyzwania, aby wprowadzać na rynek więcej nowości, takich jak uniwersalny NVR, którego premiera odbędzie się w czwartym kwartale 2022 r., czy zewnętrzna pamięć masowa Deepstor. Pozwoli to rozszerzyć sprzedaż produktów naszej marki na całym świecie. Dlatego w 2023 r. prognozujemy 20-proc. wzrost rok do roku – wyjaśnił Jeff Burgess z BCDVideo. 

Efektywna ochrona przeciwkradzieżowa

Elektroniczne systemy zabezpieczeń



- Systemy anten w technologii AM / RF
- Wysoka czułość, niskie prawdopodobieństwo fałszywego alarmu
- Wyjątkowa precyzja, wysoka odporność na zakłócenia
- Integracja z kamerami CCTV i oprogramowaniem DSS PRO*
- Regulacja głośności i podświetlenia alarmowego

*1) wybrane modele

Nowe modele anten

Seria ISC-EAA2 (AM)
Seria ISC-EAA6/EAR6 (AM / RF)
Seria ISC-EAA8/EAR8 (AM / RF)

Nasze systemy przeciwkradzieżowe sprawdzają się w każdej przestrzeni, niezależnie od tego, czy mowa o supermarkecie, aptece, drogerii, sklepie odzieżowym czy przechowalni bagażu.

Dahua Technology Poland Sp. z o.o.

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





Handel przyszłości

na wyciągnięcie ręki

Co jest wyznacznikiem udanych zakupów? Z pewnością cena produktu, szeroki wybór towarów, mnogość opcji, a także łatwość i przyjemność dokonywania wyboru. A gdyby to wszystko było dostępne zawsze, niezależnie od pory dnia i godziny, a do tego okraszone szczyptą prywatności i możliwością swobodnego decydowania o własnych wyborach? Brzmi jak utopia? Od jakiegoś czasu już niekoniecznie...



Michał Marciniak

WYZWANIE?

Handel detaliczny każdego dnia mierzy się z coraz większymi wyzwaniami. Po pierwsze, personel: rekrutacja i utrzymanie pracownika to dziś nie lada wyczyn/zadanie, a częsta rotacja nie ułatwia budowania trwałych i zgranych zespołów. Po drugie, wszechobecna inflacja i rosnące koszty. Z każdej strony zaskakują nas podwyżki, które zmieniają cały rynek, powodując próby dostosowania się do nowych realiów albo zamykania działalności gospodarczych. Po trzecie, przepisy prawne. Tutaj zdania są podzielone, głównie w kontekście handlu w niedziele i święta. Większość znanych mi osób z kręgu retail opowiada się zdecydowanie za wolnymi ustawowo niedzielami, ale są i tacy, którzy preferują dokonywanie zakupów właśnie tego dnia. Oczywiście można powiedzieć, że to tylko kwestia organizacji czasu, jednak ile osób, tyle różnych opinii. Te trzy punkty to tylko wierzchołek góry lodowej. Handel mierzy się z tysiącem innych – mniejszych bądź większych wyzwań, jednakże te trzy wiodą prym, jeśli chodzi o próbę znalezienia panaceum na problemy w tym obszarze.

ROZWIĄZANIE?

Ludzie są kreatywni i chcą ułatwiać sobie życie. Cechy te powodują czy też stają się pretekstem do zmian, często rewolucyjnych czy po prostu ewolucyjnych. Brak pracowników? Osoby zza wschodniej granicy okazały się świetną alternatywą dla tego (i nie tylko tego) sektora, uzupełniając braki personalne w wielu sklepach. Wprawdzie obecna sytuacja związana z konfliktem wojennym zmniejszyła liczbę potencjalnych kandydatów, jednakże nadal stanowią oni znaczący wolumen, aczkolwiek obwarowany ryzykiem fluktuacji w związku z decyzjami politycznymi.

Inflacją zarządza się dużo trudniej. Rosnące koszty paliw czy energii przekładają się na wzrost cen produktów i usług. Rezygnacja z powierzchni sprzedażowych (był to zauważalny trend już w czasie pandemii koronawirusa) i przejście do sprzedaży zdalnej lub w systemie dostaw z lokalnie rozmieszczonych magazynów stanowi coraz większy udział w rynku.

Kwestie ustawowe aż się proszą o swobodną interpretację, co jest nagminnie wykorzystywane przez działy prawne dużych firm. Pokłósiem tego byłyby rozmieszczone w całym kraju (wręcz na każdym kroku) „urzędy pocztowe”, w których przy okazji zakupu kaszanki i bochenka chleba można było odebrać i nadać paczkę (choć często pracownicy nie wiedzieli, jak obsłużyć takie zadanie).

ROZWIĄZANIE!

A gdyby tak wszystkie wskazane problemy (czy też wyzwania) należały do przeszłości? Co ciekawe, jest to możliwe już teraz dzięki wykorzystaniu obecnych rozwiązań i technologii. Odpowiedzią na większość bolączek segmentu retail są sklepy autonomiczne. Czym się cechują, czym tak właściwie są? Synonimami słowa „autonomiczny” są „samowystarczalny, samodzielny, samoistny, oddzielny” itp. Daje to jasny sygnał, że dążymy w tym przypadku do stworzenia produktu niezależnego, niewrażliwego na czynniki zewnętrzne i działającego w swoim ekosystemie. Zadanie polegające na opracowaniu takiego produktu wydaje się skomplikowane i... takie też jest! Produkt ten wymaga zdecydowanie więcej wysiłku technologicznego na etapie początkowym, jednak korzyści płynące z jego stosowania rekompensują w krótkim czasie proces wdrożenia. Ale po kolei.

Wyzwanie: uruchomienie sklepu bezobsługowego, otwartego 24/7, mającego szeroki asortyment i dającego klientowi przyjemność dokonywania wyborów.

Rozwiązanie: sieć sklepów autonomicznych zarządzanych lokalnie tylko przez obsługę merchandisingową oraz zewnętrznie (zdalnie) poprzez nadzorowanie/monitorowanie działania systemów wykorzystywanych do obsługi klientów.

Na tym etapie należy wyjaśnić, o jakich systemach i rozwiązaniach mowa. Obecnie tylko kilka firm na świecie tworzy systemy autonomiczne dla branży handlu detalicznego bazujące na uczeniu maszynowym i sztucznej inteligencji, a jeszcze mniej wdrożyło je z sukcesem w praktyce, samodzielnie lub we współpracy z sieciami sklepów.

Działają one najczęściej w dwójaki sposób: śledzą i reagują na zachowania klientów w sklepie oraz rozpoznają wybierane produkty. Wszystko opiera się na dedykowanym systemie kamer i czasami zestawie czujników IoT, np. systemach wa-

gowych w półkach. Z punktu widzenia unijnych realiów rozwiązania te są zgodne z regulacjami RODO. Przetwarzanie danych oparto na wirtualnych modelach postaci (brak danych wrażliwych), a system rozpoznawania produktów reaguje tylko na elementy zapisane w sklepowej bazie.

Takie sklepy w zasadzie wymagają tylko dwóch rzeczy, aby być w pełni funkcjonalne – dostępu do Internetu i prądu. Lokalizacja może być dowolna: strefy biurowe, mobilne formy kontenerowe, klasyczne sklepy będące częścią budynku, centra logistyczne i fabryki. Ograniczają nas tylko wyobrażenia i analizy wcześniejszych badań dotyczących przepływu potencjalnych klientów. Jedyny kontakt personelu ze sklepem jest przy zatowarowaniu lub serwisowaniu, a te czynności można zaplanować. Tym samym personel może objąć swoim zasięgiem większą liczbę punktów. Minimalizujemy też wymagania na dodatkowe pomieszczenia, gdyż w tym przypadku nie jest konieczne zaplecze sanitarne, nie wspominając o tym, że nie borykamy się z brakami personelu, urlopami, zwolnieniami lekarskimi itd.

Sam proces dokonywania zakupów jest prosty i nie wymaga specjalnej wiedzy technicznej. Przed wejściem do sklepu klient skanuje kod z dedykowanej aplikacji lub przykładą kartę płatniczą. System go weryfikuje i drzwi się otwierają. Po wejściu wybiera towar i... kieruje się do wyjścia. Przez cały czas działa technologia śledzenia klientów i rozpoznawania produktów. Po procesie zakupowym klient otrzymuje rachunek w aplikacji lub w formie SMS-a. Jako ciekawostkę warto dodać, że zakupy mogą być realizowane w mniej niż 30 sekund. Proszę wyobrazić sobie tę oszczędność czasu chociażby w roku!

KONKLUZJA

Czy sklepy autonomiczne oznaczają koniec tradycyjnego handlu opartego na bezpośrednim kontakcie sprzedawca-klient? To dość częste pytanie. Odpowiedź brzmi: absolutnie nie! Głównym zamyśleniem rozwiązania jest uzupełnienie oferty klasycznych sklepów detalicznych poprzez lokowanie sklepów autonomicznych w miejscach, gdzie handel może odbywać się przez 24 h/dobę (dworce, szpitale, przejścia podziemne itd.), lub jest nasilony tylko w określonych porach dnia. Są też miejsca, gdzie handel powinien być dostępny przez cały dzień, jednak ze względów ekonomicznych nieoptyczne jest zatrudnianie sprzedawców (oddalone centra magazynowe, fabryki, zakłady produkcyjne itp.).

Ciekawym podejściem jest również model hybrydowy – w ciągu dnia (np. w godzinach pomiędzy 6.00 a 23.00) klient jest obsługiwany przez regularny personel, a po godz. 23.00 sklep przechodzi w tryb autonomiczny i zakupów można dokonać, korzystając z dobrodziejstw nowej technologii.

Warto też wspomnieć, że Polska jest liderem, jeśli chodzi o liczbę sklepów autonomicznych w Europie (a przy obecnym tempie rozwoju za chwilę może i na świecie). Największa z sieci detalicznych w naszym kraju ma ich już ponad 50 i liczba ta stale rośnie. 📍



MICHAŁ MARCINIAK

Technical Project Manager w obszarze CCTV. Od 20 lat w branży IT i security – promotor, wdrożeniowiec i pasjonat nowych technologii z pogranicza monitoringu wizyjnego oraz IT.



Bezpieczeństwo firm rodzinnych

Odcinek 1. Handel detaliczny

W listopadowym numerze „Forbes” opublikowano listę 100 największych polskich firm prywatnych. Znamienne jest to, że nastąpiła zmiana lidera klasyfikacji. Na pierwszym miejscu znalazła się założona przez Tomasza Biernackiego firma Dino Polska, której wartość szacuje się na ponad 30 mld zł. W lipcu br. liczba marketów tej sieci przekroczyła 2000. Dla porównania, liczba placówek Lidl na całym świecie wynosi 10 800 (w tym 700 w Polsce). Należy więc z uznaniem odnotować, że pozycja Dino i dynamika jego rozwoju są imponujące, nie dając powodów do kompleksów.



Jacek Tyburek

C oraz częściej, przyglądając się finansowym aspektom gospodarki polskiej, nie sposób nie zauważyć znaczenia i wpływu ekonomicznego firm rodzinnych, zwłaszcza w sektorze małych i średnich przedsiębiorstw. Według raportu *Firma rodzinna to marka* opracowanego przez Instytut Biznesu Rodzinnego na podstawie badań w ramach projektu „Statystyka firm rodzinnych” 92% wszystkich działających na naszym rynku podmiotów prywatnych należy do osób prywatnych lub są to przedsiębiorstwa rodzinne z 36-procentowym ich udziałem. Większość firm rodzinnych w Polsce działa bez pełnej świadomości, że należą do tej kategorii. Taki stan znacząco wpływa na dalszy rozwój przedsiębiorstwa, niosąc duży potencjał wzrostu, ale także stwarzając ryzyko, które wcześniej nie było definiowane.

Firmy rodzinne mają swój status i są uznawane za specjalny typ podmiotów o unikalnych zaletach, mogących przesądzać o istotnej przewadze konkurencyjnej, np. nad firmami należącymi do Skarbu Państwa czy korporacjami zachodnimi. Wynika to ze struktury własności i powiązań pomiędzy właścicielami, a także (często) między właścicielami i pracownikami. Więzy rodzinne często są przenoszone również na pracowników spoza rodziny, dla których właściciel lub szef staje się niemal rodzicem. Umacnia je ponadto fakt, że ze względu na skalę firmy rodzinnej właściciel najczęściej:

- czynnie udziela się i pracuje w firmie, co sprawia, że zna osobiście większość bądź wszystkich swoich pracowników;
- kontroluje przepływ informacji wewnątrz firmy pomimo zatrudniania menedżerów różnego szczebla;
- jako założyciel firmy lub jej dziedzic ma emocjonalny stosunek do jej działalności pomimo pewnych ograniczeń biznesowych z tego powodu, co przyczynia się do traktowania swojego zespołu pracowniczego jak członków rodziny.

Pracownicy firm rodzinnych są często bardziej zmotywowani, sumienni, pilni i zaangażowani niż w firmach o innej strukturze własności. Nie musi to wynikać tylko z bliskości i kontroli właściciela – czasami wystarczy jego przykład i zaangażowanie, a czasami fakt, że przedsiębiorcy niechętnie inwestują swoje pieniądze w pracowników nieproduktywnych. Podważni, wiedząc o tym, starają się wykazać jak największe zaangażowanie. Właściciele firm rodzinnych są bardziej dostępni w porównaniu z właścicielami i kierownictwem innego typu przedsiębiorstw. Atrybutami firm rodzinnych często wymienianymi przez ich pracowników są:

- szacunek i przywiązanie do tradycji (gdy firma rodzinna ma historię);
- bezpieczeństwo utrzymania stałości zatrudnienia;
- stawianie na jakość (zwłaszcza gdy firma rodzinna działa na rynku regionalnym, gdzie wszyscy klienci znają właścicieli);
- długofalowe cele oraz duży margines samodzielności w myśleniu i działaniu.

Dobrze zarządzane firmy rodzinne mają kierownictwo zdolne do szybkiego podejmowania decyzji, w większym stopniu wykazując gotowość do realizowania śmiałych, ryzykownych przedsię-

wzięć, potrafią szybko się zmieniać i lepiej przystosować do nowych potrzeb rynkowych oraz charakteryzują się lepszą komunikacją wewnętrzną. Członkowie rodziny zazwyczaj posiadają głębokie poczucie własności firmy, przejawiają dużą motywację, są wyjątkowo lojalni i często pracują znacznie więcej niż nawet najbardziej sumienni pracownicy z zewnątrz.

Kolejnymi zaletami firm rodzinnych są elastyczność i szybkość podejmowania decyzji. Łatwiej dostosowują się do zmieniających się warunków rynkowych niż wielkie i z definicji często sparaliżowane decyzyjnie korporacje. W czasie kryzysu to właśnie takie firmy radzą sobie lepiej. Szybciej dostosowują swoją ofertę do potrzeb rynku, a jednocześnie cierpliwie czekają na zmianę sytuacji gospodarczej. Wartości, którymi się kierują, nie dotyczą tylko chęci zysku, lecz przede wszystkim odnoszą się do kontynuacji biznesu jako wartości samej w sobie i wynikających z tego faktu mierzalnych korzyści dla wszystkich członków zespołu.

W Polsce firmy zza zachodniej granicy kojarzą się przede wszystkim z korporacjami. Niewielu z nas zdaje sobie sprawę, że wiele codziennych marek, które lubimy i z których produktów korzystamy, należą do firm rodzinnych. Przykładem jest austriacka rodzina Porsche, kontrolująca dziś (poprzez swój pakiet kontrolny w Grupie Volkswagen) markę samochodów nie tylko Porsche, ale także Audi, Bentley, Bugatti, Lamborghini, SEAT, Škoda i Volkswagen. Największa w Stanach Zjednoczonych sieć sklepów Wal-Mart należy do rodziny Waltonów.

Prawie wszystkie funkcjonujące dziś na Zachodzie przedsiębiorstwa zaczęły jako firmy rodzinne, począwszy od banków (Rothschildowie), poprzez przemysł ciężki (Rockefellerowie), samochodowy (Fordowie), sanitarno-kosmetyczny (Johnson & Johnson) – długo by tę listę wymieniać. Dziś jest dla nas naturalne, że ich firmy odniosły sukces, bardzo często był to jednak wynik ciężkiej pracy wielu pokoleń. Polska, ze względu na uwarunkowania historyczne, firm rodzinnych z tak długimi tradycjami praktycznie nie ma. Założyciele tych, którym udało się odnieść sukces i wypromować własną markę, np. Grycan, PPL Koral (bracia Koral), Ziaja (małżeństwo Ziajów), Ochnik, Mokate (Kazimierz i Teresa Mokryszowie), prowadzą i promują swoje biznesy, korzystając z najlepszych zachodnich wzorców.

Siłą firm rodzinnych są wartości, na których opierają swoje decyzje i działania. Społeczna odpowiedzialność biznesu nie jest dla nich tylko pustym sloganem. To firmy rodzinne najczęściej wspierają lokalną społeczność, a także angażują się w działalność charytatywną. Nauczono doświadczeniem przekazy-



zywany z pokolenia na pokolenie zdają sobie sprawę, że zainwestowane w lokalną społeczność pieniądze przynoszą wymierne korzyści, najczęściej w perspektywie długofalowej (tzw. opóźniona gratyfikacja).

Firmy handlowe to swego rodzaju kwintesencja firm rodzinnych. Właśnie handel, drobne usługi i manufaktury mikro stanowiły początek rodzinnych biznesów. W Polsce firmy rodzinne funkcjonujące w handlu to bardzo znaczne grono – nie tylko lider rankingu Dino, ale także takie firmy, jak LPP z siecią sklepów, Euro-net, Neonet, Komputronik SA, żeby wymienić tylko te z listy 100 największych. Do tego dochodzą lokalne sieci handlowe, choćby zrzeszone pod marką Lewiatan. W ramach tej organizacji funkcjonują sieci rodzinne, które mają kilkadziesiąt sklepów wraz z własnymi centrami logistycznymi. Do tego dochodzą sieci hurtowni, sklepów specjalistycznych, np. sieci salonów meblowych (Black Red White, Nowy Styl z Krosna) i wiele innych.

Z tego wyliczenia wyłania się obraz poważnego komponentu biznesowego, który potrzebuje również sfery zarządzania bezpieczeństwem biznesu. Niektóre z wymienionych firm, głównie te największe, posiadają wewnętrzne struktury (działy) bezpieczeństwa zapewniające ochronę. Wszystkie z pewnością korzystają w mniejszym lub większym stopniu z technologii zabezpieczeń.

Z perspektywy branży security to niezwykle interesujący obszar, zwłaszcza w czasach tzw. VUCA, czyli w warunkach niestabilności i pełzającego kryzysu, którego skutki obecnie odczuwamy w skali zarówno globalnej, jak i lokalnej. Jednym z symptomów pogarszającej się sytuacji gospodarczej są nasilające się kradzieże w sklepach. Dochodzi do sytuacji, że niektórzy sprzedawcy byli zmuszeni do zabezpieczania towarów pierwszej potrzeby, np. masła, w urządzenia alarmujące przy bramkach sklepowych.

W różnych mediach społecznościowych pojawiają się doniesienia o kradzieżach klienckich, ale też o nieuczciwości pracowników. Ponadto należy zapewnić stabilność dostaw towaru, dokonać zmiany dostawców, a więc i konieczność zweryfikowania ich rzetelności. Nie można również zapominać o sferze cybersecurity i możliwości sparaliżowania pracy sieci handlowej w wyniku ataków grup hakerskich.

Firmy rodzinne z branży handlowej to również obszar zapewnienia bezpieczeństwa osobistego rodziny właścicieli. Jedną z najgłośniejszych tego typu spraw w świecie wielkich pieniędzy było porwanie w 1971 r. Theo Albrechta, współzałożyciela niemieckiej sieci supermarketów Aldi. Zaginiony w tajemniczych okolicznościach miliarder odnalazł się po 17 dniach. Został zwol-



niony przez porywaczy po przekazaniu gigantycznego okupu. Brat porwanego Karl Albrecht wpłacił 7 mln marek. Był to wówczas największy okup, jaki zapłacono w historii RFN. Theo Albrecht wysuwał pretensje do państwa niemieckiego o to, że policja nie była w stanie tak długo go odnaleźć, i zdecydował się na wyjście z oficjalnym roszczeniem do władz o rozliczenie tych 7 mln marek w formie ulg podatkowych dla swojego przedsiębiorstwa. Działania te były nieskuteczne. Wracając do potencjalnej oferty branży security dla dużego handlu prowadzonego przez firmy rodzinne, trzeba pamiętać o specyfice tych firm i ogromnym tempie ich rozwoju w ostatnich latach. Od momentu wejścia Polski do Unii Europejskiej, dostępności funduszy rozwojowych i systematycznego wzrostu zamożności społeczeństwa firmy znacznie zwiększyły swoje zasoby biznesowe. Nie zawsze jednak rozwijały swoje metodologie zapewniania bezpieczeństwa. Ustrukturyzowane polityki bezpieczeństwa i wynikające z nich zaplanowane działania są raczej wyjątkiem, nie mówiąc już o zestawie wypracowanych przez dziesięciolecia rozwiązań korporacyjnych, jak w przypadku konkurencji zagranicznej. Dlatego też wyraźnie widać potrzebę wsparcia rodzimego biznesu już od etapu koncepcyjnego, przez dostarczanie rozwiązań, po monitorowanie sytuacji związanej z bezpieczeństwem w biznesie. W przypadku firm handlowych raczej ma to formę procedur *loss prevention* na poziomie sklepów oraz klasycznego zarządzania bezpieczeństwem biznesu i odpornością na ryzyka z pozycji zarządów firm. Dotyczy również dystrybucji oraz wdrażania najnowocześniejszych, najbardziej efektywnych rozwiązań technologicznych i organizacyjnych.

Miałem przyjemność pomagać jednej z takich rodzinnych sieci handlowych. Firma działająca w północno-wschodniej Polsce posiada sieć ponad 60 sklepów i własne nowoczesne centrum logistyczne. Ponieważ w każdym ze sklepów był już system CCTV, naturalną potrzebą było zintegrowanie tych systemów w jednym miejscu, czyli w centrum logistycznym, gdzie znajduje się siedziba spółki rodzinnej.

Takich przykładów z pewnością jest w Polsce więcej, trzeba tylko dotrzeć z ofertą do właścicieli. Jest jeden aspekt, o którym należy pamiętać – firma rodzinna to zazwyczaj dorobek całego życia pokoleń. Bezpieczeństwo ekonomiczne zazwyczaj jest dla nich absolutnie podstawową potrzebą. Właściciele są do bólu pragmatyczni, szybko podejmują decyzje, ale nie są chętni do inwestowania w rozwiązania nowe, niesprawdzone. W wielu przypadkach nie powstaną wewnętrzne komórki bezpieczeństwa zasilane własnymi zasobami ludzkimi, technicznymi i organizacyjnymi. Tutaj jest pole do popisu dla eksperckich firm doradczych (*interim security managerów*), z ofertą maksymalnie elastyczną pod kątem czasu pracy i zadaniowości, oraz pomoc wynajętych zasobów monitorujących sytuację.

Firmy rodzinne, w tym z obszaru handlu, stanowią ogromną część gospodarki Polski. Wsparcie i wzmocnienie ich działalności poprzez zapewnienie im bezpieczeństwa jest nie tylko celem biznesowym. Powinno być również swego rodzaju misją dla polskich profesjonalistów branży bezpieczeństwa biznesu. 📍



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.

BLACK FRIDAY SALE!!!

Uniview 4MP EASYSTAR CCTV-KIT 4+1 MONITORING KIT

CONTACT YOUR DISTRIBUTOR FOR MORE DETAILS

You have following choices:

Easystar Camera Serie: IPC2124LE-ADF28KM-G、IPC324LE-DSF28K-G、IPC3614LE-ADF28K-G



Zhejiang Uniview Technologies Co., Ltd

www.uniview.com
Email: hongxingfang@uniview.com

Uniview Official Distributor



Analityka w handlu detalicznym

więcej cennych informacji niż można się spodziewać

W minionych latach można było zauważyć znaczący spadek ruchu w sklepach stacjonarnych. Wpływ na to miało kilka czynników, zwłaszcza globalna pandemia i zwiększająca się popularność sklepów internetowych. W 2020 r. w Polsce, według raportu ExpertSender, przybyło aż 11,8 tys. nowych sklepów internetowych. Równocześnie w ostatnich miesiącach w handlu detalicznym zauważalne są znaczne wzrosty – w grudniu 2021 r. według raportu GUS zauważono ośmioprocentowy wzrost sprzedaży w porównaniu z grudniem 2020 r. Powoli zaczynamy wracać do sklepów stacjonarnych – przed przedsiębiorcami stoi jednak nie lada wyzwanie związane z powrotem do wyników sprzedażowych sprzed pandemii. Do tego celu niezbędne będą szczegółowe dane analityczne, które mogą zostać pozyskane... wprost ze sklepu. Inteligentne systemy monitoringu wizyjnego, oparte na analityce i rozwiązaniach end-to-end mogą nie tylko dostarczyć aktualnych informacji wpływających na sprzedaż, ale także przyczynić się do znacznej poprawy doświadczeń klientów podczas robienia zakupów.

LICZENIE OSÓB I MONITOROWANIE KOLEJEK

Dzięki analityce właściciel jest w stanie wprowadzić do swojego sklepu wiele udogodnień, nie tylko tych skierowanych do klientów, ale także znacznie ułatwiających pracę personelu. Rozwiązania analityczne połączone z monitoringiem wizyjnym można wykorzystać do zliczania osób w czasie rzeczywistym. Uzyskane dane będą przydatne do podejmowania kluczowych decyzji biznesowych, np. o poziomie zatrudnienia w godzinach szczytu. Natomiast monitorowanie kolejek może znacznie zwiększyć poziom zadowolenia klientów dokonujących zakupy w sklepie. Dzięki wykorzystaniu tej funkcji pracownicy zostaną powiadomieni o liczbie oczekujących osób. Dodatkowo informacje o średnim czasie oczekiwania i wskaźnikach rezygnacji pozwalają na szybkie wprowadzenie zmian.

IDENTYFIKACJA DEMOGRAFICZNA I MAPY CIEPŁA

W celu gromadzenia statystyk przydatna będzie funkcja identyfikacji demograficznej polegająca na zbieraniu informacji na temat wieku i płci odwiedzających sklep. Pomoże to właścicielowi zdefiniować grupy docelowe klientów, a także dostosować komunikaty marketingowe kierowane do odwiedzających. Ponadto informacje statystyczne pozyskiwane z map ciepła, identyfikujących gorące punkty i martwe obszary umożliwiają wizualizację wzorców ruchu w czasie.

Przez długi czas systemy dozoru wizyjnego były gwarantem bezpieczeństwa w sklepie. To się nie zmieniło – jednakże spektrum zastosowań tego typu rozwiązań jest znacznie większe. Systemy te mogą się stać również przydatnym narzędziem biznesowym zwiększającym wydajność i wyniki finansowe firmy. Przydatne będą kompleksowe rozwiązania oparte na monitoringu wizyjnym i analityce.



– Zastosowanie analityki w monitoringu wizyjnym dostarcza przedsiębiorcom garść cennych statystyk, pomocnych w przygotowaniu strategii działania firmy, a także ustalania celów przekładających się na poprawę zysków i doświadczeń klientów. Przykładowo dzięki mapom ciepła można zoptymalizować układ całego sklepu, czyniąc go miejscem bardziej przejrzystym dla klientów – mówi Dagmara Pomirska z Axis Communications.

NOWY TYP KLIENTA

Badania potwierdzają, że współczesny klient wymaga specjalnego podejścia. Każda minuta spędzona przez niego w centrum handlowym jest bardzo cenna. Kiedy odwiedza dany sklep czy punkt usługowy chce szybko i sprawnie zaspokoić potrzeby konsumpcyjne, a także spędzić czas w przyjemnej atmosferze. Oczekuje również spersonalizowanej oferty. Projektowanie spójnego i spersonalizowanego doświadczenia wymaga zrozumienia potrzeb klienta. Najnowsze systemy telewizji dozorowej są w stanie dostarczyć odpowiedzi na szereg pytań, które mogą znacznie ułatwić pracę menedżerom i zarządcom obiektów handlowo-usługowych, np. jakie są nawyki zakupowe klienta, gdzie lubi spędzać czas i jak długo przebywa w centrum handlowym.

– Dzięki kamerom sieciowym z funkcją analiz opartych na technologii sztucznej inteligencji detaliści i menedżerowie zyskują dostęp do niezwykle cennych danych dotyczących zachowań zakupowych klientów i mogą precyzyjnie dostosowywać swoją ofertę do preferencji poszczególnych grup demograficznych – podkreśla Dagmara Pomirska.

SZEROKIE MOŻLIWOŚCI AUDIO I ANALITYKA IOT

Kamery sieciowe, oprócz dbania o bezpieczeństwo, mają wpływ na kształtowanie doświadczeń klientów, wykorzystując inteligentne rozwiązania audio i IoT. Systemy audio mogą nie tylko wspierać personel sprzedaży, wysyłając alerty głosowe, np. o aktualnym obłożeniu sklepu i obszarach wymagających większego wsparcia, ale także zadbać o nastrój klientów. Muzyka w tle i głosowe komunikaty o okazjach, budują atmosferę pomagającą w podejmowaniu decyzji zakupowych. Analityka IoT natomiast stwarza całe spektrum inteligentnych możliwości wykorzystywanych do precyzyjnej identyfikacji osób przychodzących do sklepu czy zapewniania optymalnych warunków do zakupów, np. odpowiedniego oświetlenia danej części sklepu czy ustawienia temperatury.

KOMPLEKSOWE ROZWIĄZANIA END-TO-END

Rozwiązania analityczne najlepiej działają w kompleksowych, zintegrowanych systemach łączących ze sobą kamery oraz inne sieciowe urządzenia zabezpieczające i analityczne. Ważne jest także dobranie właściwego oprogramowania do zarządzania materiałem wizyjnym, które nie tylko integruje się ze wszystkimi elementami systemu, takimi jak kamery, systemy audio, aplikacje analityczne i czujniki, ale także jest nieskomplikowane w obsłudze. Pomaga to w gromadzeniu wszystkich niezbędnych informacji w jednym miejscu i prostym zarządzaniu nimi.

– Systemy dozoru muszą być skrojone na miarę, co znaczy, że powinny z łatwością odpowiadać na specyficzne potrzeby danej branży – poczynawszy od wyboru kamer po oprogramowanie zarządzające całym ekosystemem. Istotne jest także to, aby wybrane rozwiązanie nie sprawiało problemów w obsłudze, a interfejs był przejrzysty i dostosowany do potrzeb klienta. Tak kompleksowe rozwiązanie może być pomocne także w innych obszarach, często niezauważalnych. Przykładowo dzięki odpowiedniemu oprogramowaniu możliwy jest szybki dostęp do dokumentacji montażowej, co pozwala uniknąć błędów podczas montażu – komentuje Dagmara Pomirska.

MŚP

Istotne jest również, aby systemy bezpieczeństwa były skalowane i odpowiadały potrzebom różnorodnych obiektów od małych sklepików po wielkopowierzchniowe centra handlowe. Duże centra handlowe mają wysokie standardy ochrony, ale też dysponują licznymi zespołami pracowników, którzy czuwają nad bezpieczeństwem klientów. Natomiast na właścicieli małych i średnich firm spoczywa wielka odpowiedzialność. Zapewnienie ciągłości działania biznesu, kontrola stanu faktycznego i ryzyko zajścia niechcianego incydentu to jedno z wielu elementów zarządzania przedsiębiorstwem. Małe i średnie firmy są kluczowym sektorem dla polskiej gospodarki. Według raportu PARP jest to aż 99,8% wszystkich przedsiębiorstw w Polsce. Ponad 70% z nich to przedstawiciele branży usługowej i handlowej. Istotne więc jest dbanie o bezpieczeństwo tych biznesów. Wysokiej jakości system telewizji dozorowej pozwala na dokładny przegląd zarejestrowanego wcześniej materiału wizyjnego w celu sprawdzenia, jaki incydent zdarzył się na terenie firmy. Przykładowo, jeżeli zauważymy nagłe braki w sklepie, przejrzenie nagrania może dostarczyć odpowiedzi, czy doszło do kradzieży i kto jej dokonał. Takie rozwiązanie jest cenne także z punktu oceny odpowiedzialności i rozwiązywania sporów. Aby móc się cieszyć urlopem w pełni i zachować spokój ducha, właściciel firmy może zdalnie, z poziomu swojego smartfona, skorzystać z podglądu na żywo lub przejrzeć nagrania z kamer, by mieć pewność, że wszystko znajduje się na swoim miejscu. Nawet jeśli miałyby miejsce jakiegokolwiek incydent, możliwe jest skonfigurowanie określonych alertów.

W przypadku małych sieci biznesowych, gdzie jedna firma ma kilka lokalizacji, przydatnym rozwiązaniem może być możliwość przyznawania uprawnień dostępu do kamer wielu użytkownikom. Dzięki temu zwiększenie poziomu ochrony, bezpieczeństwa i wydajności może być znacznie łatwiejsze. 📍

AXIS COMMUNICATIONS POLAND

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



HikCentral

dla sieci handlowych

Armen Moska



Zarządzanie siecią handlową jest w dzisiejszych czasach zadaniem niełatwym. Współpracując od lat z największymi sklepami w Polsce, często bywam zaskoczony mnogością wyzwań, jakim trzeba stawić czoła – zmieniającym się trendom, warunkom gospodarczym, a ostatnio pandemii, wojnie i załamaniom globalnych łańcuchów dostaw. To doprawdy syzyfowa praca, tym bardziej że stopień trudności kolejnych wyzwań ma zdecydowaną tendencję do wzrostu w tempie geometrycznym.

Niełatwym zadaniem jest zapobieganie stratom i kradzieżom przy jednoczesnym dbaniu o fantastyczne wrażenia zakupowe klientów czy sprawianiu, by załódze pracowało się przyjemniej i efektywniej. W związku z tym, że wyzwania naszych klientów stają się poniekąd również naszymi, w Hikvision staramy się precyzyjnie definiować problemy i jednocześnie szukać dla nich jak najefektywniejszych rozwiązań. Prześledźmy więc kluczowe wyzwania technologiczne dla handlu detalicznego i zastanówmy się, jak można na nie odpowiedzieć.

Z punktu widzenia menedżerów zarządzających kluczowe jest odpowiednie zabezpieczenie obiektów sklepowych i logistycznych oraz zapobieganie stratom. Z pewnością też zauważają, że systemy zabezpieczeń ewoluują w szybkim tempie i trzeba śledzić na bieżąco najnowsze rozwiązania wykorzystujące zdobycze nowych technologii. W zakresie detekcji intruza nic nie zastąpi starych poczwirych czujek PIR i kontaktowników, aczkolwiek dzisiaj warto zoptymalizować ten obszar dzia-

łania i rozważyć zastosowanie zaawansowanych systemów detekcji wideo bazujących na algorytmach VCA, które zoptymalizują i zautomatyzują proces ochrony. Obsługę i zabezpieczenie linii kas wesprze weryfikacja transakcji kasowych wspomagana analityką wideo w postaci nakładki na systemy POS. W ten sposób sprawdzimy zgodność transakcji z rzeczywistym przepływem produktów oraz przeanalizujemy konkretne elementy pod kątem produktowym i specyficznych operacji, takich jak storna.

W procesach dotyczących bezpieczeństwa decydująca jest szybka i właściwie przekierowana informacja o zdarzeniu. Najlepsze systemy niewiele pomogą, jeśli nie będzie docierała na czas do odpowiednich osób/komórek. Stąd niezwykle istotną rolę spełnia scentralizowana platforma do zarządzania sygnałami alarmowymi, która na bazie predefiniowanych scenariuszy bezpośrednio prześle informacje i odpowiednio zareaguje na niepożądane zdarzenia. Równie ważne w tym zakresie jest zabezpieczenie magazynów i centrów logistycznych. W tego typu obiektach do niewątpliwie kluczowych należą zagrożenia związane z intruzami i wybuchem pożaru. Można im zapobiec w sposób kompleksowy, stosując kamery termowizyjne, które na bazie zaawansowanych algorytmów wykryją zarówno podejrzanie wyższą temperaturę, jak i potencjalnych intruzów.

Z punktu widzenia sieci handlowych istotne znaczenie ma możliwość centralnego zarządzania systemami zabezpieczeń i monitorowania. Tu z pomocą przyjdą inteligentne ściany wideo, na których można śledzić to, co dzieje się w poszczególnych obiektach, a także zarządzać konkretnymi alertami.

Kolejnym wyzwaniem dla zarządców sklepów, tym istotniejszym, że dotyczy kluczowego obszaru działania, czyli sprzedaży, jest analiza zachowania klientów. W tym zakresie warto wspomnieć o trzech funkcjach, które mogą dostarczyć informacji interesujących z biznesowego punktu widzenia. Pierwszą jest liczenie klientów. To funkcja przydatna dla wybranych grup sklepów, w których liczba odwiedzających nie zawsze przekłada się na zrealizowane zakupy, jednak dla tych właśnie sieci dane o przepływie potencjalnych klientów wydają się być kluczową informacją. Tu z pomocą przyjdą kamery uzbrojone w algorytmy Deep Learning, które dostarczają wiarygodnych i rzetelnych danych o potencjale sprzedażowym placówki.

Gdy już wiemy, ilu potencjalnych klientów odwiedza sklep, warto również zdefiniować strefy, po których się poruszają, i stworzyć dokładne mapy pomocne w zidentyfikowaniu preferencji odwiedzających w zakresie najchętniej wybieranych tras. To wartościowa informacja przy planowaniu rozmieszczania poszczególnych produktów na półkach. Najlepszym rozwiązaniem w tym zakresie są kamery typu *fish-eye*, które nie tylko rejestrują obraz panoramiczny w wysokiej rozdzielczości, ale także rozpoznając warunki cieplne w poszczególnych obszarach sklepu, tworzą zaawansowane heatmapy. Kolejnym aspektem są doświadczenia zakupowe klientów, które w dużej mierze bazują na komforcie realizacji procesu zakupowego. W tym przypadku czas oczekiwania w kolejce to jeden z głównych czynników *customer experience*. Z kolejkami przed kasami można sobie poradzić, wykorzystując do tego celu specjalistyczne kamery monitorujące w czasie rzeczywistym klientów, a w przypadku przekroczenia zdefiniowanej liczby osób w kolejce wygenerują alert z odpowiednią informacją.

Mamy więc zabezpieczone placówki i zebrane najistotniejsze informacje o klientach w naszych sklepach wraz z dokładną analizą ich zachowania. W jaki jednak sposób „spieniężyć” te dane, jak przekuć je na konkretne efekty sprzedażowe? Najprostszym rozwiązaniem wydaje się zastosowanie systemów Digital Signage. To uniwersalne rozwiązanie sprawdzi się zarówno w klasycznych supermarketach, w sklepach typu *convenience*, jak i na stacjach paliw czy w restauracjach.

Nie od dziś wiadomo, że właściwie dobrany контент potrafi czynić sprzedażowe cuda. Odpowiednio rozmieszczone ekrany z atrakcyjnie wyeksponowaną ofertą mogą znacząco zwiększyć wartość koszyka zakupowego.

Podsumowując, kluczowymi aspektami zastosowań technologii w najważniejszych obszarach zarządczych dla sieci handlowych są:

- inteligentne systemy zabezpieczeń i zapobiegania stratom,
- aktywny i stargetowany marketing,
- procesy sprzedażowe i zwiększanie koszyka zakupowego.

Należałoby jeszcze dodać optymalizację procesów, zarządzanie danymi oraz usieciowienie i łatwość zarządzania infrastrukturą IT.

Wszystkie powyższe czynniki wydają się krytyczne z punktu widzenia zarządzania biznesem, żadnego z nich pominąć nie można. Dzisiaj, przy tak dużej liczbie wyzwań i mnogości kluczowych obszarów zarządczych, nie da się prowadzić skutecznej polityki sprzedażowej bez odpowiednich, zaawansowanych narzędzi, które nie tylko dostarczą danych, ale także będą potrafiły nimi zarządzać, archiwizować je w jednym miejscu, weryfikować i aktywować określone scenariusze.

Tego typu narzędzi jest dziś dużo na rynku, większość pod wieloczołonowymi, anglojęzycznymi nazwami i trudnymi do rozszyfrowania skrótami. Niewiele jest jednak narzędzi prostych, w sposób kompleksowy odpowiadających na potrzeby handlu detalicznego w całościowej formie, a przy tym integrujących w jednym miejscu wiele różnych obszarów.

Jednym z takich rozwiązań jest platforma HikCentral wraz z całą gamą urządzeń wspierających różne obszary zarządzania procesowego w handlu. W Hikvision staramy się wychodzić naprzeciw potrzebom naszych klientów, a zastosowanie HikCentral znacząco ułatwia projektowanie kompleksowych rozwiązań dostosowanych do specyfiki działania sieci handlowych. Dzięki naszej platformie całość procesów sklepowych jest nadzorowana z poziomu centralnego rozwiązania sterującego działaniem wszystkich urządzeń podłączonych do systemu.

Czy wyobrażamy dziś sobie choć jeden dzień bez smartfona? HikCentral to taki właśnie smartfon, tyle że dla sieci handlowych. 📱

HIKVISION POLAND

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





Głos branży →

PRZEDSTAWICIELE RÓŻNYCH
DZIAŁÓW GOSPODARKI
OPISUJĄ WYZWANIA, JAKIE
STOJĄ PRZED MENEDŻERAMI
SECURITY I LOSS PREVENTION.



Robert Kujawa

Retail Security Academy

Kompromis pomiędzy nakładami a korzyściami

Cokolwiek powiemy o działaniach podejmowanych w celu zminimalizowania kradzieży w placówkach handlowych, dane Komendy Głównej Policji wskazują, że są one niewystarczające. Od czasów pandemii obserwujemy ciągły wzrost kradzieży sklepowych. Obecnie najbardziej popularną inwestycją w poprawę bezpieczeństwa w sklepach jest zakup systemów monitoringu, które pełnią funkcję odstraszającą potencjalnych złodziei oraz pozwalają udokumentować zdarzenia na potrzeby postępowań dowodowych prowadzonych przez policję lub ubezpieczycieli. Częściej niż przed pandemią są wykorzystywane systemy przeciwwkradzieżowe do ochrony większej grupy produktów, np. zabezpieczanie etykietami antykradzieżowymi produktów spożywczych pierwszej potrzeby, ostatnio nawet masła. W USA i w krajach Europy Zachodniej można dostrzec trend do utrudniania klientom dostępu do najczęściej kradzionych produktów (tzw. CRAVED), zamykające

w gablotach lub udostępniając tylko w wyznaczonych miejscach, np. przy kasie lub w punkcie obsługi klienta. W tych krajach duży nacisk kładzie się też na szkolenia personelu w celu zwiększenia efektu synergii pomiędzy potencjałem pracowników a możliwościami technicznymi systemów zabezpieczeń.

Czy rosnąca inflacja nie zahamuje inwestycji w systemy zabezpieczeń w obiektach handlowych? Część organizacji, poszukując oszczędności, będzie oczywiście ograniczać te inwestycje do momentu przekroczenia akceptowalnego przez zarząd progu strat. Mając jednak na uwadze rosnące drastycznie koszty pracy, inwestycja w technikę ochronną jest najlepszym kompromisem pomiędzy nakładami a korzyściami.

Na pewno można oczekiwać wzrostu na rynku urządzeń z algorytmami sztucznej inteligencji, co w perspektywie przełoży się na ograniczenie udziału i kosztów osobowych w zapewnieniu bezpieczeństwa. W czasie kryzysu zawsze jednak istnieje chęć oszczędzania, co skutkuje wyborem rozwiązań najtańszych, nie zawsze dobrej jakości. A te często nie spełniają postawionych przed nimi wymagań, np. nagrania ze zdarzeń są tak słabej jakości, że uniemożliwiają identyfikację sprawców.

Nie można także zapominać o wydawalności się prostej, ale kluczowej kwestii, jaką jest budowanie świadomości pracowników z zakresu bezpieczeństwa i umiejętności obsługi coraz bardziej zaawansowanej technologii, gdyż – jak potwierdzają badania w nurcie teorii Davisa dotyczącej TAM (*Technology Acceptance Model*) – tylko technologie uznane przez użytkowników (w tym przypadku personelu sklepu) za przydatne i łatwe w użyciu są efektywnie wykorzystywane. Oszczędności na szkoleniach pracowników mogą wzmocnić ich opór przed stosowaniem nowych technologii zabezpieczeń lub skutkować nieumiejętnym wykorzystaniem systemów, co będzie sprzyjać narracji „o braku korzyści” i w konsekwencji może być zachętą do krótkowzrocznych decyzji zarządów o zaniechaniu inwestycji w bezpieczeństwo w czasach wysokiej inflacji.



Maciej Ptaszyński

Polska Izba Handlu

Wyzwania przed branżą handlową

Bez wątpienia w najbliższym czasie możemy spodziewać się rosnącej liczby przypadków kradzieży, którą bezpośrednio stymuluje galopująca inflacja. Już dziś wystarczy zapoznać się z danymi policji i porównać je choćby z sytuacją sprzed roku. Przedstawiciele branży handlu detalicznego stoją przed coraz większym



wyzwaniem związanym z odpowiednim zabezpieczeniem swoich towarów na półkach sklepowych, a jednocześnie muszą się mierzyć z kolejnymi wzrostami niemal wszystkich kosztów prowadzenia działalności handlowej, począwszy od czynszów, przez wynagrodzenia dla personelu, skończywszy na rosnących z dnia na dzień cenach hurtowych czy opłatach związanych z transportem i logistyką.

W czasach niewątpliwie bardzo trudnych dla branży handlowej państwo powinno raczej starać się podać jej pomocną dłoń, gdy tymczasem najwyraźniej zamierza postawić sprzedawców w obliczu kolejnego wyzwania. Mowa o planowanym przez rząd podniesieniu progu przestępstwa kradzieży z 500 do 800 zł.

Jako Polska Izba Handlu jednogłośnie sprzeciwiamy się temu projektowi, wiedząc, jak dotkliwie dla całego sektora handlowego byłoby jego wejście w życie. Już dziś na skutek kradzieży każdy mały sklep traci rocznie asortyment o wartości kilkudziesięciu tysięcy złotych, natomiast zdecydowana większość incydentów tego typu kończy się niewspółmierną karą w postaci mandatu dla nieuczciwych klientów. Podniesienie progu o, nie ukrywamy, niemałą kwotę 300 zł może być w dobie rosnącej inflacji niejako zachętą do kradzieży i przytłaczania jednorazowo produktów o większej wartości, zwiększając jeszcze straty sklepu, stąd też nasze stanowisko bezwzględnie wetujące tę poprawkę kodeksu karnego.



Krzysztof Poznański

Polska Rada Centrów Handlowych

Bezpieczeństwo w centrach handlowych

Centra handlowe funkcjonują w Polsce już od ponad 30 lat. Przez ten czas zostały wypracowane efektywne procedury i systemy, które stale ewoluują wraz ze zmieniającą się rzeczywistością, wymogami i pojawiającymi się nowymi potrzebami. W codziennym funkcjonowaniu zarządcy współpracują ze sprawdzonymi, wyspecjalizowanymi firmami ochrony. Używają technologii, która pomaga minimalizować ryzyko kradzieży.

Powszechne jest korzystanie z systemów monitoringu wizyjnego, który ma m.in. jak najlepiej udokumentować ewentualną próbę kradzieży. Wykorzystuje się także systemy zabezpieczeń i weryfikacji. Jednakże oprócz ww. aspektów kluczową rolę odgrywają przeszkoleni pracownicy zarówno ochrony, jak i osoby zatrudnia-

ne przez najemców. Ważnym aspektem jest także wymiana wiedzy o bieżących zagrożeniach pomiędzy zarządcami a wynajmującymi oraz policją. Rekordowa inflacja i mniej stabilna sytuacja gospodarcza mają duży wpływ na decyzje podejmowane przez przedsiębiorców, w tym inwestycje. W kontekście systemów zabezpieczeń efektywną pomocą dla firm, która umożliwia optymalizację, jest wciąż rozwijająca się technologia. Rozumiejąc, jak ważne są zagrożenia bezpieczeństwa w centrach handlowych, Polska Rada Centrów Handlowych opracowuje specjalny raport. Będzie zawierał wyniki badań przeprowadzonych przez PRCH wspólnie z Grupą Impel, partnerem projektu. W raporcie znajdą się analizy szeregu zagadnień, od bezpieczeństwa epidemiologicznego, przez ochronę fizyczną, możliwości optymalizacji usług ochrony, ich monitorowanie i raportowanie, nadzór i delegowanie zadań pracowników ochrony, poważne sytuacje kryzysowe, aż po innowacje i rekomendacje wyboru firmy ochrony.

Jest to tym istotniejsze, ponieważ w tym roku Sejm rozpoczął prace nad zmianami w kodeksie karnym i kodeksie ds. wykroczeń, które mają doprowadzić do podniesienia kwoty wyznaczającej granicę uznania kradzieży za przestępstwo do 800 zł. To poważny problem dla handlu. Zwłaszcza że z danych publikowanych przez Komendę Główną Policji wynika, iż liczba kradzieży w sklepach z roku na rok wzrasta. W takiej sytuacji zarządcy, mimo rosnących kosztów, będą dalej inwestować w ochronę i sprzęt także ze względów bezpieczeństwa.



Agnieszka Sawicka

Checkpoint Systems

Systemy EAS zapobiegają kradzieżom

Stale rosnąca inflacja, bijąca z miesiąca na miesiąc kolejne rekordy, nie pozostaje bez wpływu na policyjne statystyki liczby kradzieży w polskich placówkach handlowych. Sprzedawcy detaliczni na całym świecie podejmują różne metody walki z nieuczciwymi konsumentami.

Najczęściej stosowanymi metodami są: zabezpieczenie produktów przez umieszczenie ich w specjalnych gablotkach (np. maszyny do golenia czy alkohole), zdejmowanie produktów z ekspozycji i umieszczenie ich pod ścisłą kontrolą sprzedawców i kasjerów. Zatrudniani są też kolejni

ochroniarze czy też instaluje się elektroniczne systemy przeciwwkradzieżowe EAS (*Electronic Article Surveillance*). Analiza prognoz rynku urządzeń EAS pokazuje, że w najbliższej przyszłości będzie to jedna z najczęściej wybieranych form walki z kradzieżami sklepowymi. W przeciwieństwie do innych rozwiązań – często generujących kolejne koszty, powodujących zmniejszenie liczby eksponowanych towarów, a przez to także ich sprzedaż, czy wymuszających zamknięcie sklepów w „twierdze” – urządzenia EAS pozwalają na kompleksową kontrolę nad każdym produktem przy jednoczesnym udostępnieniu go klientom oraz zachowaniu estetyki i spójności z aranżacją i wystrojem sklepu.

Spodziewane kolejne wzrosty inflacji nie powinny zahamować inwestycji w systemy zabezpieczeń antykradzieżowych głównie z jednego podstawowego powodu. Chodzi o szybkość zwrotu w tę inwestycję, a więc o tzw. ROI. Ich skuteczność w ograniczaniu strat w handlu oznacza, że instalacja narzędzi EAS zwraca się już w ciągu kilku miesięcy. Rośnie też zadowolenie klientów z dostępności produktów na półkach i ich lojalność do marki.



Urszula Zielińska-Jończyk

CCC

Prewencja w zapobieganiu stratom

Placówki handlowe w obliczu obecnej sytuacji ekonomicznej w kraju i geopolitycznej na świecie znalazły się w bardzo trudnym położeniu. W prasie co chwilę pojawiają się artykuły *Uwaga, plaga! Polacy z biedy zaczęli kraść na potęgę!*

Coraz częściej sprawcy przestępstw i wykroczeń to do niedawna zwykli klienci, którzy tłumaczą się brakiem pieniędzy na podstawowe życiowe potrzeby. Jak wynika z danych KG Policji, w I połowie br. liczba przestępstw kradzieży w sklepach wzrosła aż o 28% w porównaniu z analogicznym okresem ub. roku, natomiast liczba wykroczeń związanych z kradzieżą sklepową – o ok. 13% w relacji rocznej. W praktyce w ostatnich miesiącach liczba różnych zdarzeń *crime* w placówkach handlowych zwiększyła się o ok. 100%. Nie brakuje opinii, które podzielam, że problem kradzieży będzie narastał i szybko się nie skończy. Jednocześnie w tym szczególnym czasie szefowie działów w większości przypadków szukają oszczędności, co skutkuje znacznymi cięciami w budżetach. Czy jednak warto oszczędzić



dzać na systemach antykradzieżowych? Na tym z całą pewnością nie. Departamenty Loss Prevention i bezpieczeństwa aktywnie poszukują rozwiązań mających na celu minimalizację strat, jednak potrzebują do tego odpowiednich narzędzi. Obecne czasy w sposób szczególny obrazują, jak istotną rolę odgrywają one w biznesie.

Najbardziej popularne i funkcjonalne, a jednocześnie niezbędne w placówkach handlowych są systemy telewizji dozorowej (CCTV), kontroli dostępu (SKD), sygnalizacji włamania i napadu (SSWiN) czy bramki antykradzieżowe EAS.

Najskuteczniejszym sposobem na uniknięcie niepożądanych strat jest prewencja, a dzięki wykorzystaniu odpowiednich technologii to zadanie staje się znacznie łatwiejsze. Optymalnym działaniem jest jednocześnie zastosowanie szeregu rozwiązań ograniczających ryzyko kradzieży. Najprostszym, a przy tym skutecznym wariantem jest rozszerzanie strategii zabezpieczania towarów oraz inwestycja w systemy CCTV.

Jedno jest pewne – obecna sytuacja stawia przed Działami Loss Prevention i bezpieczeństwa wiele wyzwań wymagających elastyczności i ciągłej analizy sytuacji.

**Ewelina Zalewska**

Super-Pharm Holding

Wyzwanie dla pracowników Loss Prevention

W ostatnich kilku miesiącach w polskich placówkach handlowych odnotowano znaczący wzrost liczby kradzieży towarów o różnej wartości. W porównaniu z poprzednimi latami zmiana, z którą teraz mamy do czynienia, polega na tym, że częściej kradzione są produkty spożywcze (np. masło) oraz produkty pierwszej potrzeby (takie jak szampony, pasty do zębów, a nawet leki).

Nie oznacza to, że zmalała liczba kradzieży produktów z dotychczasowego topu kradzieżowego (perfumy, dermokosmetyki, produkty makijażowe czy nożyki do gołenias) – te również giną i także w większych ilościach niż dotychczas. Statystyki policyjne mówią o 30% wzrostach kradzieży.

Głównymi ich powodami są czynniki ekonomiczne (wzrost inflacji i ogólne zubożenie społeczeństwa). Coraz częściej sprawcami kradzieży są grupy zorganizowane. Dla nas, pracowników Loss Prevention, to obecnie największe wyzwanie, z którym zmagamy się każdego dnia. By stawić czoło znacząco zwiększonemu ryzyku kradzieży

wykorzystujemy nowoczesne i innowacyjne rozwiązania technologiczne, a także techniki operacyjne, które skutecznie wspierają nas w tej nierównej walce. Rozbudowa centralnego monitoringu wizyjnego i rozszerzone działania detektywów sklepowych pozwalają nam efektywnie przeciwdziałać kradzieżom. Dzięki rozbudowanemu procesom niezwłocznie dowiadujemy się o zagrożeniach, co pozwala nam działać błyskawicznie, często wzbudzając niemałe zdziwienie u sprawców kradzieży, którym wydaje się, że nie widząc ochroniarza, pozostaną bezkarni. Olbrzymie znaczenie ma tu również wsparcie ze strony policji.

Szacujemy, że zbliżający się okres świąteczny, ale także początek nowego roku może owocować w dalsze wzrosty kradzieży sklepowej. Jesteśmy na to przygotowani. Polegamy na stałej i doświadczonej kadrze pracowników ochrony, których umiejętności stale podnosimy za pomocą szkoleń specjalistycznych, i bardzo dbamy o to, by móc niezwłocznie reagować na pojawiające się ryzyka.

**Jarosław Sapko**

Axis Communications

Monitoring w obiektach handlowych

Pojęcie „obiekty handlowe” jest pojemne – obejmuje różnorodne miejsca, od lokalnych małych sklepików po wielkopowierzchniowe centra handlowe. Ich potrzeby w zakresie bezpieczeństwa też różnią się ogromnie i wymagają bogatego portfolio urządzeń, które umożliwi indywidualne dopasowanie do specyfiki zabezpieczanego obiektu.

Dlatego też kamery monitoringu wizyjnego coraz częściej przyjmują bardziej różnorodne formy, np. dyskretnych koputek lub modeli modułowych, których obiektywy mogą być chowane w różnych miejscach, np. w futrynach drzwi wejściowych czy obudowach bankomatów. W obiektach wielkopowierzchniowych coraz częściej spotyka się kamery wieloprzetwornikowe, ponieważ jedno takie urządzenie zapewnia dozór w zakresie nawet 360 stopni. Ich połączenie z kamerami PTZ pozwala na dokładną obserwację dużych przestrzeni. W przypadku wystąpienia incydentu wymagającego reakcji operator może skierować kamerę PTZ na wybrany punkt i dzięki przybliżeniu obrazu skupić się na szczegółach tego, co dzieje się w danym miejscu.

Systemy monitoringu wizyjnego w obiektach handlowych coraz częściej pełnią nie tylko funkcje związane z dozorowaniem towaru i prewencją przed kradzieżami, ale także stają się narzędziami do analizy zachowania klientów czy wspierania decyzji biznesowych. Co więcej, zastosowanie różnych algorytmów analizujących obraz z kamery pozwala też wykryć zastawione drzwi ewakuacyjne, zawiadomić obsługę o kolejce oczekujących przy kasie czy przesłać jej informacje o osobie zbyt długo przebywającej w danej części sklepu.

Kamery stają się też pewnego rodzaju „bramkami”, które pozwalają połączyć obraz z informacjami z innych czujników połączonych w sieci. Dzięki zastosowaniu otwartych protokołów mogą stawać się agregatorami danych z takich urządzeń, jak czujniki temperatury, kontaktrony czy czujki PIR. Funkcja kamer nie sprowadza się jedynie do zbierania tych danych i przesyłania ich dalej, umożliwia także ich wyświetlanie na obrazie w postaci nakładki na zarejestrowanym materiale w stylu rozszerzonej rzeczywistości AR.

**Armen Moska**

Hikvision

Optymalizacja staje się priorytetem

Dla sieci handlowych nastały nie najlepsze czasy. Trudności, z jakimi przyszło im się obecnie borykać, z jednej strony mogą porażać, z drugiej – nie sposób nie podziwiać elastyczności i skuteczności działań podmiotów z branży retail, które w imponujący sposób potrafią radzić sobie z bieżącymi wyzwaniami.

Bez trudu można zauważyć, że hasłem odmienianym obecnie przez wszystkie przypadki jest „optymalizacja”. Trudno się dziwić, margines braku optymalizacji w dzisiejszym świecie właściwie przestał istnieć. Każde nieoptymalizowane działanie czy proces niesie wymierne negatywne skutki dla całości działań firmy. Z mojego punktu widzenia najbardziej interesujący w tym jest widoczny wzrost zainteresowania narzędziami, które te procesy optymalizacyjne będą w stanie wspierać, co wcale nie jest zadaniem prostym.

Rodzime sieci handlowe świetnie radzą sobie w obszarze online/e-commerce. W ostatnich latach zauważyłem dość raziący paradoks polegający na tym, że o ile

w strategiach sprzedaży wielokanałowej, tak dynamicznie rozwijanej ostatnimi czasy, kanał offline generował dla większości sieci największe przychody, o tyle – w zakresie centralnego zarządzania i analityki danych – był tak naprawdę dość ubogą przystawką do prężnie rozwijających się aplikacji i platform online'owych.

Tymczasem dziś wyraźnie widać, że odpowiednie zagospodarowanie i zoptymalizowanie procesów zachodzących w fizycznych sklepach staje się priorytetem, co ma bezpośredni związek z drastycznym wzrostem kosztów funkcjonowania klasycznych placówek. Stąd większe zainteresowanie rozwiązaniami z zakresu AI IoT, które pozwalają na maksymalne wykorzystanie danych zbieranych przez różne sieciowe urządzenia w sklepie i automatyczną optymalizację zdefiniowanych procesów. W tym właśnie tkwi dzisiaj największy potencjał dla ograniczania kosztów i zwiększania sprzedaży.

**Marcin Walczuk**

BCS

Technologie zabezpieczeń w branży handlowej

Zabezpieczenie obiektów handlowych – od małych sklepów po centra handlowe – już dawno przestało bazować na prostym systemie alarmowym czy systemie telewizji dozorowej złożonym z kilku lub kilkunastu kamer. Niejednokrotnie, a w przypadku dużych obiektów praktycznie zawsze są to zarządzane centralnie zaawansowane systemy zabezpieczeń, w których skład wchodzi wspomniane systemy SSWiN i CCTV, ale też ppoż. i kontroli dostępu.

Priorytetem powinno być zapewnienie bezpieczeństwa osobom przebywającym na terenie obiektu handlowego. Tutaj podstawą powinno być przestrzeganie i stosowanie się do przepisów budowlanych, norm ppoż. czy instrukcji BHP. Zastosowanie nowych rozwiązań technologicznych z zakresu monitoringu wizyjnego może zdecydowanie podnieść poziom bezpieczeństwa, ułatwić obsługę i odciążać operatora, wykonując za niego coraz więcej zadań.

Wykorzystanie różnych funkcji zaawansowanej analizy wideo pozwala znacząco ograniczyć liczbę fałszywych alarmów i reagować na sytuacje, które faktycznie



stanowią zagrożenie. Sprawdza się np. funkcja detekcji pozostawionych obiektów, która pomoże szybko namierzyć przedmiot i podjąć odpowiednie działania. Dzięki skróceniu czasu reakcji zwiększamy też szansę na odnalezienie osoby odpowiedzialnej za całe zdarzenie. Z kolei funkcja monitorowania zachowania tłumu czy poszczególnych osób pozwoli wychwycić z otoczenia osoby zachowujące się w sposób podejrzany bądź zareagować, zanim dojdzie do paniki.

Nowoczesny system CCTV może służyć już nie tylko do zabezpieczenia obiektu. Zaczyna stanowić coraz potężniejsze narzędzie analityczne, które w handlu detalicznym może podnieść skuteczność sprzedaży. Dane spływające z kamer w postaci map cieplnych, które obrazują, gdzie był największy ruch, pozwolą lepiej pozycjonować produkty, na których sprzedaży zależy najbardziej. Raporty z kamer zliczających ludzi dają informacje, ile osób odwiedziło sklep. Można je powiązać np. z liczbą wystawionych paragonów w danym okresie. Metadane pozyskane z kamer, identyfikujące twarze czy z inteligentnych rejestratorów, określające płeć, przedział wiekowy lub nastrój pozwolą lepiej ukierunkować działania marketingowe skierowane do docelowej grupy odbiorców.

Pokazuje to jasno, że rozwój technologii zabezpieczeń jest ściśle związany z sektorem handlowym. Z jednej strony zapewniają bezpieczeństwo, co cały czas powinno być celem nadrzędnym każdego systemu dozorowego, z drugiej – dzięki analizie pozyskanych danych pozwalają zwiększyć przychody. Dlatego tak ważna jest bliska współpraca producentów urządzeń zabezpieczeń technicznych obiektu z jego odbiorcami, czyli w tym wypadku z różnego rodzaju obiektami handlowymi.

**Daniel Kamiński**

Smart-i

Zastosowanie analizy obrazu w handlu

W ostatnim czasie zaobserwowaliśmy zwiększone zainteresowanie analizą obrazu w sieciach handlowych. Klienci poszukują narzędzi, które pomogą im usprawnić powtarzalne procesy, w szczególności pozwalające utrzymać wysoką sprzedaż oraz ograniczyć straty.

W tych rozwiązaniach kamery pełnią funkcję sensorów, które przekazują informacje do systemów biznesowych, takich jak programy magazynowe, transportowe czy finansowe. Jednym z pożądanych zastosowań jest tzw. monitorowanie półki. Właściciele sieci handlowych zauważyli, że wielkość sprzedaży jest niższa w sklepach, w których półki są puste. Klienci po prostu je omijają, dlatego obsługa sklepu powinna na bieżąco reagować i uzupełniać towar. Niestety ograniczenia liczby personelu powodują, że czynność ta jest zaniedbywana.

Rozwiązaniem problemu mogą być kamery z analizą obrazu, które montuje się w pobliżu regatów. System analizy obrazu rozpoznaje produkty stojące na półce i przekazuje na zaplecze dokładną informację o brakach, gdy klienci kupią określone produkty. Personel nie musi sprawdzać półek, system automatycznie zleca ich uzupełnienie, wskazuje miejsce i ilość. Pełna półka zwiększa obroty.

Inną potrzebą jest wykrywanie nietypowych zachowań klientów, w szczególności kradzieży. Analitka behawioralna jest jeszcze w początkowym okresie rozwoju, ale pojawiają się pierwsze firmy, które udostępniają algorytmy do testów. Obecny wzrost kradzieży sklepowych i kosztów osobowych przyczyni się do szybkiego rozwoju tego typu rozwiązań. Tradycyjne metody nie są skuteczne i wsparcie przez oprogramowanie analizujące obraz jest bardzo oczekiwane.

Analizą kradzieży interesują się zwykłe działy bezpieczeństwa, a analizą zajętości półek – działy logistyki. Przy tradycyjnym podejściu trudno pogodzić potrzeby obu działów. Jeśli jednak traktuje się kamery jako sensory, można przekazywać metadane do obróbki przez różne systemy wspomagające. Należy pamiętać, aby wybrane kamery i platformy VMS wspierały integrację z systemami biznesowymi. 📍

Zarządzanie projektem

Cz. 2. Poszczególne etapy

Kontynuując tematykę wstępu do zarządzania projektem, poruszoną na łamach poprzedniego numeru, tym razem przyjrzymy się zagadnieniom ściśle związanym z prowadzeniem samego projektu opartego na rozwiązaniach elektronicznego systemu zabezpieczeń. Kluczową rolę odgrywają tu poszczególne etapy bezpośrednio związane z pracami projektowymi, co pozwoli usystematyzować pracę i znaleźć wspólny mianownik dla wszystkich uczestników przedsięwzięcia.



Tomasz Dacka

Wybrana przeze mnie metodologia nie jest złotym środkiem, posłuży jako przykład tego, na co należy zwrócić szczególną uwagę podczas koordynacji prac.

FAZOWANIE PROJEKTU

Zadanie długoterminowe warto podzielić na pewne etapy. Pozwala to na lepsze przygotowanie się do każdego z nich, bardziej szczegółowe zaplanowanie prac (w przeciwieństwie do podejścia „wszystko naraz”). Są to:

- Etap 1. Studium wykonalności
- Etap 2. Rozwinięcie projektu
- Etap 3. Wykonanie
- Etap 4. Zamknięcie

Każdy z nich będzie wymagał intensyfikacji pracy rozłożonej na inne aktywności, zaangażowania innych zespołów. Co istotne, przez cały czas trwania wszystkich etapów należy pamiętać o głównym celu zadania. Zbyt duże skupienie się na dygresyjnych czynnościach może rozmywać całościątł prowadzonych prac.

PRZYGOTOWANIE

Zanim przejdziemy przez poszczególne etapy, należy wykonać kilka czynności, które powinny poprzedzić typowe prace projektowe:

1. AKTYWNOŚCI

Mając określony główny cel podzielony na zadania, trzeba przeanalizować aktywności, które pozwolą na ich osiągnięcie. Istotne są tu zależności pomiędzy nimi i nakład sił potrzebny do ich realizacji. Niepożądana jest sytuacja, w której zespół jest zaskoczony koniecznością zaangażowania np. prac deweloperskich w oprogramowaniu zarządzającym materiałem wideo. To nie tylko dodatkowy czas potrzebny na realizację, ale przede wszystkim koszty z tym związane.

2. DIAGRAM PRACY

Rozpisanie wszystkich aktywności jest potrzebne, ale nie daje pełnego obrazu zadania. Można to przedstawić na przykładzie klocków Lego. Wiemy, jakie części są nam potrzebne, nie wiemy jednak, w jakiej kolejności ich użyć. W tym celu buduje się tzw. diagram pracy, który:

- determinuje aktywności potrzebne do finalizacji zadań,
- wskazuje, które czynności wymagają większego wysiłku (czas, koszty, zagadnienia merytoryczne, np. integracja poszczególnych podsystemów),

- układa zadania w porządku chronologicznym, tworząc coś na wzór kalendarza prac (niektóre zadania muszą czekać na rozpoczęcie aż do zakończenia innych, np. nie ma potrzeby wieszać kamer przed położeniem do nich okablowania lub pisać program integracji z systemem SSWiN przed jego gruntowną aktualizacją),
- pozwala na przyspieszenie prac (np. niektóre aktywności mogą być realizowane równolegle, niezależnie od siebie).

3. NA WSZELKI WYPADEK

Każdy projekt, bez względu na jego zakres, jest obciążony ryzykiem wystąpienia zdarzeń losowych lub niepewnością związaną z realizacją poszczególnych zadań. Niepożądanym efektem ich wystąpienia są implikacje związane, tutaj nie będzie zaskoczenia, z czasem i kosztem. Na pewne rzeczy wpływu nie mamy, niektóre ryzyka możemy jednak zaplanować. Aktywności obciążone takim ryzykiem powinny zostać skalkulowane w następujący sposób:

Czas trwania, wystąpienia niepożądaney aktywności x prawdopodobieństwo wystąpienia = skalkulowane opóźnienie

Planując np. zakup kamer pod koniec roku, możemy założyć, że czas ich dostawy wydłuży się o 4 tygodnie z 50-proc. prawdopodobieństwem. Wówczas dopuszczalne opóźnienie w pracach projektowych określamy jako 2 tygodnie. Jako że czas to pieniądz, możemy adekwatnie wyliczyć niepewność związaną bezpośrednio z poniesionymi kosztami. Jeśli np. materializacja ryzyka podniesienia cen zakupu czytników kontroli dostępu wyniesie 10 000 zł z prawdopodobieństwem 30%, należy zwiększyć budżet zadania o 3000 zł.

4. DOBRE PRAKTYKI

Skracając do minimum tematykę, dobrym zwyczajem będzie przestrzeganie następujących porad:

- Wszystkie ustalenia powinny być prowadzone w formie pisemnej (papierowej lub elektronicznej). To, czego nie udokumentowano, może być traktowane jako niebyłe.
- W pracach projektowych można wspierać się odpowiednim oprogramowaniem do zarządzania projektem (np. Jira).
- Warto postawić granicę, do kiedy można w sposób szybki nanosić zmiany w projekcie, np. do etapu 2. zmiany może nanosić zespół projektowy, od etapu 3. będzie wymagana zgoda wszystkich zaangażowanych w projekt. Należy też wprowadzić wzór dokumentacji wprowadzanych zmian.
- Dla szybkiego oszacowania kosztów można posłużyć się złotymi zasadami, np. instalacja systemu pochłonie 40–50% budżetu.
- Warto przygotować się przed czasem na najczęściej pojawiające się problemy w trakcie realizacji projektu (np. utrata zasobów zaangażowanych w projekt z powodu niezainteresowania projektem kadry zarządzającej, wprowadzanie zbyt dużej ilości małych zmian przekładających się na dużą zmianę zakresu projektu, ramy czasowe i kosztowe zaczynają wykradać się z pierwotnych założeń czy występujące zmęczenie materiałem zespołu projektowego).

ETAP 1. PLANOWANIE

W momencie dzielenia całości na części często padają pytania, która część jest najważniejsza. W zarządzaniu projektem można stwierdzić, że to właśnie planowanie jest najistotniejszym etapem. Wystarczy przypomnieć stare, sprawdzone powiedzenie „Jak sobie pościelisz, tak się wyśpisz”. Niekompletnie przeprowadzony etap planowania jest najczęstszym powodem niepowodzeń realizacji całego projektu.

Głównym celem omawianego etapu jest zapewnienie, że wprowadzone środki zabezpieczenia poprzedzone analizą ryzyka będą stanowiły dla organizacji wartość dodaną, swego rodzaju benefit w zabezpieczeniu aktywów, usprawnieniu procesów czy przygotowaniu się do wsparcia zapewnienia



ciągłości działania. To właśnie podczas planowania powinny zostać określone:

- cele projektu,
- sposób, w jaki wdrożenie projektu pozwala mitygować wcześniej zidentyfikowane ryzyka,
- opisy funkcjonalne wdrażanych rozwiązań bez wchodzenia w detale techniczne,
- celowość projektu,
- wstępny budżet projektu,
- ramy czasowe.

Na tym etapie należy zbudować zespół projektowy, na którego czele powinien stać PM (Project Manager). Istotnymi aspektami są identyfikacja wszystkich interesariuszy i zaangażowanie ich przedstawicieli do pracy zespołu. Wdrażając system kontroli dostępu powiązany np. z rejestracją czasu pracy, nie można zapomnieć o działach odpowiedzialnych chociażby za cyberbezpieczeństwo, HR, zakupy czy ogólnie pojętej administracji budynków, w których mamy zamiar taki system wdrożyć. Kolejnym istotnym elementem jest analiza ryzyka. To temat na tyle obszerny, że wymaga oddzielnego opracowania, na potrzeby artykułu przypominę jedynie podstawowe elementy, z jakich poprawnie wykonana analiza powinna się składać:

1. Wskazanie i identyfikacja aktywów ze wskazaniem ich wartości dla organizacji.
2. Wskazanie zagrożeń, biorąc pod uwagę kontekst zarówno zewnętrzny, jak i wewnętrzny organizacji.
3. Określenie prawdopodobieństwa wystąpienia danego zagrożenia.
4. Określenie podatności danych aktywów na materializację zagrożenia.
5. Identyfikacja ryzyka zgodnie z przyjętą metodologią (np. jakościową).



6. Wprowadzenie zarządzania ryzykiem poprzez odpowiednią pracę z ryzykiem określonym w poprzednim kroku jako nieakceptowalne (np. transfer ryzyka za pomocą odpowiedniego ubezpieczenia na wypadek materializacji ryzyka).

Wynikiem etapu planowania powinna być dokumentacja zawierająca takie elementy, jak wyniki przeprowadzonej analizy ryzyka, wskazanie procedury zakupowej, estymacja budżetowa zakupu danego rozwiązania, wybór kierownika projektu, wskazanie zespołu projektowego, wskazanie, kto i w jaki sposób ma wykonać projekt techniczny (np. czy będziemy to robić wewnątrz organizacji lub za pomocą biura projektowego, czy wykorzystując postępowania oparte na zasadach „zaprojektuj i wybuduj”). Na koniec należy wskazać wszystkie wymagania związane z kontraktowaniem w danej organizacji i literą prawa, jaka nas w danym obszarze obowiązuje.

ETAP 2. ROZWINIĘCIE PROJEKTU

Należy się skupić nad dokumentacją projektową w ujęciu jej specyfikacji kryteriów wyboru. Dokumentacja powinna być ujęta w określone z góry ramy, aby była maksymalnie kompletna. Wszelkie aspekty pominięte na tym etapie mogą stanowić spore wyzwanie na etapie wdrożeniowym. Kluczowa jest współpraca z zespołem projektowym. Zlecenie dokumentacji i bierne oczekiwanie na jej finał zazwyczaj nie kończą się sukcesem. Branżowi projektanci, nawet w pełni profesjonalnie zaangażowani w dane zagadnienie, nie będą znali specyfiki naszej organizacji. Koordynacja w tym momencie odgrywa główną rolę, przepływ informacji w obie strony będzie miarą naszego sukcesu.

Specyfikacja powinna uwzględniać trzy główne obszary: operacyjne, siłę ludzką oraz architekturę. Projektowanie systemów elektronicznej ochrony bez uwzględnienia personelu i procedur nie będzie efektywne.

Coraz częściej pojawiającymi się elementami są kryteria projektowania, na których podstawie projektuje się dane rozwiązanie. Oto najbardziej popularne:

- Wydajność systemu – np. jak szybko system kontroli dostępu jest w stanie wykonać identyfikację, autentykację i autoryzację oraz obsłużyć aktywator danego przejścia kontrolowanego (np. kolowrót). Możemy zagwarantować sobie odpowiednią przepustowość, potrzebną w godzinach szczytu pracy, np. biurowca.
- Pojemność systemu – rozumiana nie tylko jako liczba obsługiwanych użytkowników, ale również gwarancja odpowiedniego miejsca w celu późniejszych modernizacji czy rozbudowy (możliwości techniczne i aplikacyjne, np. licencji).
- Unikatowość – jeśli nie jest to konieczne, warto unikać pewnych rozwiązań, które mogą być realizowane jedynie przez jednego dostawcę na rynku. Wiąże się to z wyzwaniami podczas modernizacji architektury. Jeśli to możliwe, warto opierać się na otwartych standardach komunikacji, np. protokoły OSDP*.
- Regulacje prawne, wytyczne organizacji, dobre praktyki.
- Budżet.
- Utrzymanie – określenie, w jaki sposób i jak często należy łożyć środki, aby dane rozwiązanie utrzymywać na akceptowalnym poziomie funkcjonalnym. Jest to związane bezpośrednio z kosztami i czasem, jakie użytkownik końcowy musi zaadresować. Dobrym pomysłem jest określenie współczynnika TCO (tzw. całkowity koszt posiadania) dla danego rozwiązania.

Wynikiem tego etapu powinien być dokument zawierający:

- Instrukcje dla oferentów, z wymaganiami organizacji koniecznymi do realizacji danego przedsięwzięcia.
- Specyfikacje techniczne wraz z odpowiednimi rysunkami oraz listą koniecznych do implementacji urządzeń (w zależności od wyboru procedury zakupowej).
- Określenie budżetu w sposób dużo dokładniejszy niż na etapie planowania, z uwzględnieniem parametru TCO.

* <https://www.securityindustry.org/industry-standards/open-supervised-device-protocol/>

ETAP 3. WYKONANIE

Ten etap składa się z trzech głównych zadań. Są to:

1. Przeprowadzenie procedury zakupowej.
2. Instalacja, szkolenia.
3. Odbiory, warunki gwarancji.

Procedura zakupowa w większości przypadków powinna zostać przeprowadzona przez odpowiednie osoby, działy, co zapewni maksymalną zgodność przetargu z wymaganiami wewnętrznymi organizacji. Nie zmienia to jednak faktu, że najważniejszą częścią jest tzw. wsad merytoryczny, za który to my, jako osoby związane z zabezpieczeniami, będziemy odpowiedzialni. Nie sposób omówić tutaj przebiegu procedury, ponieważ co organizacja, to inny pomysł. Niemniej jednak warto zachować pewne standardy, tj. przeprowadzenie konferencji dla oferentów, na której omawia się główne cele i założenia projektu, bada zainteresowanie i zrozumienie drugiej strony, pozyskuje cenne informacje nt. możliwości technicznych, operacyjnych oferentów. Jeśli sytuacja tego wymaga, spotkanie można zorganizować w strefach bezpieczeństwa objętych przedmiotem zapytania. Każda taka konferencja czy spotkanie powinno kończyć się możliwością zadawania pytań, ich dokumentowaniem oraz listą obecności.

Kolejnym ważnym krokiem jest określenie kryteriów ocen danych ofert, tj. doświadczenie w podobnych instalacjach, posiadane uprawnienia firmy oraz osób oddelegowanych do implementacji zadania, cena, aspekty właścicielskie, zabezpieczenia jakościowe dostarczanych rozwiązań, określenie łańcucha dostaw itp.

Kwestia instalacji i szkoleń to kolejny temat. Na tym etapie powinny być monitorowane w sposób szczególny: zgodność wykonania z dokumentacją wykonawczą (wszelkie odstępstwa powinny być dokumentowane, z podaniem ich przyczyn oraz uzyskaniem zgody wszystkich zainteresowanych stron), pełen nadzór nad wykonawcami i podwykonawcami (np. uprawnienia do prowadzenia prac czy dostępu do informacji niejawnych), przygotowanie planu odbiorów, przygotowanie wymagań co do dokumentacji powykonawczej, komunikowanie wszystkich wymagań poprzedzających prace instalacyjne oraz po-instalacyjne, wytyczne co do instalacji okablowania, urządzeń (normy, wytyczne, dobre praktyki), zastosowanie wytycznych wydajnościowych a nie ilościowych (np. kamery są tam, gdzie miały być, ale niestety generują dużą liczbę fałszywych alarmów ze względu na źle dobrany osprzęt punktu kamerowego), przeprowadzenie testów operacyjnych.

Ze względu na specyfikę rozwiązań plan szkoleń powinien być przedstawiany wykonawcom na wcześniejszych etapach. Zdarzają się sytuacje, że trudno inwestorowi zebrać naraz cały zespół albo obszary odpowiedzialności są rozmyte na kilka podzespołów. Wykonawca w takim wypadku jest w stanie wcześniej odpowiednio skalkulować taką usługę, a następnie przeprowadzić ją zgodnie z wymaganiami inwestora.

Przekazanie do użytkownika powinno odbywać się zgodnie z góry określonym planem odbiorów, który powinien w sposób jasny opisywać zakres oceny i wskazywać osoby niezbędne do jego przeprowadzenia. Po każdym spotkaniu należy sporządzić notatkę opisującą, co zostało zrobione, a co należy poprawić. Zalecam, aby odbiory również były przeprowadzane na zasadzie sprawdzania/testowania danej funkcjonalności, a nie tylko sprawdzenia ilościowego urządzeń podsystemów bezpieczeństwa. Jest to szczególnie istotne w zakresie implementacji zintegrowanych systemów bezpieczeństwa. Podobnie jak w temacie szkoleń, odpowiednio wcześniej komunikowany plan odbiorów pomoże wykonawcom lepiej się do nich przygotować. Na koniec należy jasno opisać warunki gwarancji urządzeń, działania systemów czy świadczenia usług klasy SLA.



ETAP 4. ZAMKNIĘCIE

Nazwa tego etapu może wprowadzać w błąd, sugerując zorganizowanie spotkania zamykającego. Jest to co prawda jeden z elementów tego etapu, jednak bardziej istotnymi obszarami są tu:

- Określenie zasad utrzymania (z podziałem na utrzymanie zapobiegawcze i zaradcze).
- Opisanie planu utrzymania (ze wskazaniem, kto i za co jest odpowiedzialny, w tym za prowadzenie dokumentacji, np. książki serwisowej).
- Wskazanie zasad szacowania wartości danego rozwiązania w danym okresie czasowym i wymagań co do wymiany, modernizacji.

Należy tu zwrócić uwagę na różnice pomiędzy utrzymaniem prewencyjnym (zapobiegawczym) a zaradczym. Systematyczne utrzymywanie systemów zgodnie z wymaganiami ich producentów, wykonawców pozwoli na maksymalne obniżenie kosztów związanych z koniecznością prowadzenia działań zaradczych (czyli tych, które musimy podjąć po wystąpieniu awarii, uszkodzenia). W rozległych systemach liczba urządzeń końcowych (np. czujniki, kamery, czytniki kart) jest niekiedy bardzo duża. Utrzymanie całej infrastruktury stanowi zatem pewne wyzwanie.

Warto zatem przeanalizować, co jest potrzebne, dokonywać wizualnej inspekcji czujników ruchu czy co jakiś czas przeglądać zdarzenia w centralach alarmowych. Czy centrala, która przez pół roku nie generuje żadnych informacji, nie powinna budzić podejrzenia? Jak często przeglądamy archiwalny materiał wideo pod kątem zarówno czasu jego przechowywania, jak i jakości obrazu? Jak duża liczba użytkowników systemu kontroli dostępu jest nieaktywna przez dłuższy czas?

Prowadzenie projektów elektronicznych systemów zabezpieczeń nie należy do najłatwiejszych. Mamy bowiem w tym przypadku częsty kontakt z wieloma interesariuszami, bazami danych, przetwarzaniem danych osobowych. Samo bezpieczeństwo również ewoluuje. Prowadzenie projektu na zasadzie „żeby było bezpieczniej” nie robi już na nikim wrażenia. Oczekuje się od nas czegoś więcej, benefitów, namacalnych korzyści w obszarze teoretycznie stricte kosztowym. Na szczęście z pomocą przychodzą nowe technologie, możliwości usprawniania procedur i generowania oszczędności. To ciekawe, aczkolwiek trudne projekty, dające jednak dużą satysfakcję. 🕒



TOMASZ DACKA

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

Rozwiązania security w obiektach muzealnych



Hubert Żak

Obiekty muzealne to nie tylko miejsca kultury budujące tożsamość historyczną i narodową, lecz także często bezcenne źródło wiedzy kształtujące edukację. To również miejsca, w których znajdują się eksponaty o ogromnej wartości materialnej. Majątek obiektów muzealnych w Polsce szacuje się na kilka, a często kilkaset milionów złotych, dlatego w kontekście wartości zarówno historycznej, jak i materialnej wymagają wyjątkowych zabezpieczeń.

Temat dotyczący rozwiązań security w obiektach muzealnych jest bardzo szeroki i zarazem specyficzny, jeśli chodzi o zakres ochrony i mnogość dostępnych rozwiązań. Podstawą zabezpieczenia takich obiektów są ustawy i rozporządzenia, które w dużym zakresie regulują projektowanie i instalowanie różnego rodzaju zabezpieczeń. Do najważniejszych należą: rozporządzenie Ministra Kultury i Dziedzictwa Narodowego z 2 września 2014 r. (Dz.U. nr 2014, poz. 1240), ustawa o muzeach z 21 listopada 1996 r. (Dz.U. 1997 r. nr 5, poz. 24; Dz.U. z 2012 r. poz. 987, z późn. zm.), rozporządzenie Ministra Kultury z 15 października 2003 r. (Dz.U. 2003 nr 193 poz. 1892) oraz wiele innych. Zakres ochrony obiektów muzealnych można podzielić na cztery kluczowe obszary:

- ochrona fizyczna, służby ochrony – formacje ustawowo uprawnione do ochrony obiektów muzealnych,
- personel pracowniczy, osoby z obsługi, transportu itp.
- procedury, instrukcje, zarządzenia regulujące zasady funkcjonowania obiektów i ich bezpieczeństwa,
- zabezpieczenia techniczne (elektroniczne i mechaniczne), sprzęt i inne dedykowane urządzenia.

Wskazane ustawy i przepisy określają jedynie podstawę funkcjonalności w obszarze stosowania rozwiązań technicznych oraz sprzętowych w ochro-

nie muzeów. Pozostałe zagadnienia są kwestią indywidualnego, prawidłowego doboru rozwiązań i urządzeń dopasowanych do charakterystyki obiektu oraz zagrożeń.

Podstawą doboru techniki – systemów i urządzeń – jest przeprowadzenie audytu bezpieczeństwa w obszarze zarówno technicznym, jak i proceduralnym (taktycznym). Rozwiązania techniczne stosowane w ochronie obiektów muzealnych dotyczą kilku kategorii, np.:

1. ochrona antykradzieżowa,
2. ochrona eksponatów bezpośrednio lub pośrednio narażonych na uszkodzenia i zniszczenia,
3. ochrona podstawowa lub systemowa obejmująca m.in. SSP, DSO, KD,
4. inne.

Odnosząc się do punktu pierwszego, nie będziemy dzielić rozwiązań na te wymagane ustawowo i dodatkowe. Ochrona antykradzieżowa to przede wszystkim właściwe zabezpieczenie muzealiów w miejscach ich przechowywania, czyli w ramach ekspozycji oraz magazynowania. W zakresie ochrony antykradzieżowej znaczenie ma dobór właściwego, rozbudowanego systemu alarmowego umożliwiającego zbieranie różnych danych, np. dotyczących ruchu, temperatury, zmiany oświetlenia, dźwięku itd. System alarmowy musi być zaprojektowany i skonfigurowany antysabotażowo oraz wyposażony w inne funkcjonalności, np. bezpośrednie i pośrednie powiadamianie wielu osób. Eksponaty, szczególnie wysokiej wartości, powinny być indywidualnie chronione takimi rozwiązaniami technicznymi, jak nadajniki GPS, beacons, nadajniki radiowe, które szybko wskażą miejsce przemiesz-

czenia obiektu.

Urządzenia muszą być również odporne na czasową lub całkowitą dezaktywację lub zakłócenie ich pracy. Najskuteczniejsze jest zastosowanie wielu urządzeń i różnych technologii, aby w przypadku awarii jednego inne przejęły jego zadania i zapewniły nieprzerwaną ochronę. Zatem zabezpieczenie jest tym skuteczniejsze, im więcej rozwiązań technicznych zastosowano. Każdorazowo należy tak je dobrać, aby wzajemnie wspomogły proces, a nie hamowały go.

W odniesieniu do punktu 2. dotyczącego ochrony ekspozycji zauważam, że coraz więcej rozwiązań oferowanych przez producentów jest dopasowanych do potrzeb placówek muzealnych i, co ważne, doskonale sobie one radzą. Systemy monitoringu wizyjnego i szeroko pojęta analityka zastosowana umiejętnie, we właściwy sposób, nie tylko podniosą poziom bezpieczeństwa, ale także wpłyną na zoptymalizowanie kosztów. Zastosowanie takiego rozwiązania w kilkunastu obiektach w Polsce znacząco wpłynęło na poziom ochrony ekspozycji i pozwoliło na redukcję mniej efektywnych rozwiązań fizycznych.

Kluczowym zagadnieniem staje się projekt systemu dozoru wizyjnego i właściwy dobór odpowiednich kamer. Co to oznacza? Większość obiektów, oprócz wystaw i ekspozycji stałych (gdzie kamery CCTV są zainstalowane na stałe), organizuje wystawy czasowe. Oznacza to, że zmienia się ustawienie ścian i wygrodzeń, aby powstał właściwy ciąg wystawowy zgodnie z przepisami ppoż. dotyczącymi np. jego szerokości, oznakowania itd. Ten obszar również należy właściwie zabezpieczyć. W tym miejscu pojawia się aspekt monitoringu „mobilnego”, przy czym mobilność oznacza właściwy model budowy sieci strukturalnej, aby bez względu na ustawienie ścian mobilnych, wygrodzeń i eksponatów można było swobodnie podłączyć urządzenia monitorujące. Przekłada się to na odpowiednio zaprojektowaną liczbę gniazd i przenośnych punktów montażowych. Obecnie doskonale funkcjonuje kilka takich obiektów.

W wielu muzeach i galeriach zadania ochrony są wykonywane przez personel stacjonarny. Na podstawie własnych doświadczeń mogę stwierdzić, iż rozwiązania sprzętowe, zwłaszcza kamery wyposażone w odpowiednio dobraną i skonfigurowaną analitykę, wykonują je lepiej. Mają znacznie większe pole obserwacji i analitykę, która szczególnie się sprawdza przy dużych grupach zwiedzających. Oczywiście eksponaty muszą być zabezpieczone nie tylko systemem monitoringu wizyjnego, ale także systemem alarmowym i technologią RFID, GPS oraz rozwiązaniami mechanicznymi, takimi jak gabloty, szyby, wygrodzenia, zabezpieczenia w postaci linek itp. Istotne jest, aby każdorazowo dobrać rozwiązania przystosowane do kon-

kretnych potrzeb.

Podstawowa ochrona obiektu (punkt 3) to oczywiście wyposażenie wynikające z przepisów prawa budowlanego, ochrony obiektów użyteczności publicznej itd. Oprócz funkcjonalności podstawowych systemów dozorowych, SSP czy DSO należy zwrócić uwagę na możliwość wykorzystania np. dodatkowych czujek, specjalnych systemów gaszenia itp. Trzeba pamiętać, aby system był zdywersyfikowany w najbardziej narażonych obszarach, dobrze i szybko się komunikował, miał możliwość współpracy i implementacji do systemów BMS i SMS.

Oddzielnym rozwiązaniem pozostaje system kontroli dostępu w muzeach. Możliwość zarządzania ruchem, sterowanie nim oraz właściwe zdefiniowanie praw dostępu w znacznym stopniu chroni zarówno muzealia, jak i całą przestrzeń podlegającą ochronie.

W punkcie 4 pod pojęciem „inne rozwiązania” kryją się przede wszystkim procedury oraz profesjonalne i systematyczne szkolenia. Przy mnogości dostępnych na rynku rozwiązań szkolenia na nieodpowiednim poziomie merytorycznym, stosowanie przestarzałych procedur, a nawet ich brak, stają się największym zagrożeniem dla tego typu obiektów. Niestety audyty bezpieczeństwa przeprowadzone przez Najwyższą Izbę Kontroli i Ministerstwo Kultury i Dziedzictwa Narodowego wykazały wiele zaniedbań wynikających z braku zarówno odpowiednich funduszy, jak i wiedzy oraz właściwego zarządzania.

Z mojej praktyki na proces zabezpieczenia obiektu muzealnego i eksponatów składają się:

- audyt proceduralny/techniczny,
- projekt,
- optymalizacja,
- realizacja,
- wdrożenia,
- stały schemat przeglądów oraz szkolenia i systematyczne ćwiczenia.

Taki model security pozwala właściwie chronić dzieła sztuki, często unikatowe, o bezcennej wartości.

Podsumowując, muzea to obiekty o wyjątkowej charakterystyce i pomimo rozwiązań ustawowych pozostają ogromnym obszarem do zagospodarowania zarówno przez producentów techniki, projektantów, jak i menedżerów security. 🕒

HUBERT ŻAK



Ekspert ds. bezpieczeństwa i techniki zabezpieczeń, menedżer projektów. Wieloletni pracownik służb, od kilkunastu lat związany z bezpieczeństwem biznesu, szczególnie z zarządzaniem kryzysowym, prewencją, zapobieganiem zagrożeniom i bezpieczeństwem publicznym. Współpracuje z korporacjami międzynarodowymi i instytucjami rządowymi, gdzie odpowiada za nowe rozwiązania w systemach bezpieczeństwa oraz specjalistyczne szkolenia.

Czy „Dama z gronostajem” jest w niebezpieczeństwie?

Branża ochrony w trudnej sytuacji

Branża ochrony osób i mienia, która zatrudnia w Polsce ok. 250 tys. osób (dwa i pół razy więcej niż policja), stoi obecnie przed wielkimi wyzwaniami finansowymi i kadrowymi. Sektor, którego sprawne funkcjonowanie wpływa na stabilność codziennego życia Polaków, jest zmuszony do podnoszenia stawek za swoje usługi.



Dla wielu firm ochrony wypracowanie kompromisu z klientami w zakresie wynagrodzenia to warunek „być albo nie być”. Urzędy, instytucje kultury, kompleksy sportowe, centra handlowe – to tylko kilka przykładowych obiektów, które nie mogą działać bez ochrony. Jak wiele firm nie przetrwa kryzysu i czy trudna sytuacja w sektorze ochrony przełoży się na zapewnienie bezpieczeństwa w Polsce?

OCHRONA JEST NIEZBĘDNA

Działania pracowników ochrony są widoczne szczególnie podczas imprez masowych. Wydarzenia takie jak koncerty czy zawody sportowe nie mogą się odbywać bez zapewnienia bezpieczeństwa ich uczestnikom. To, jak niezbędna jest ochrona podczas imprez na wielką skalę, pokazała choćby sytuacja podczas nawałnicy na tegorocznym Open'er Festival. Gdyby nie dobrze wyszkolone zespoły pracowników ochrony, ewakuacja kilkudziesięciotysięcznej publiczności z terenu festiwalu w ekstremalnie trudnych warunkach pogodowych mogłaby skończyć się katastrofą.

Pracownicy ochrony są niezbędni również w instytucjach publicznych. 14 października aktywistki z organizacji Just Stop Oil oblały zupą „Stonieczniki” van Gogha w National Gallery w Londynie. Ten incydent potwierdza, że w obiektach, w których są ekspozowane drogie dzieła sztuki, konieczny jest stały i skrupulatny nadzór pracowników ochrony. To oni bowiem potrafią zauważyć podejrzane zachowanie poprzedzające akt dewastacji.

Wśród przykładów nie można pominąć obiektów handlowych ze względu na ich ogólnodostępny charakter i duże nagromadzenie ludzi w jednym miej-

scu. W ostatnim czasie w tzw. centrach handlowych coraz częściej dochodzi do różnych incydentów bezpieczeństwa, a wtedy ochrona obiektu odgrywa kluczową rolę. Tego typu sytuacja miała miejsce w ostatnich tygodniach w jednej z wrocławskich galerii, w której doszło do ataku nożownika. Dzięki sprawnej interwencji pracowników ochrony udało się zapobiec tragedii.

NASTAŁY TRUDNE CZASY

Polskie społeczeństwo nie czuje się bezpieczne w codziennym życiu. Według ankiety CBOS¹ odsetek osób obawiających się, że mogą paść ofiarą przemocy, wzrósł w latach 2019-22 aż o 7 punktów procentowych – z 33 do 40%. Czy strach społeczny jest uzasadniony? Niestety tak. Dane Głównego Urzędu Statystycznego dotyczące zabójstw w Polsce² nie pozostawiają złudzeń – w 2021 r. odsetek osób zabitych wzrósł o 8% w stosunku do 2019 r. Policijne statystyki wskazują natomiast, że w 2021 r. popełniono w Polsce o ponad 19 tys. więcej przestępstw kryminalnych niż rok wcześniej³.

Na obecny poziom poczucia bezpieczeństwa Polaków ma także wpływ wojna w Ukrainie.

– W niepewnych czasach geopolitycznych na firmach zajmujących się ochroną osób i mienia spoczywa jeszcze większa odpowiedzialność. Konflikt zbrojny toczący się za naszą granicą, a także związane z nim natężone migracje to wyzwanie nie tylko dla władz rządowych i samorządowych, ale również dla firm świadczących usługi z zakresu bezpieczeństwa. Wysoka specjalizacja ich pracowników, podnoszenie kwalifikacji i odpowiednie wykształcenie kadr nabiera obecnie szczególnego znaczenia – podkreśla Jarosław Kot, członek zarządu Polskiego Związku Pracodawców Ochrona.

SEKTOR OCHRONY MIERZY SIĘ Z WYZWANIAM

Równoległe ze strachem społecznym nasila się kryzys w branży ochrony. Na pogorszenie sytuacji wpływa wiele czynników. Jednym z ważniejszych jest decyzja rządu o podniesieniu w 2023 r. płacy minimalnej o prawie 20% w stosunku do kwot obowiązujących obecnie. W połączeniu z rekordowo wysoką inflacją (17,9%)⁴ zmiany te bardzo osłabia kondycję firm z sektora ochrony. Kolejnym problemem, z którym mierzy się branża, jest wzrost cen artykułów niezbędnych do realizacji usług ochrony – o 20 do ponad 10%, np.:

- umundurowanie – o ok. 23%
- kamery i rejestratory – o 23%

- okablowanie – o ponad 40%
- modemy GSM – o ponad 50%
- buty taktyczne – o ok. 55%
- amunicja – o ponad 90%
- mikroprocesory – o 190%

Branża ochrony osób i mienia – a to rynek o wartości 11 mld zł – stoi więc obecnie przed prawdziwym wyzwaniem: jak zapewnić swoim klientom bezpieczeństwo w obliczu problemów rynkowych i nadchodzącej zmiany przepisów.

ROSNA WYMAGANIA PRACOWNIKÓW OCHRONY

Z powodu rekordowo niskiego bezrobocia (5,1%)⁵ mamy obecnie rynek pracownika, co powoduje trudności w pozyskaniu kandydatów do pracy.

– Pracownicy ochrony coraz częściej oczekują pensji w wysokości, która jest bliższa średniej krajowej niż minimalnemu wynagrodzeniu. W przypadku kwalifikowanych pracowników ochrony z bronią, pracowników grup interwencyjnych, konwojentów czy operatorów systemów zabezpieczenia technicznego ta stawka osiąga nawet dwukrotność płacy minimalnej – mówi Jarosław Kot.

Tymczasem, w związku z podwyżkami płacy minimalnej, od przyszłego roku znacząco zwiększą się minimalne koszty, jakie musi ponieść firma świadcząca usługi ochrony, która chce zatrudniać zgodnie z prawem pracowników etatowych i zleceniobiorców. Problem niedoboru kadry najdotkliwiej odczuwają instytucje, w których zapewnienie bezpieczeństwa jest obowiązkowe i na miejscu muszą być zatrudnieni wykwalifikowani pracownicy ochrony. Są to głównie placówki publiczne – muzea, filharmonie, sądy, prokuratury, ZUS, ministerstwa i jednostki wojskowe, a także działające w obszarze infrastruktury krytycznej (energetyka, kopalnie, stocznie, przedsiębiorstwa miejskie, wodociągi, oczyszczalnie ścieków itp.).

ŁUDZIE SĄ NIE DO ZASTĄPIENIA

Czy istnieje alternatywny sposób ratowania polskiej branży ochrony, np. poprzez poszerzanie wachlarza usług o rozwiązania technologiczne?

– Tego typu zwiększanie zakresu usług nie rozwiąże problemu – uważa Tomasz Wojak, prezes zarządu Polskiego Związku Pracodawców Ochrona. – Trzeba bowiem pamiętać, że inteligentne systemy bezpieczeństwa jeszcze długo nie będą w stanie całkowicie zastąpić człowieka. W krytycznych momentach, takich jak konieczność interwencji na terenie chronionego obiektu, to ludzie muszą trafnie ocenić sytuację i zdecydować o działaniu adekwatnym do zagrożenia – dodaje.

Firmy zrzeszone w Polskim Związku Pracodawców Ochrona, zatrudniające prawie 100 tysięcy pracowników, prowadzą właśnie proces renegocjacji stawek za swoje usługi – zmiany muszą wejść w życie od stycznia 2023 r.

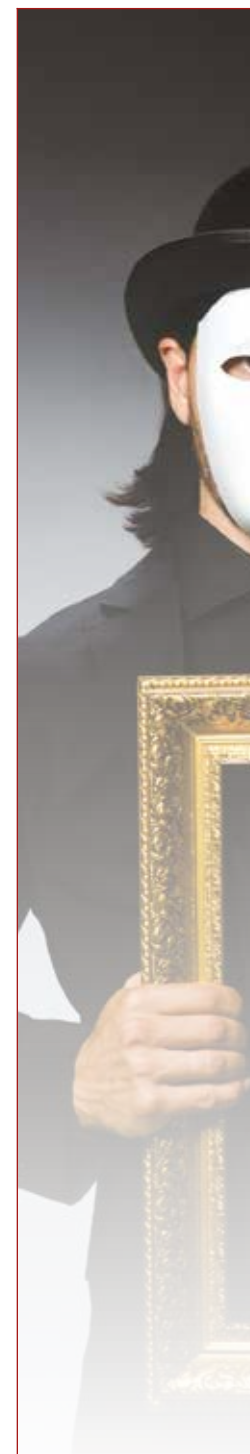
– Musimy sprostać istniejącym i nadchodzącym wyzwaniom, by zapewnić ciągłość działania i utrzymać wysokie standardy usług świadczonych naszym klientom – zaznacza Jarosław Kot. 📍

¹ Badanie CBOS „Poczucie bezpieczeństwa i zagrożenie przestępczością”, czerwiec 2022.

² Źródło: stat.gov.pl/obszary-tematyczne/wymiar-sprawiedliwosci/wymiar-sprawiedliwosci/przestepstwa-przeciwko-zyciu-i-zdrowiu,3,1.html, dostęp 14.10.2022.

³ Źródło: statystyka.policja.pl/st/przestepstwa-ogolem/przestepstwa-kryminalne/63470,Przestepstwa-kryminalne-ogolem.html, dostęp 14.10.2022.

⁴ Dane za październik 2022 r.
⁵ Dane za październik 2022 r.



POLSKI ZWIĄZEK PRACODAWCÓW OCHRONA

ul. Koszykowa 61, 00-667 Warszawa
biuro@pzpochrona.pl
www.pzpochrona.pl



Metody komunikacji central alarmowych Galaxy Dimension

Tomasz Górski

1. KOMUNIKACJA CA-PC W STANDARDZIE RS232

Najbardziej ekonomiczną i przy okazji najczęstszą formą komunikacji CA-PC jest RS232 – interfejs komunikacyjny przeznaczony do szeregowej transmisji danych. Każda centrala z rodziny central Galaxy Dimension GD48, GD96, GD264, GD520 jest fabrycznie wyposażona we wspomniany interfejs.

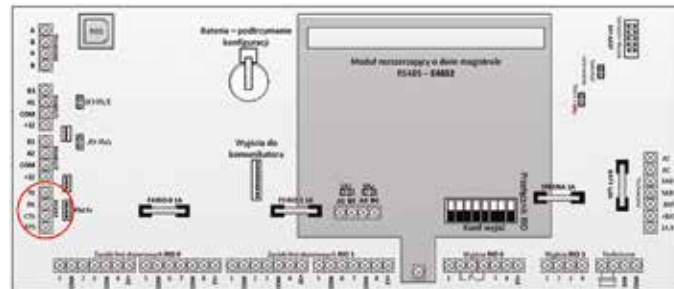
Na rys. 1 kolorem czerwonym zaznaczono lokalizację fizyczną interfejsu na płycie CA. Warto zwrócić uwagę, że zaciski śrubowe sygnałów Tx, Rx, CTS, RTS zo-

Centrale Galaxy charakteryzują się dużą różnorodnością interfejsów komunikacyjnych. Najczęściej stosuje się cztery podstawowe metody komunikacji CA-PC.

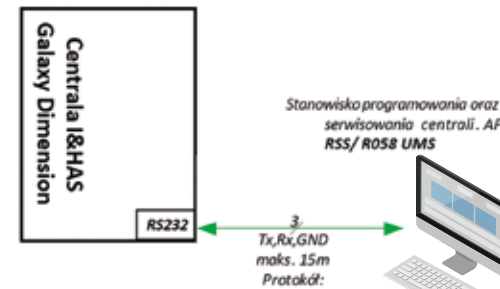
stały zwielokrotnione szybkołączką 5PIN możliwą do wykorzystania za pomocą przewodu RS232 o symbolu A234.

Na rys. 2 przedstawiono fizyczną prezentację połączenia PC-CA z wykorzystaniem interfejsu szeregowego RS232. Ważną zaletą tego rozwiązania jest duża prędkość transmisji danych pomiędzy centralą a komputerem – maks. 56 700 b/s. Ograniczeniem jest maks. odległość skutecznej transmisji – 15 m oraz brak możliwości szyfrowania i kontroli łącza.

Interfejs RS232 może być wykorzystywany do pracy z programami natywnymi GALAXY – RSS R056 Remote Servicing Suite, UMS R058 User Management Suite z wykorzystaniem protokołu Microtech lub do pracy ze środowiskiem wizualizacji graficznej (SMS, PSIM) Axxon Intellect, IFTER EQU z protokołem SIA lev. 4. Należy pamiętać, że port RS232 na płycie jest interfejsem elektrycznym, nie ma więc możliwości jednoczesnej pracy portu z wieloma aplikacjami. Diagnostycznie interfejs RS232 jest w programie centrali widziany jako COM6.



Rys. 1. Płyta główna centrali Galaxy Dimension

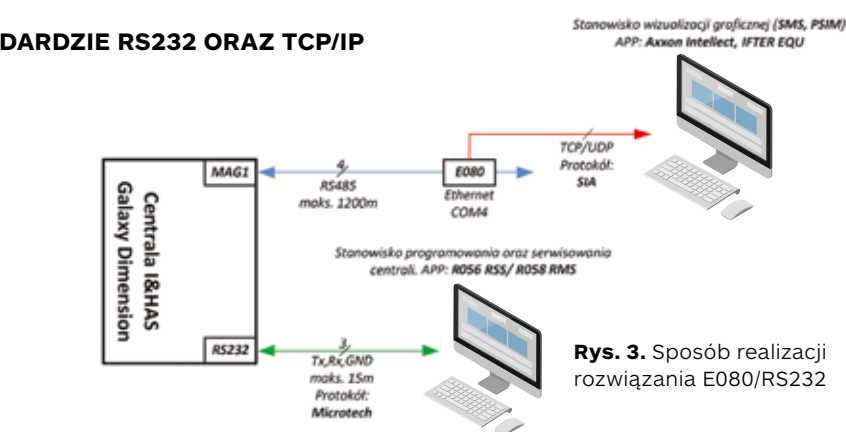


Rys. 2. Sposób realizacji podłączenia PC-CA w standardzie RS232

2. KOMUNIKACJA CA-PC W STANDARDZIE RS232 ORAZ TCP/IP

W przypadku potrzeby jednoczesnej komunikacji do stanowiska wizualizacji (SMS, PSIM) oraz stanowiska programowania i serwisu należy użyć dodatkowego interfejsu E080 Ethernet. Moduł komunikacyjny E080 może być instalowany tylko na magistrali „1” LINK RS485 (najczęściej w obudowie centrali, LINK), diagnostycznie funkcjonuje w systemie jako COM4. Moduł wspiera zarówno protokół TCP/IP (Transmission Control Protocol), jak i UDP/IP (User Datagram Protocol) – 10Base-T lub 100Base-T – zgodnie z EN50136-2:2013 Grade 4. Moduł wspiera również enkrypcję przesyłanych danych – 128-bit.

W przypadku zastosowania dwóch niezależnych interfejsów komunikacyjnych RS232/E080 tworzymy optymalne środo-



Rys. 3. Sposób realizacji rozwiązania E080/RS232

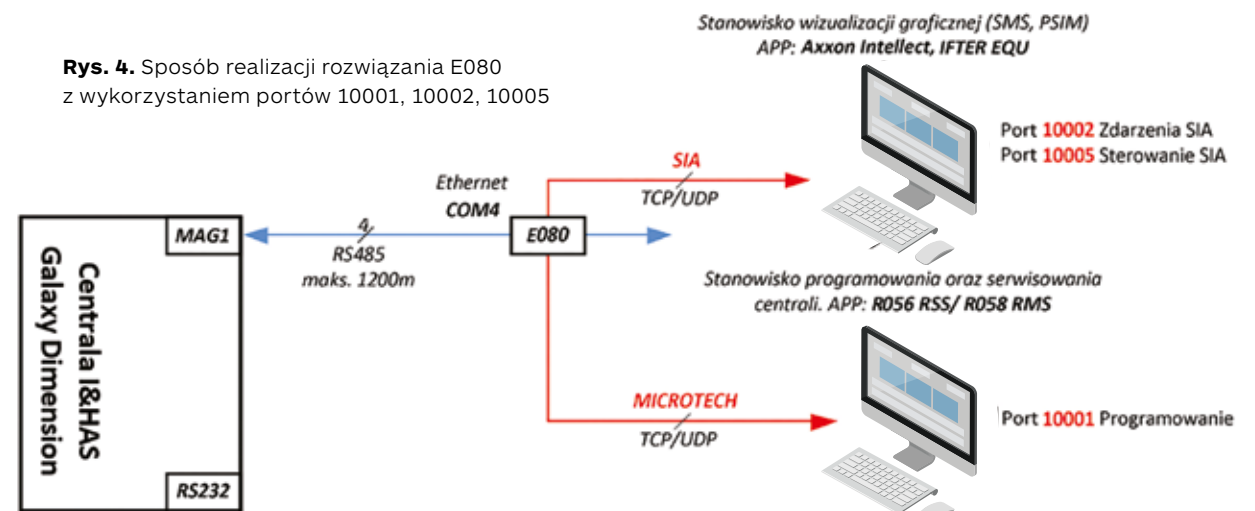
wisko pracy dla dwóch protokołów transmisji Microtech – programowanie, serwis oraz SIA – wizualizacja (SMS, PSIM). Rozwiązanie pokazane na rys. 3 umożliwia jednoczesne programowanie i wizualizację podległego systemu GALAXY Dimension. Oczywiście przypisanie protokołu, a tym samym usługi do interfejsu jest kwestią programową i zależy tylko od inwencji oraz potrzeb inwestora/użytkownika systemu (COM4-SIA, COM6-Microtech lub COM4-Microtech, COM6-SIA).

3. KOMUNIKACJA CA-PC W STANDARDZIE TCP/IP Z WYKORZYSTANIEM MODUŁU ETHERNET E080

Moduł Ethernet E080 udostępnia trzy główne porty transmisyjne: 10001 – do programowania i serwisowania centrali GD, 10002 – do „obsługi zdarzeń” wysyłanych przez centralę do stacji monitorującej (SMS, PSIM), 10005 – do „obsługi komend sterujących SIA”. Mając do dyspozycji trzy niezależne porty komunikacyjne, system „teoretycznie” umożliwia jednoczesną komunikację dla sygnałów SIA do stacji (SMS, PSIM) oraz MICROTECH dla programowania.

Niestety tego typu działania, tj. wykorzystanie dwóch protokołów komunikacyjnych w tym samym czasie z zastosowaniem interfejsu komunikacyjnego Ethernet E080, czasami prowadzi do niestabilnej pracy (zawieszania się) modułu. W takiej sytuacji niezbędny jest restart napięciowy modułu. Dlatego rozwiązanie należy traktować jako ostateczność, wykorzystując do realizacji inne wspomniane możliwości formy komunikacji.

Rys. 4. Sposób realizacji rozwiązania E080 z wykorzystaniem portów 10001, 10002, 10005

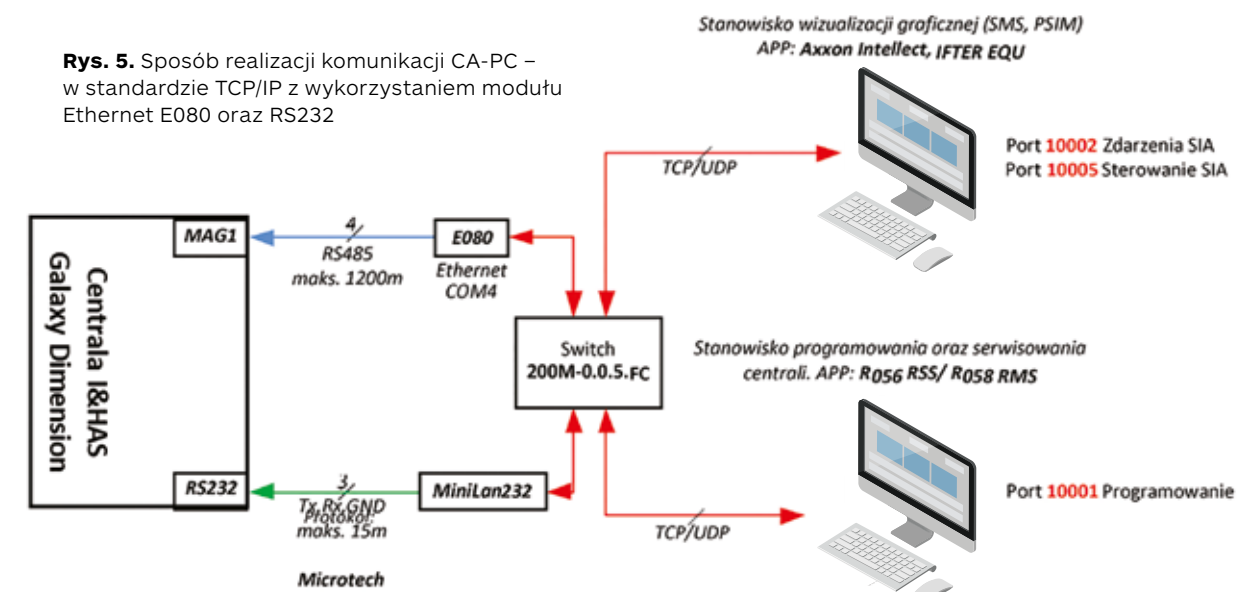


4. KOMUNIKACJA CA-PC W STANDARDZIE TCP/IP Z WYKORZYSTANIEM MODUŁU ETHERNET E080 ORAZ RS232 – STANDARD OPTIMALNY

Rozwinięciem wariantu 2 jest konwersja interfejsu RS232 do sieci TCP/IP z wykorzystaniem serwera portu szeregowego MiniLan232. Takie rozwiązanie eliminuje naturalne ograni-

czenie portu RS232 w kwestii zasięgu – 15 m. Poniższe rozwiązanie przedstawione na rys. 5 należy uznać za optymalne i docelowe.

Rys. 5. Sposób realizacji komunikacji CA-PC – w standardzie TCP/IP z wykorzystaniem modułu Ethernet E080 oraz RS232



Przedstawione zagadnienia związane z problematyką wizualizacji graficznej, serwisowania oraz programowania central alarmowych I&HAS Galaxy Dimension nie wyczerpują tematu. Po szczegóły zapraszamy do kontaktu. ☎

TAP SYSTEMY ALARMOWE

ul. Tatrzańska 8, 60-413 Poznań
www.tap.com.pl



Modelowe zabezpieczenie techniczne centrum danych

Nedap Security Management w Talex Data Center

Anna Twardowska



Centra danych są zazwyczaj doskonale chronione przed cyberatakami czy zakłóceniami ciągłości działania.

Nie można jednak zapominać o bezpieczeństwie fizycznym. Kluczowym elementem w tym zakresie jest pewna i stabilna kontrola dostępu. Nedap Security Management zbudował modelowy system KD w centrach danych firmy Talex w Poznaniu i we Wrocławiu.

Talex posiada dwa ośrodki, które oferują profesjonalne, stabilne i bezpieczne zaplecze dla wielu firm. To jedyne w Polsce Data Center, którego dwa obiekty posiadają certyfikat EN 50600 klasy 4, certyfikat ISO/IEC 22237 i są zasilane przez dwie niezależne linie zewnętrzne, agregatory prądowe i UPS w układach N+1. W zakresie kontroli dostępu firma także wybrała rozwiązanie z najwyższej półki.

BEZPIECZEŃSTWO FIZYCZNE CENTRUM DANYCH

Ośrodki Data Center firmy Talex w Poznaniu i we Wrocławiu zostały zaprojektowane zgodnie z najwyższymi standardami

i wykonane w najwyższej jakości. Szczególną wagę przywiązano do bezpieczeństwa fizycznego, które zostało zidentyfikowane jako jeden z najwyższych priorytetów.

W 2015 r. eksperci Talex rozpoczęli poszukiwania partnera, który byłby w stanie sprostać ich wysokim wymaganiom i oczekiwaniom. Analiza rynku i poznanie dostępnych rozwiązań nie trwały długo. Talex szybko zdecydował się na współpracę z holenderską firmą Nedap Security Management, która ma ponad 40 lat doświadczenia w zakresie fizycznych zabezpieczeń technicznych, a jej flagowym produktem jest system AEOS.

AEOS to system fizycznej kontroli dostępu, który z powodzeniem może zabezpieczyć zarówno wymagające najwyższego poziomu bezpieczeństwa centra danych, jak i obiekty, które nie potrzebują tak wysokiego stopnia ochrony. System został zaprojektowany z myślą o możliwości skalowania do rozmiaru wdrożenia, poziomu wymaganej od użytkowników weryfikacji uprawnień (od zwykłej karty magnetycznej, po identyfikatory biometryczne) oraz integracji z innymi działającymi już systemami.



Wnętrze Talex Data Center

– Talex to firma posiadająca własne ośrodki Data Center. Jej pracownicy doskonale wiedzieli, czego od nas oczekują. Wymagania związane z bezpieczeństwem były jasno sprecyzowane, jednak dodatkową potrzebą była możliwość samodzielnego zainstalowania oraz dalszego rozwijania systemu w ośrodkach danych i budynkach biurowych. O wyborze systemu AEOS zdecydowały najwyższa jakość na rynku, szeroka możliwość integracji oraz możliwość udostępnienia ekspertom firmy Talex wiedzy o systemie i jego instalacji – mówi Maciej Puciński z firmy Talex.

KLUCZOWE OBSZARY ZABEZPIECZONE

Ekspertom Talex szczególnie zależało na kilku obszarach, które zidentyfikowali jako kluczowe. Podstawowymi kwestiami były odpowiedni standard sprzętu oraz dostępność jego poszczególnych wariantów – firma była zainteresowana nie tylko czytnikami kart magnetycznych, ale także czytnikami biometrycznymi i skanerami zdalnymi, weryfikującymi uprawnienia na odległość. W sumie platforma miała obsłużyć 1000 identyfikatorów dla 200 przejeżdżających. Równie ważnym aspektem była możliwość centralnej kontroli nad systemami zabezpieczeń we wszystkich lokalizacjach, które mieszczą się nie tylko w dwóch ośrodkach Data Center, ale także w innych budynkach biurowych i punktach w całym kraju.

AEOS spełnił oczekiwania także jako system antywłamaniowy, który obsługuje w sumie ponad 600 czujek. Dzięki niemu udało się znacznie zredukować liczbę fałszywych alarmów. System umożliwia ponadto natychmiastowe dostosowanie uprawnień dla poszczególnych użytkowników, dzięki czemu można precyzyjnie kontrolować dostęp przydzielone pracownikom i gościom. Nie bez znaczenia była także sprawna integracja systemu firmy Nedap Security Management z rozwiązaniami innych dostawców, które już działały w obiektach Talex, w tym z istniejącymi już systemami kontroli dostępu (także bezprzewodowymi i z biometrią) oraz monitoringu wizyjnego.

cymi już systemami kontroli dostępu (także bezprzewodowymi i z biometrią) oraz monitoringu wizyjnego.

Eksperci Talex zwrócili uwagę także na szczegółowość informacji, jakich dostarcza system AEOS. To ważne zwłaszcza w przypadku tak dużej liczby obiektów i powierzchni przy stosowaniu różnych poziomów zabezpieczeń oraz w związku z dużą liczbą pracowników o zróżnicowanym poziomie przydzielonych dostępu. System pozwala nie tylko na wizualizację graficzną, co zwiększa przejrzystość i czytelność ogromnej ilości prezentowanych informacji, ale również na automatyzację procedur (np. wycofania dostępu osobie odchodzącej z firmy lub zmiany zakresu dostępu osoby przechodzącej do innego działu w wewnętrznych strukturach).

PEŁNA SAMODZIELNOŚĆ

Pierwsze wdrożenie systemu AEOS zostało przeprowadzone w 2015 r. w Data Center w Poznaniu przez zewnętrznego integratora. W trakcie tego procesu eksperci Talex zbudowali bazę wiedzy i zgromadzili kompetencje niezbędne do samodzielnego przeprowadzenia takiego projektu w przyszłości. Od tego czasu zarządzają systemem oraz kolejnymi integracjami i aktualizacjami, bazując już na własnym doświadczeniu. Co więcej, w ramach struktur Talex powstało nawet laboratorium bezpieczeństwa, w którym są przeprowadzane symulacje zdarzeń i kolejnych wdrożeń. To wszystko pozwoliło ekspertom Talex samodzielnie zaimplementować system AEOS w drugim centrum danych we Wrocławiu w 2018 r. Proces zakończył się sukcesem, a wrocławskie Data Center do dziś jest w pełni zarządzane i obsługiwane przez wewnętrzny zespół Talex.

– Doświadczenia z systemem AEOS, jego instalacją, integracją i obsługą nauczyły nas wiele na temat bezpieczeństwa fizycznego. Firma Nedap Security Management wspierała nas w decyzji o pełnej samodzielności. Nasz zespół wciąż optymalizuje systemy, przeprowadza symulacje i jest gotowy, by przeprowadzić kolejne wdrożenie w następnym obiekcie Talex lub w roli zewnętrznego integratora czy konsultanta wspierającego innych użytkowników w trakcie ich pierwszego wdrożenia – podsumowuje Maciej Puciński.



NEDAP SECURITY MANAGEMENT

al. Niepodległości 18, 02-653 Warszawa
www.nedapsecurity.com/pl/
anna.twardowska@nedap.com



Pod ziemią może być bezpieczniej

Fot.: Muzeum Górnictwa Węglowego w Zabrzu

Ewelina Dembińska



Aby móc podnieść poziom bezpieczeństwa oraz efektywność działania muzeum, C&C Partners – na bazie wieloletniego doświadczenia – dostosowała szereg rozwiązań do specyfiki czterech obiektów składających się na muzeum, biorąc pod uwagę obowiązujące przepisy.

ZARZĄDZANIE OBRAZEM

Jednym z podstawowych systemów poprawiających bezpieczeństwo w Kopalni Guido jest system monitoringu wizyjnego dostosowany do specyfiki obiektu. Dzięki oprogramowaniu VMS do zarządzania materiałem wizyjnym możliwa jest rejestracja i analiza obrazu pochodzącego z kamer rozmieszczonych na terenie kopalni. Kluczową cechą tego systemu jest otwartość na współpracę z kamerami zarówno analogowymi, jak i IP od wielu producentów.

SYSTEM ALARMOWY

System sygnalizacji włamania i napadu informujący o nieautoryzowanych wejściach do wybranych pomieszczeń pozwala na automatyczne uzbrajanie i rozbrajanie stref bezpieczeństwa oparte na zaplanowanym harmonogramie eksploatacji obiektu.

Kopalnia Guido to unikatowy na skalę europejską obiekt turystyczny, w którym można zjechać do podziemi oryginalną szolą i doświadczyć tego, jak wyglądała i nadal wygląda praca górników. Na turystów czeka niemal 5 km tras turystycznych w pokopalnianych korytarzach. I to wszystko do 355 metrów pod ulicami Zabrze.

Informacje o alarmie są przysyłane do służb ochrony. Natomiast zarządzanie całym systemem odbywa się z poziomu wizualizacji w centrum monitoringu.

KONTROLA DOSTĘPU

Kolejnym systemem zapewniającym bezpieczeństwo w Kopalni Guido jest kontrola dostępu umożliwiająca zarządzanie dostępem do pomieszczeń administracyjnych. Integracja systemu kontroli dostępu z depozytorem kluczy pozwala w łatwy sposób zarządzać uprawnieniami do kluczy z poziomu jednego systemu.

ZARZĄDZANIE BEZPIECZEŃSTWEM Z JEDNEGO MIEJSCA

Efektywne zarządzanie bezpieczeństwem polega przede wszystkim na zbieraniu informacji ze wszystkich zdarzeń w jednym miejscu. Do tego służy rozwiązanie iProtect (SMS) dedykowane do monitorowania i zarządzania wszystkimi systemami z jednego stanowiska operatorskiego w ramach jednego centrum nadzoru. W przypadku kopalni system integruje różnorodne podsystemy, m.in. kontroli dostępu, sygnalizacji włamania i napadu, monitoringu wizyjnego. Co wię-

cej, wdrożone rozwiązanie, dzięki rozbudowanym interfejsom umożliwiło integrację z systemem firm trzecich. W przypadku kopalni – z systemem sygnalizacji pożarowej oraz systemem zarządzania kluczami.

PODSUMOWANIE

Dostarczane do Kopalni Guido systemy wspomagają pracę oraz podnoszą poziom bezpieczeństwa zarówno gości, jak i obsługi technicznej. Zapewniają ochronę i funkcjonalność muzeum, przy jednoczesnej optymalizacji kosztów związanych z ich zarządzaniem. Wprowadzenie zintegrowanego systemu zarządzania bezpieczeństwem gwarantuje modularną rozbudowę oraz otwarte interfejsy dla innych urządzeń działających na terenie obiektu. Takie podejście zapewnia bezpieczeństwo inwestycji i możliwość jej rozbudowy w czasie. ☑

C&C PARTNERS

ul. 17 Stycznia 119, 121
64-100 Leszno
www.ccpartners.pl
e.dembińska@ccpartners.pl



Wytyczne 2N dotyczące automatyki domowej



W październiku br. firma badawcza ResearchAndMarkets opublikowała raport na temat rynku inteligentnej automatyki domowej. Przewiduje się, że do 2028 r. osiągnie on globalnie wartość 187,8 mld USD, ze średnioroczną stopą wzrostu (CAGR) na poziomie 15,2%. Część tego wzrostu będzie pochodzić od systemów automatyki domowej rozszerzonych o kontrolę dostępu. Ten trend zaczyna być widoczny w wielu krajach na całym świecie.

Uwzględniając tendencję wzrostową, a także z okazji „Europejskiego miesiąca cyberbezpieczeństwa 2022”, firma 2N – światowy lider w dziedzinie systemów kontroli dostępu IP – wydała wytyczne mające na celu pomoc integratorom i instalatorom, którzy rozważają włączenie urządzeń kontroli dostępu do systemów automatyki domowej swoich klientów.



WYTYCZNE 2N DOTYCZĄCE INTEGRACJI TECHNOLOGII KONTROLI DOSTĘPU Z SYSTEMAMI AUTOMATYKI DOMOWEJ

1 Należy pamiętać o pełnym zakresie dostępnych korzyści w kwestii bezpieczeństwa

Wielu właścicielom domów, którzy chcą przenieść swój system zabezpieczeń na wyższy poziom, integracja kontroli dostępu z systemem automatyki domu może dać dokładnie to, czego szukają. Wyobraźmy sobie np., że włamywacz krąży wokół posesji i dzwoni domofonem, aby sprawdzić czy w domu są domownicy. Dzięki interkomowi IP możemy odbierać połączenia na smartfonie. Możemy zobaczyć włamywacza i porozmawiać z nim, a jeśli chcemy – możemy również udawać, że jesteśmy w domu. Podłączenie interkomu do systemu automatyki domowej oznacza, że możemy pójść krok dalej, podejmując działania w czasie rzeczywistym, np. poprzez zdalne włączenie światła w wybranych częściach domu. W większości przypadków to wystarczy, by odwieść włamywacza od złych zamiarów.

2 Warto rozważyć wszystkie udogodnienia, jakie może zaoferować kontrola dostępu

Integracja takich produktów, jak 2N® Indoor Touch 2.0 z systemami automatyki domowej, np. firm Crestron, GIRA, Basalte, LOXONE oraz innych stosujących standardy KNX, może przekształcić je w centralny panel sterowania, regulujący wszystko, począwszy od oświetlenia, klimatyzacji i systemu audio, a skończywszy na bramie garażowej i systemie nawadniania trawnika. Ponadto podłączenie interkomów IP do sys-

temów *smart home* może np. ułatwić dostawę przesyłek, gdy właściciel znajduje się poza domem. Korzystając ze zdalnego sterowania drzwiami, można za pośrednictwem aplikacji otworzyć bramę kurierowi, a nawet zaprogramować system tak, aby z interkomu odtwarzany był spersonalizowany komunikat powitalny. Następnie można przełączyć się w aplikacji do strumienia z zewnętrznej kamery IP i upewnić się, że kurier umieści przesyłkę we właściwym miejscu.

3 Zdalne zarządzanie pozwala zaoszczędzić czas i pieniądze

Klienci automatyki domowej zazwyczaj cenią sobie możliwość dodawania nowych, niezwykłych funkcji do swoich inteligentnych domów. Opcje zdalnego zarządzania, takie jak platforma w chmurze My2N, mogą tu naprawdę wiele zmienić, umożliwiając integratorom skuteczniejszą obsługę klientów, dzięki czemu oszczędzają oni zarówno czas, jak i pieniądze.

4 Priorytetowe podejście do cyberbezpieczeństwa urządzeń kontroli dostępu

Cyberbezpieczeństwo jest oczywiście tak samo ważne, jak bezpieczeństwo fizyczne. ☑

2N TELEKOMUNIKACE

Pod Vinicí 20, 143 01 Praha 4
Czech Republic
www.2n.com



Innowacyjne rozwiązania biometryczne



Rozmowa
z Markiem Piotrowskim,
przedstawicielem firmy
ZKTeco na Polskę



Co wyróżnia firmę ZKTeco wśród dostawców oferujących rozwiązania do kontroli dostępu?

Rynek kontroli dostępu staje się coraz bardziej konkurencyjny. Chcąc odnieść sukces, firmy muszą nieustannie wprowadzać innowacje technologiczne i stosować zaawansowane funkcje do gromadzenia oraz analizy danych uzyskanych z urządzeń KD, a następnie stosować je do sterowania przepływem osób, śledzenia przemieszczających się gości w określonych obszarach czy tworzenia innych specjalnych aplikacji wykraczających poza zwykłe otwieranie i zamykanie drzwi.

Oferowane rozwiązania powinny zapewniać kontrolę dostępu realizowaną w sposób ciągły, a dostęp do niej powinien być możliwy z każdego miejsca na świecie. Pod tym względem firma ZKTeco radzi sobie bardzo dobrze, stając się uznanym na świecie

dostawcą rozwiązań z zakresu technologii biometrycznych i analitycznych rozwiązań informatycznych.

Co można powiedzieć o waszych rozwiązaniach biometrycznych?

Pod względem technologii biometrycznych firma ZKTeco zawsze plasowała się w czołówce innowacji. Jako jedna z pierwszych już w 2012 r. wprowadziła do urządzeń KD algorytmy do rozpoznawania twarzy, a dwa lata później algorytmy do analizy układu naczyń krwionośnych dłoni. Obie technologie identyfikacji zyskały popularność na świecie, zwłaszcza podczas ostatniej pandemii, która zmusiła użytkowników do korzystania z bezdotykowych rozwiązań biometrycznych.

Firma wdrożyła do produkcji szereg modułów rozpoznawania twarzy i dłoni, które do analizy wykorzystują obrazy z kamer uzyskane w świetle widzialnym lub bliskiej podczerwieni. Liczymy, że szczególnie analiza dłoni stanie się technologią głównego nurtu ze względu na łatwość jej użycia i dokładność identyfikacji. Jest technologią najbardziej przyjazną dla użytkownika i najbezpieczniejszą. Aby uzyskać uwierzytelnienie, wystarczy „przywitać się” z urządzeniem, podobnie jak witamy się ze znajomym, jednak nie dotykając urządzenia. Ta metoda zdecydowanie wypiera nieco już przestarzałe rozwiązania rozpoznające linie papilarne palców.

Co więcej, nasze rozwiązania „trzy w jednym” integrują najnowocześniejsze bezdotykowe analizatory biometryczne do rejestrowania cech geometrycznych dłoni i naczyń krwionośnych pod jej skórą, oferując doskonałą ochronę przed fałszowaniem i możliwość szybkiej weryfikacji uzyskanych danych z odległości do 35 cm od urządzenia.

Jesteśmy pionierami w łączeniu różnych rozwiązań biometrycznych w jednym urządzeniu, mogą zaofiarować najwyższy poziom bezpieczeństwa i wydajności dla każdego projektu, przy jednoczesnym zapewnieniu wygody korzystania z tych rozwiązań.

Czy pandemia COVID-19 wpłynęła na wzrost popytu na technologie biometryczne?

Niewątpliwie tak. Nastąpił przyspieszony rozwój technologii wywołany znaczącym wzrostem popytu na urządzenia do bezkontaktowej weryfikacji. Firmy oferujące technologie biometryczne, łącząc je ze sztuczną inteligencją i algorytmami głębokiego uczenia, przeszły przyspieszoną ewolucję. Powstała w tym czasie ogromna liczba urządzeń dodatkowo wzbogaconych o takie funkcje, jak zdalny pomiar temperatury ciała, wykrywanie masek ochronnych na twarzach czy sprawdzanie posiadania certyfikatów szczepień. Oczywiście i tu dla zapewnienia wyższego poziomu bezpieczeństwa mieliśmy do czynienia z integracją tych funkcji.

Jak zmieniły się wymagania Państwa klientów w ostatnim czasie?

Coraz częściej klienci decydują się na systemy oparte na chmurze, które gromadzą dane na zewnętrz-

nych serwerach i którymi można zarządzać z dowolnego miejsca na świecie.

Po pandemii praca zdalna już z nami zostanie, rosną więc wymagania co do bezpieczeństwa stosowanych w tej formie narzędzi. Wzrosła popularność rozwiązań biometrycznych i to nie tylko w obiektach o wymaganym wysokim stopniu zabezpieczenia. Rozwiązania te są już masowo stosowane w obiektach handlowych, w branży transportowej i turystycznej, budynkach użyteczności publicznej, placówkach służby zdrowia itp. Nawet integratorzy systemów zabezpieczeń przekształcają swoje rozwiązania dla biznesu tak, aby sprostać rosnącym wymaganiom nowych technologii, rozszerzając ich funkcje dozoru wizyjnego o rozpoznawanie twarzy.

Jakie są główne zalety wykorzystania rozwiązań biometrycznych?

Systemy oparte na cechach biometrycznych mają wiele zalet. Przykładowo użytkownik nie musi pamiętać hasła, ani nosić przy sobie karty magnetycznej. Wzorce służące do uwierzytelniania nie mogą zostać utracone ani przeniesione, jak inne dane identyfikacyjne, co zapobiega oszustwom.

Weryfikacja tożsamości i precyzyjne śledzenie aktywności konkretnych osób odgrywa kluczową rolę również w poprawie bezpieczeństwa.

Rozwiązania te można łatwo zintegrować z istniejącymi systemami, a uzyskane dane poddać analizie w celu oceny ryzyka i tworzenia unikalnych procedur w zarządzaniu dostępem do obiektu i jego bezpieczeństwem.

Jak będzie ewoluował rynek biometrii w ciągu najbliższych pięciu lat?

Zastosowanie technik biometrycznych szybko rośnie, wciąż pojawiają się nowe dziedziny i branże, w których zaczynają być wdrażane. Stawiamy na biometrię w opiece zdrowotnej, szkolnictwie, systemach bezpieczeństwa na lotniskach i przy wejściu na pokład samolotów, w branży rozrywkowej i hotelarskiej, usługach finansowych, handlu detalicznym i przemysle motoryzacyjnym.

W ochronie zdrowia biometria ma już bardzo ciekawe zastosowania, takie jak potencjalna redukcja błędów medycznych czy weryfikacja e-recept. W przypadku studentów i uczniów rośnie zastosowanie w dostępie do określonych sal i materiałów dydaktycznych.

Widzę popularność naszych rozwiązań w branży motoryzacyjnej. Pewnego dnia kierowca otworzy drzwi swojego samochodu i uruchomi go, kładąc dłoń na czytniku, który zidentyfikuje uprawnienia



do kierowania pojazdem. Po pozytywnej weryfikacji fotel, lusterka, radio i pozostała elektronika w samochodzie zostaną automatycznie dostosowane do niego. Opracowaliśmy już innowacyjne rozwiązania do automatów sprzedażowych, usług bankowych i finansowych. Oferowane przez nas rozwiązania biometryczne umożliwiają producentom z dowolnej dziedziny integrację naszych modułów, czytników i terminali biometrycznych z ich rozwiązaniami, co prowadzi do praktycznie nieograniczonych zastosowań.

Co myślicie o modnym ostatnio zastosowaniu kodów QR w kontroli dostępu?

Rzeczywiście popularność kodów QR w kontroli dostępu, tak jak w innych dziedzinach, rośnie. Rozwiązania z czytnikami tych kodów nie zapewniają wysokiego stopnia zabezpieczenia. Biorąc jednak pod uwagę ich popularność w niektórych zastosowaniach, oferujemy szereg urządzeń z wbudowanymi czytnikami kodów QR, traktując ten wygodny sposób uwierzytelniania jako dodatek do istniejących innych rozwiązań. Co więcej, aby podnieść poziom bezpieczeństwa, opracowaliśmy unikalny system generowania dynamicznych kodów QR. Kod taki staje się nieaktywny od razu po jego pierwszym użyciu, a w jego miejsce jest generowany i wysyłany do użytkownika nowy kod QR.

A co z innymi urządzeniami z waszej oferty handlowej?

Jak każda firma chcemy się rozwijać. Dlatego niezależnie od rozwoju technologii stosowanych w kontroli dostępu i rejestracji czasu pracy – w tym obszarze czujemy się liderami – rozszerzamy intensywnie naszą ofertę innych produktów związanych z sektorem zabezpieczeń, starając się je integrować ze sobą. I tak nasze bramki przejścia, kotłowroty, szlabany czy wykrywacze metali łatwo można zintegrować z naszymi urządzeniami KD, a dzięki oferowanym narzędziom integrującym (SDK, API) także z urządzeniami innych producentów. 🔄



ZKTECO EUROPE

Carretera Fuencarral 44,
Edificio 1, Planta 2,
28108 Alcobendas, Madryt
marek.piotrowski@zkteco.eu
www.zkteco.eu





35 lat temu zaczęła się nasza historia

Rozmowa z Tomaszem Bujakiem,
prezesem Telbud SA



Gratulujemy jubileuszu 35-lecia działalności firmy. To dobra okazja do świętowania.

Bardzo dziękuję. Jubileusz świętowaliśmy wiosną na dwudniowym wyjeździe integracyjnym połączonym z prezentacją dotychczasowych osiągnięć i planów firmy na najbliższy czas. Natomiast na przełomie września i października zorganizowaliśmy trzydniową wycieczkę, podczas której spędziliśmy wspólnie czas w Ojcowskim Parku Narodowym i Katowicach. Wybraliśmy się też do Spodka na stand-up i zwiedziliśmy Kopalnię Guido w Zabrze. Było dość intensywnie – te trzy dni spędziliśmy razem, zarówno w podróży, jak i w odwiedzanych przez nas miejscach. Chcieliśmy po prostu dobrze się zintegrować. Nasz zespół to zarówno młodzi specjaliści, jak i doświadczona, od wielu lat związana z firmą kadra fachowców. Był to dla nas ważny czas.

Od końca lat 80. sporo się zmieniło. Jakie były początki firmy?

Zaczynaliśmy od opracowania komputerowego systemu billingowego dla analogowych central telekomunikacji publicznej. Systemy nazywały się TPT-Emp i TPT-E. Do 2005 r. rozbudowaliśmy prawie 500 takich central dla służby zdrowia, energetyki, górnictwa i hotelarstwa.

Teraz specjalizujecie się w integracji systemów zabezpieczeń technicznych. Jak doszliście do tego momentu?

Nasze dzisiejsze know-how to spory bagaż doświadczeń związanych z projektowaniem i budową systemów zabezpieczeń technicznych. Lata 1993 – 2005 były dla nas szczególnie ważne. W pierwszej połowie lat 90. ub. w. opracowaliśmy system nadzoru i sterowania urządzeń technicznych dla obiektów radio-telewizyjnych TP-Emitel. W 1997 r. przejęliśmy poznański oddział pracowni automatyki „Elektroprojekt”, która opracowała pierwszy w kraju system komputerowej automatyki bazy paliw w Rejowcu Poznańskim. W tym okresie stworzyliśmy też komputerowy system integrujący ARGUS, który został wykorzystany do integracji ochrony technicznej stacji elektroenergetycznych PSE SA. W 2002 r. za system ARGUS otrzymaliśmy Medal Europejski Business Center Club.

Można więc przyjąć, że system ARGUS też w tym roku obchodzi jubileusz.

Ma dobre 20 lat. Aktualnie ARGUS zabezpiecza obiekty w branżach paliwowo-energetycznej, infrastruktury krytycznej i służb

mundurowych. W 2014 r. system uzyskał certyfikację CNBOP-PIB, może więc być stosowany do monitoringu i sterowania instalacjami ochrony przeciwpożarowej i instalacjami wykorzystywanymi w trakcie alarmu pożarowego. W przyszłym roku startujemy z nową odsłoną platformy integrującej ARGUS w wersji 2.0. Pierwsze testy na „żywych” obiektach mamy już za sobą.

Czym będzie się różniła nowa wersja systemu ARGUS od poprzedniej?

ARGUS w wersji 2.0 jest wykonany z zastosowaniem najnowszych technologii. Duży nacisk postawiliśmy na bezpieczeństwo transmisji i zabezpieczenie przed utratą danych. Stworzyliśmy mechanizmy redundancji baz danych, co oznacza, że system w momencie utraty komunikacji z serwerem centralnym przełącza się na jeden z serwerów zapasowych. W ARGUS 2.0 zastosowaliśmy nowoczesny interfejs graficzny z udoskonaloną ergonomią. Uprościliśmy zarządzanie systemem, które w pełni może być prowadzone przez administratora. Wdrożyliśmy też mechanizm bazy edycyjnej i ruchowej, który umożliwia wprowadzanie zmian bez ingerencji w aktualnie działający system.

Cechą niezmienną jest elastyczność naszej platformy integrującej. W ARGUS może zostać zintegrowany każdy system, do którego producent udostępnia protokół komunikacyjny, serwer OPC lub biblioteki programistyczne do integracji. Mamy kod źródłowy oprogramowania, możemy więc szybko dostosować software do bieżących zmieniających się wymagań dla systemów już działających w obiektach.



W 2002 r.
za system ARGUS
otrzymaliśmy

**Medal
Europejski
Business
Center Club.**

Dla nowego systemu zaplanowaliśmy wersję BASIC z myślą o integracji systemów w mniejszych obiektach. Dla dużych i rozproszonych obiektów będzie przeznaczona wersja ENTERPRISE.

Jak zaplanowaliście kanały dystrybucji dla tych wersji?

Wersję ENTERPRISE przeznaczoną dla większych obiektów chcemy wdrażać za pośrednictwem firm instalatorskich. Kilka rozmów z takimi firmami już przeprowadziliśmy. Nadal wdrożenia ARGUS 2.0 w wersji ENTERPRISE będziemy realizować także we własnym zakresie, zarówno podczas budowy systemów zabezpieczeń, jak i podczas integracji systemów już istniejących w obiekcie.

Natomiast sprzedaż wersji BASIC planujemy realizować za pośrednictwem dystrybutorów systemów zabezpieczeń i poprzez naszą stronę internetową. ARGUS 2.0 BASIC będzie oprogramowaniem łatwym w instalacji i obsłudze. Instalatorzy po zapoznaniu się z instrukcją i prezentacjami wideo będą mogli bez trudu integrować takie systemy, jak CCTV, ppoż., SSWiN czy KD w mniejszych lub mniej skomplikowanych obiektach.

Czym wyróżniacie się na rynku security po 35 latach działania?

Mamy za sobą wiele doświadczeń w projektowaniu i budowie elektronicznych systemów zabezpieczeń. Z naszych usług korzystają największe i strategiczne dla gospodarki kraju przedsiębiorstwa. Nasi projektanci posiadają licencje pracowników zabezpieczenia technicznego II stopnia, uprawniające do projektowania systemów alarmowych i ppoż. oraz wymagane uprawnienia budowlane telekomunikacyjne i elektryczne. Posiadane przez nas krajowe świadectwo bezpieczeństwa przemysłowego I stopnia, jak również odpowiednie świadectwa bezpieczeństwa NATO SECRET i SECRET UE/EU SECRET, potwierdzają pełną zdolność do ochrony i przetwarzania informacji niejawnych oznaczonych klauzulą „tajne”. Możemy więc projektować infrastrukturę obiektów wojskowych i bezpieczeństwa kraju. Pełna zdolność w tym zakresie jest rzadkością w naszej branży.

Poza tym dysponujemy autorskim oprogramowaniem ARGUS klasy PSIM oraz kompletnym systemem certyfikowanym przez CNBOP-PIB do integracji urządzeń ppoż. ARGUS RV-C. Świadectwo dopuszczenia obejmuje wszystkie podstawowe elementy w zabudowach w pełni wyposażonych w urządzenia zasilające, komunikacyjne i zabezpieczające. Umożliwia nam to budowanie zintegrowanych systemów zarządzania bezpieczeństwem pożarowym bez potrzeby stosowania dodatkowych urządzeń nieposiadających certyfikacji, jak serwery czy switchy.

Chciałbym podkreślić, że nie byłoby w tym miejscu, gdyby nie fantastyczny zespół pracowników, ekspertów i podwykonawców. Mamy też świetnych partnerów, z którymi od wielu lat współpracujemy przy zabezpieczaniu obiektów.

Czy przewiduje Pan wzrost zapotrzebowania na integrację systemów zabezpieczeń?

Znaczenie bezpieczeństwa w ostatnich dwóch latach znacznie wzrosło. Większe zapotrzebowanie na zaawansowane zabezpieczenia zarówno dużych, jak i mniejszych obiektów obserwujemy m.in. po liczbie zapytań. Wzrosło też zainteresowanie systemami PSIM i SMS ze strony instalatorów. Klienci szukają wyższej efektywności w sterowaniu i monitorowaniu systemów. Ważna jest dla nich również optymalizacja kosztów ochrony obiektów. ☺

TELBUd SA

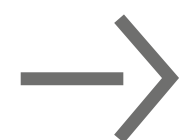
ul. Krauthofera 23, 60-203 Poznań
telbud@telbud.pl
<https://telbud.pl>





System Zarządzania Ciągłością Działania (BCMS)

Część 7. Kolejne kroki – Etap 2. Przeglądy, testy i budowanie świadomości



To już ostatnia część cyklu o wdrażaniu systemu BCMS. Przejście poszczególnych kroków usprawni pracę systemu i działanie firmy.



Tomasz Guzikowski

Celem kolejnego kroku jest utrzymanie systemu zarządzania ciągłością działania w organizacji (w tym m.in. jego monitorowanie i przeglądy), zapewnienie bieżących aktualizacji dokumentacji wdrożonego systemu, wykonania testów i odpowiedniego przeszkolenia zaangażowanych w cały proces osób.

Aby osiągnąć cel niniejszego kroku, należy przeprowadzić następujące działania:

1. WSKAZANIE OSÓB ODPOWIEDZIALNYCH ZA REALIZACJĘ PRZEGLĄDÓW, AKTUALIZACJI I TESTÓW OPRACOWANYCH PLANÓW DLA ZAPEWNIENIA ICH AKTUALNOŚCI I ADEKWATNOŚCI.

O tym była mowa w poprzednich częściach naszego cyklu.

2. OPRACOWANIE ZAŁOŻEŃ, ŁĄCZNIE Z HARMONOGRAMEM, CYKLICZNYCH AUDYTÓW I PRZEGLĄDÓW SYSTEMU ORAZ ICH TERMINOWA REALIZACJA

Audyt BCMS powinien się odbywać cyklicznie na podstawie harmonogramu i programu zatwierdzonego przez najwyższe kierownictwo. Powinien być prowadzony przez niezależnych, przeszkolonych audytorów wewnętrznych. Celem audytu jest weryfikacja, czy wdrożony system spełnia wymogi zgodności z przyjętą przez organizację polityką zarządzania ciągłością działania, opracowaną strategią, przepisami prawa, normami i rekomenda-

cjami. Z punktu widzenia potencjalnych efektów audyt pełni następujące funkcje:

- **weryfikującą** – potwierdzi, czy ustanowiony i utrzymywany system zarządzania jest zgodny z wymaganiami normatywnymi i wewnętrznymi, a także czy wcześniej wskazane niezgodności zostały usunięte;
- **wartościującą** – oceni stopień skuteczności i efektywności BCMS;
- **informującą** – dostarczy informacji nt. funkcjonowania badanego BCMS, co będzie kluczowe dla wspomagania procesów decyzyjnych na różnych szczeblach zarządzania;
- **korygującą** – w przypadku stwierdzenia niezgodności podczas przeprowadzonego audytu będą wprowadzane działania korygujące, mające na celu wykrucie i wyeliminowanie przyczyn tych niezgodności;
- **zapobiegawczą** – w przypadku wykrycia podczas audytu możliwości powstania niezgodności, w przyszłości będą wprowadzane działania zapobiegawcze, wyprzedzające wystąpienie niezgodności;
- **doskonalącą** – audyt zidentyfikuje słabości organizacji i wskaże obszary, które powinny być doskonałe;
- **instruktażową** – audytor będzie mógł podpowiedzieć stronie audytowanej prawidłowe metody postępowania lub dobre praktyki w audytowanym obszarze.

Program audytu powinien określać kryteria, zakres, częstotliwość oraz sposób ich przeprowadzania. Będzie wspierał także elementy, jak:

- Monitorowanie i badanie efektywności systemu
- Przegląd systemu przez kierownictwo
- Pomiar stopnia osiągnięcia celów
- Samoocenę organizacji
- Koszty funkcjonowania BCMS.

Wynikiem przeglądu BCP powinna być aktualizacja tych jego części, w których stwierdzono konieczność wprowadzenia zmian. Aktualizację BCP przeprowadza się w przypadku wystąpienia następujących zmian:

- listy procesów biznesowych objętych planem,
- struktury organizacyjnej lub struktury zarządzania kryzysowego,
- krytycznych zasobów, w tym systemów informatycznych,
- sposobu realizacji procesu biznesowego objętego planem,
- krytycznych dostawców usług i partnerów biznesowych lub warunków współpracy,
- wynikających z rekomendacji z przeprowadzonych audytów, testów lub rzeczywistych awarii,
- w regulacjach prawnych.

Za aktualizację BCP odpowiadają właściciele procesów nim objętych.

3. OPRACOWANIE HARMONOGRAMU I REALIZACJA CYKLICZNYCH TESTÓW OPRACOWANYCH PLANÓW BCP, DRP

Jednym z koniecznych elementów wskazanego etapu projektu wdrażania BCMS

jest opracowanie i wdrożenie programu ćwiczeń i testów w organizacji. Wskazany etap pozwala na określenie praktycznej zdolności organizacji do kontynuacji i odtworzenia krytycznych procesów biznesowych. Dzięki temu można dokonać weryfikacji całego systemu zarządzania. W trakcie prowadzenia testu, kiedy dochodzi do interakcji pomiędzy zespołami kryzysowymi, mogą zostać ujawnione braki. Ponadto wyniki testów mogą w konsekwencji doprowadzić do optymalizacji procedur.

Testy BCMS mogą być realizowane w następujących formach:

- **TESTU ORIENTACYJNEGO** – polegającego na szkoleniu mającym zapoznać uczestników z ogólnymi zasadami postępowania w sytuacji kryzysowej, ze wskazaniem odpowiedzialności, rolami zespołów, zadaniami i oczekiwaniami. Celem testu jest weryfikacja znajomości procedur w ramach BCP.
- **TESTU POWIADAMIANIA** (komunikacyjnego) – mającego na celu weryfikację:
 - skuteczności przepływu informacji w ramach struktury zarządzania kryzysowego w organizacji,
 - aktualności listy kontaktowej (m.in. członków struktury zarządzania kryzysowego, dostawców, instytucji publicznych itd.),
 - dostępności pracowników organizacji wchodzących w skład struktury zarządzania kryzysowego.
- **GRY SZTABOWEJ** – zorganizowanej w formie dyskusji panelowej, podczas której omawia się kolejne kroki postępowania w sytuacji kryzysowej. Test ma na celu:
 - zbadanie spójności i prawidłowości opracowanych procedur,
 - sprawdzenie przygotowania jednostek struktury zarządzania kryzysowego do stosowania właściwych procedur awaryjnych oraz współpracy pomiędzy jednostkami struktury zarządzania kryzysowego,
 - weryfikację listy zasobów niezbędnych jednostkom struktury zarządzania kryzysowego do pracy w sytuacji kryzysowej.
- **TESTU SYMULACYJNEGO** – przeprowadzonego w formie ograniczonej symulacji sytuacji kryzysowej. Ma on na celu:
 - zweryfikowanie zdefiniowanego wycinka planów i procedur,
 - koordynację działań jednostek struktury zarządzania kryzysowego,
 - weryfikację dostępności niezbędnych zasobów.
- **TESTU OPERACYJNEGO** – przeprowadzonego z wykorzystaniem środowiska zapasowego, stworzonego do zasymulowania sytuacji kryzysowej. Test ma na celu:
 - weryfikację stopnia przygotowania jednostek wchodzących w skład struktury zarządzania kryzysowego do zarządzania i pracy w sytuacji kryzysowej,
 - weryfikację kanałów komunikacji przyjętych w procedurach awaryjnych,
 - kontrolę poprawności wykonania przełączenia systemów informatycznych niezbędnych do realizacji kluczowych procesów biznesowych,
 - weryfikację możliwości kontynuacji procesów kluczowych w środowisku zapasowym,
 - sprawdzenie efektywności rzeczywistej mobilizacji personelu i zasobów w wybranych lokalizacjach.

4. OPRACOWANIE HARMONOGRAMU I PROWADZENIE SZKOLEŃ DLA PRACOWNIKÓW ZAANGAŻOWANYCH W REALIZACJĘ PLANÓW BCP, DRP ORAZ UTRZYMANIE SYSTEMÓW KLUCZOWYCH

Program budowania świadomości w zakresie BCMS powinien być skierowany do wszystkich pracowników organizacji. Ma on na celu zwiększenie prawdopodobieństwa skutecznej realizacji BCP w przypadku konieczności jego uruchomienia. Uświadamianie pracowników może być realizowane m.in. poprzez:

- zbudowanie portalu intranetowego zawierającego informacje o BCMS,
- ćwiczenia ewakuacyjne i ppoż.,
- akcje promujące znaczenie BCMS wewnątrz organizacji (m.in. dni bezpieczeństwa, prezentacje dla nowo przyjętych pracowników w ramach on-boardingu, artykuły w newsletterze, prezentacje materiałów filmowych z przeprowadzonych testów, konkursy wiedzy, plakaty itp.),
- szkolenia w formie e-learningowej z możliwością przeprowadzenia testu.

Kluczową rolę w podnoszeniu świadomości ma bezpośrednie zaangażowanie najwyższego kierownictwa organizacji we wszystkie działania związane z promowaniem BCMS.

Oprócz budowania świadomości niezbędne jest przygotowanie i wdrożenie programu szkoleniowego dla wszystkich

pracowników. Szkolenia mają na celu dostarczenie informacji niezbędnych do uczestnictwa w praktycznych działaniach dotyczących BCMS. W trakcie szkoleń pracownicy zdobywają wiedzę m.in. o tym, jaki jest cel i zakres BCMS, kto jest odpowiedzialny za poszczególne elementy planu oraz jaka jest ich rola w całym systemie zarządzania ciągłością działania. Szkolenia mogą być podzielone na ogólne – skierowane do wszystkich pracowników, także tych, którzy nie uczestniczą w odtwarzaniu procesów krytycznych (mogą obejmować podstawowe zagadnienia BCMS) oraz specjalistyczne – skierowane do członków struktury zarządzania kryzysowego i zespołów awaryjnych (powinny obejmować zagadnienia specyficzne do pełnionej funkcji w ramach planów ciągłości działania). Szkolenia powinny być organizowane cyklicznie, m.in. w formie seminariów, instruktażu oraz ćwiczeń praktycznych, jak również metodą e-learningową z obowiązkiem odbycia testu sprawdzającego przyswojoną wiedzę.

5. KOLEJNYM, ALE OPCJONALNYM ETAPEM W TRAKCIE WDRAŻANIA BCMS JEST WYBÓR JEDNOSTKI CERTYFIKUJĄCEJ ORAZ WYKONANIE AUDYTU CERTYFIKUJĄCEGO.

Funkcja audytu programu zarządzania ciągłością polega na porównaniu zgodności zdefiniowanej Polityki Ciągłości Działania, standardów i procedur ze stanem faktycznym, wykryciu ewentualnych luk w ich realizacji oraz wydaniu rekomendacji korygujących.

6. DOBRĄ PRAKTYKĄ JEST RÓWNIEŻ CYKLICZNA OCENA DOJRZAŁOŚCI BCMS.

Jedną z metod oceny dojrzałości BCMS jest opracowana przez amerykańską firmę Vityal Corporation Inc. Business Continuity Maturity Model (BCMM). Metoda zakłada, że organizacja stopniowo osiąga coraz wyższe poziomy dojrzałości, wprowadzając trwale umocowane i systematycznie doskonalone:

- struktury organizacyjne,
- role, zakresy odpowiedzialności, kompetencje i uprawnienia osób związanych z BCMS,
- zasady postępowania,
- świadomość BCMS wśród kierownictwa i pracowników.

SKALA OCENY JEST 6-STOPNIOWA:

- **POZIOM 1.** – Problematyka ciągłości działania nie jest postrzegana przez najwyższe kierownictwo jako znacząca i wymagająca centralnego kierowania. Zajmują się tym poszczególne jednostki organizacyjne według własnego rozeznania i w stopniu, które same uznają za słuszny.
- **POZIOM 2.** – Strategiczne znaczenie problematyki ciągłości działania nie jest dostrzegane przez wszystkie jednostki organizacyjne. W organizacji lub wśród jej doradców jest specjalista, który wspiera prace w obszarze BCM. Najwyższe kierownictwo ma świadomość wagi problemu, ale jeszcze nie nadaje mu odpowiedniego priorytetu.
- **POZIOM 3.** – Najbardziej zainteresowane problematyką jednostki organizacyjne prowadzą wspólne działania. Nie jest to jeszcze BCMS dla całej organizacji. Najwyższe kierownictwo jest świadome działań, sprzyja im, ale jeszcze nie jest zdolne do ustanowienia struktur i zadań w ramach BCMS.
- **POZIOM 4.** – Najwyższe kierownictwo jest świadome strategicznego znaczenia BCMS. Utworzono jednostkę zarządzającą problematyką BCMS. Pracuje się nad zintegrowanymi rozwiązaniami, wspólnymi w całej firmie. Zidentyfikowano krytyczne procesy oraz opracowano plany ich ochrony. Są one cyklicznie aktualizowane i testowane.



- **POZIOM 5.** – Wszystkie jednostki organizacyjne testują BCP oraz na bieżąco wprowadzają działania korygujące. Najwyższe kierownictwo uczestniczy w testach. Opracowano kilkuletni program rozwoju BCMS,
- **POZIOM 6.** – W ramach BCMS dokonuje się oceny BCP jednostek organizacyjnych, a stopień ich przygotowania jest wysoko oceniany. Testuje się współdziałanie jednostek. Wszelkie zmiany w procesach biznesowych, a także w rozwiązaniach BCP są na bieżąco weryfikowane i adaptowane do rozwiązań BCMS.

Doszliśmy do celu, jeśli chodzi o pełne wdrożenie i utrzymanie BCMS w organizacji. Oczywiście w dużych organizacjach, które decydują się na wdrożenie systemu ciągłości działania w wybranych obszarach działalności bądź skupiają w swoich strukturach wiele jednostek organizacyjnych (np. zakładów produkcyjnych), można podejść do wdrożenia wieloetapowo, tworząc przy pierwszym wdrożeniu swego rodzaju framework. Takie ramy wdrożeniowe powinny obejmować:

- metodykę opisującą proces wdrożenia na bazie zrealizowanych działań,
- szablony i wzory dokumentów wykorzystywanych na potrzeby wdrożenia (np. szablon macierzy BCM, szablony macierzy analizy ryzyka, analizy BIA, wzory planów BCP itp.),
- przykładowe produkty na bazie zrealizowanych działań.

Kluczowe jednak będzie opracowanie planu prac niezbędnych do wykonania w celu wdrożenia BCM w kolejnych obszarach czy jednostkach organizacyjnych oraz założeń realizacyjnych, a także przeprowadzenie warsztatu strategicznego z właścicielem projektu po stronie jednostki dominującej w celu podsumowania zrealizowanych prac w ramach wdrożenia w obszarze pilotażowym i przedstawienia propozycji dalszych działań.

Mam nadzieję, że cały cykl artykułów poświęconych metodyce wdrażania systemu zarządzania ciągłością działania okaże się pomocny i wielu menedżerów skorzysta z przedstawionych krok po kroku zasad realizacji. 🕒



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 globalnym koncernie chemicznym CIECH.

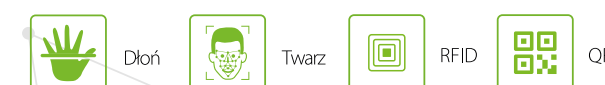
Działaj bezdotykowo, bądź gotowy na nowy standard

Alternatywne rozwiązanie o szerokim zastosowaniu

Urządzenia serii **ProFace X** i **SpeedFace-V5L** z zaawansowaną bezdotykową techniką weryfikacji dłoni i twarzy, z pomiarem temperatury i funkcją wykrywania maski do zastosowań w kontroli dostępu i rejestracji czasu pracy.

Seria ProFace X i SpeedFace-V5L

Weryfikacja z wykorzystaniem funkcji rozpoznawania twarzy i dłoni, z wbudowanymi czytnikami RFID i kodu QR.



Bezdotykowe rozwiązania do kontroli przejść oparte na urządzeniach serii **ProFace X** i **SpeedFace-V5L**

Nieprecyzyjne Warunki Techniczne

Czy to rzeczywiście przeszkoda w procesie sprawnego projektowania?

Wiele osób uważa, że brak precyzyjności zapisów Warunków Technicznych, zamieszczonych w Rozporządzeniu Ministra Infrastruktury z 12 kwietnia 2002 r. w sprawie warunków technicznych, jakim powinny odpowiadać budynki i ich usytuowanie, ostatnia aktualizacja z 14.02.2022, jest poważną przeszkodą w sprawnym, optymalnym projektowaniu.



Michał Zalewski

Do niedawna też tak uważałem, jednak doświadczenia, które nabyłem w ostatnich latach, skłoniły mnie do zmiany stanowiska. Jeżeli we wspomnianym dokumencie, który jest oficjalną wytyczną dla projektantów, jakaś kwestia nie jest precyzyjnie określona i – co więcej – w innych ważnych wytycznych (odpowiednie normy, rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie ochrony przeciwpożarowej) projektant również nie znajduje gotowych zasad projektowania jakiejś kwestii, to nie oznacza niejasności, a wręcz odwrotnie – jest bezspornym stanowiskiem, że kwestia ta jest wyłączną prerogatywą projektanta. Teza kontrowersyjna, mam tego świadomość, ale czy na pewno... Zagadnienie to omówię na podstawie kilku przykładów z dziedziny, w której mam największe doświadczenie, czyli systemów bezpieczeństwa pożarowego.

PRZYKŁAD 1. RODZAJ OKABLOWANIA ZASILAJĄCEGO KLAPY ODCINAJĄCE NA WENTYLACJI BYTOWEJ

§ 187 p 5: Przewody i kable elektryczne w obwodach urządzeń alarmu pożaru, oświetlenia awaryjnego i łączności powinny mieć klasę PH* odpowiednią do czasu wymaganego do działania tych urządzeń, zgodnie z wymaganiami.

Projektant przewiduje więc zasilanie do tych klap zespołami kablowymi w odporności PH. Ale czy na pewno tak trzeba? Moim zdaniem nie. Jeżeli siłowniki tych

klap są sterowane przerwą zasilania ze sprężyną zwrotną, czyli do zmiany pozycji tych klap w warunkach pożaru do pozycji bezpiecznej nie jest wymagane dostarczenie energii, to projektant ma prawo zaplanować kable, dobierając jedynie ich przekrój oraz ew. wymogi rozporządzenia CPR lub wytyczne inwestora, ale to odrębna kwestia. W mojej ocenie projektant ma przewidzianą przez WT dowolność.

PRZYKŁAD 2. MONITOROWANIE STANU POŁOŻENIA KLAP ODCINAJĄCYCH WENTYLACJI

§ 268 p. 6: W strefach pożarowych, w których jest wymagana instalacja sygnalizacyjno-alarmowa, przeciwpożarowe klapy odcinające powinny być uruchamiane przez tę instalację, niezależnie od zastosowanego wyzwalacza termicznego.

O monitorowaniu nie ma ani słowa, czyli projektant, projektując mechanicznie monitorowanie przez system SSP, idzie na skróty. Rozwiązanie to należy dopasować do charakteru obiektu. W przypadku niewielkich obiektów, bez systemu zarządzania budynkiem BMS, należy wykorzystać możliwości SSP i włączyć to monitorowanie do systemu jako stan techniczny, ale jedynie jako sygnał techniczny, który nie może wywoływać żadnych algorytmów sterowań. Nie ma potrzeby drukować tych sygnałów w stanie alarmowym oraz zastanowiłbym się nad rejestrowaniem w pamięci zdarzeń.

Co innego duże obiekty wyposażone w system BMS, który wspomaga obsługę w zarządzaniu budynkiem. W takich przypadkach

poprawnym rozwiązaniem jest monitorowanie stanu klap właśnie przez ten system. Przemawia za tym kilka argumentów.

Po pierwsze i najważniejsze, jeżeli jakaś klapa będzie w stanie niewłaściwym, należy w algorytmach automatyki przewidzieć zatrzymanie wentylacji, by ochronić instalację przed zniszczeniem spowodowanym wzrostem ciśnienia na kanałach (dotyczy to dużych systemów o dużych wydajnościach). Po drugie, służby techniczne mają możliwość wprowadzenia dodatkowych automatycznych reakcji systemu BMS: powiadomienie e-mail lub SMS. Te funkcjonalności są znacznie ukoźsze w systemach SSP, a to ułatwi szybką identyfikację usterki i reakcję służb utrzymaniowych.

Po trzecie, systemy BMS mają znacznie większe i znacznie lepiej zarządzalne rejestry zdarzeń, co pozwoli zarchiwizować podobne zdarzenia i odpowiednio je filtrować przy przeglądaniu historii dla sprawnego zarządzania budynkiem.

Podsumowując, projektant ma prawo zdecydować, w którym systemie – SSP czy BMS – odbywa się monitorowanie stanu klap, a także to czy w ogóle będą monitorowane. Ostatniej opcji nie polecam stosować, chociaż formalnie jest taka możliwość.

Na koniec ostatni przykład rozwiązania nieokreślonego w WT, czyli kwestia liczby modułów sterowań do zamykania klap wentylacji bytowej. Czy projektant, projektując osobny moduł dla każdej klapy, przyjmuje optymalne rozwiązanie? Moim zdaniem niekoniecznie. Jeżeli mamy duży i skomplikowany obiekt, przewidzieliśmy monitorowanie położenia klap w systemie BMS, to warto rozważyć grupowe sterowanie zespołami klap znajdującymi się w pobliżu.

Jeżeli formalne wytyczne nie precyzują rozwiązań, to w gestii projektanta jest dobranie ich tak, by osiągnąć zamierzony efekt, czyli uzyskać efektywną i bezpieczną eksploatację budynku przy minimalnie skomplikowanych rozwiązaniach. Należy jednak rozważyć wiele kwestii i dokładnie sprawdzić przyjęte założenia. Można np. przeoczyć funkcję klapy jako klapy na instalacji oddymiającej lub też wynikającą ze scenariusza pożarowego funkcję klapy odcinającej z opóźnieniem, np. w systemie wentylacji transformatorów. Dlatego zachęcam wszystkich projektantów do analizowania wytycznych i w miejscach, gdzie otrzymali dowolność stosowania rozwiązań, do korzystania z tej sposobności. Oznacza to dla projektanta więcej pracy, więcej działań koordynacyjnych z pozostałymi branżami, ale nie ma innej drogi.

Często napotykam argumentację, że jeżeli Warunki Techniczne czegoś nie precyzują, to służby odbiorowe mogą zakwestionować takie rozwiązania. Uważam, że to niewłaściwe podejście. Jeżeli projektant z dbałością o szczegóły techniczne rozwiąże określoną kwestię, która nie jest szczegółowo zapisana w wytycznych WT, nie można tego zakwestionować. Ważne jest natomiast, by być precyzyjnym, a do zagadnienia można również odnieść się w części opisowej projektu, zapisać, że rozważono różne rozwiązania, ale przyjęto określone, wraz z argumentacją, która przesądziła o wyborze. **Kiedy nieprecyzyjne zapisy WT spotkają się z nieprecyzyjnymi zapisami w projekcie, wtedy pojawia się problem.**

Kolejną kwestią jest doprecyzowanie, w którym projekcie należy zawierać opisy rozwiązań. Od 19 września 2021 r. zmieniły się zasady opracowywania dokumentacji wymaganej przez urzędy przy wydawaniu decyzji. Istnieje projekt architektoniczno-budowlany, który składamy w celu uzyskania pozwolenia na budowę, oraz projekt techniczny, który z kolei składamy przy wniosku o uzyskanie pozwolenia na użytkowanie albo zawiadomieniu o zakończeniu robót wraz z oświadczeniem, że ten projekt jest zgodny z projektem architektoniczno-budowlanym.

I tu jest pułapka – jeżeli projekt architektoniczno-budowlany nie określa precyzyjnie rozwiązań, to sam projekt techniczny nie jest wystarczający. Stąd prosty wniosek, że projekt architektoniczno-budowlany musi być na tyle precyzyjny, by projekt techniczny mógł zostać określony jako w pełni zgodny z projektem architektoniczno-budowlanym i być tylko jego rozszerzeniem. Nie oznacza to jednak konieczności zawierania w projekcie architektoniczno-budowlanym całości (w naszym przypadku) systemu SSP, a jedynie precyzyjne opisanie założeń technicznych, które zostaną szczegółowo wskazane w projekcie technicznym. Jeżeli dokumenty będą w ten sposób przygotowane, nie należy się spodziewać problemów z akceptacją rozwiązań podczas czynności kontrolnych.

Opisywany przeze mnie problem jest uniwersalny, wielobranżowy. Zasady, które omawiam, powinni rozważyć wszyscy projektanci, a przytoczone przykłady służą jedynie opisaniu toku mojego rozumowania w tej kwestii.

Dowolność, o której kilkakrotnie wspominałem, nie oznacza oczywiście tzw. wolnoamerykanki – odpowiedzialna dowolność to techniczna analiza problemu, rozważenie wielu opcji, techniczne i precyzyjne przeanalizowanie „za” i „przeciw” oraz wybranie najlepszej, co niekoniecznie może oznaczać najtańszą, najbardziej oczywistą lub zgodną z zasadą „od 15 lat tak projektuję i zawsze było OK”. Ta dowolność nie może stać w sprzeczności z warunkami stosowania urządzeń i materiałów określonymi przez producentów w dokumentach DTR, instrukcjach montażowych i deklaracjach zgodności. A takie próby też miałem okazję opiniować. Jedną z najbardziej kuriozalnych była próba wykorzystania czujek liniowych dymu do kontroli strzałki ugięcia konstrukcji stalowej hali... Na szczęście udało się zatrzymać zapędy projektanta i inwestor nie zmarnował kilkuset tysięcy złotych. Wspomniana dowolność to praca i odpowiedzialność, a wsparta techniczną argumentacją oznacza sukces projektu. To niełatwe zadanie, ale ambitny projektant nie powinien obawiać się o rezultaty swojej pracy.

Mam nadzieję, że tym artykułem pobudzę czytelnika do samodzielnego przeanalizowania poruszanych kwestii. Zachęcam do polemiki na ten temat, chętnie podejmę dyskusję z dochoowaniem merytoryczności.

Na koniec chciałbym pozdrowić studentów Politechniki Łódzkiej z Wydziału Architektury i podziękować za zainteresowanie moimi artykułami, a przede wszystkim pogratulować profesjonalnego podejścia do problematyki projektowania jako odpowiedzialnego zadania kształtującego otaczający nas świat. 🍷



MICHAŁ ZALEWSKI

Absolwent Politechniki Gdańskiej i studiów podyplomowych Zarządzania Projektami Politechniki Warszawskiej. W branży od 25 lat, od 13 lat niezależny konsultant, inżynier uruchomieniowy.



Instrukcja Bezpieczeństwa Pożarowego

element systemu zarządzania kryzysowego



Łukasz Stępień

Komu jest potrzebna Instrukcja Bezpieczeństwa Pożarowego? Odpowiedź wydaje się oczywista. Wszystkim podmiotom wymienionym w rozporządzeniu w sprawie ochrony ppoż. budynków, innych obiektów budowlanych i terenów¹. I na tym można by poprzestać, gdyby nie to, że idąc za literą prawa, często pomijamy jego ducha i zapominamy, że może to być całkiem przydatny dokument.

W obiegowej opinii Instrukcja Bezpieczeństwa Pożarowego (IBP) jest przeznaczona dla jednostek straży pożarnej. Ma to być dokument ułatwiający kierującemu działaniami ratowniczymi ich realizację na miejscu zdarzenia. Od strony prawnej jest jednak jasno wskazane, że realną wartość dla jednostek ratowniczych stanowi tylko część dokumentu. O ile IBP powinna się znajdować w miejscach dostępnych dla ekip ratowniczych, o tyle informacje nt. warunków ochrony ppoż. i rzuty graficzne muszą być przechowywane w sposób, który powinien zapewnić możliwość ich natychmiastowego wykorzystania na potrzeby prowadzenia działań ratowniczych. Ponadto obiekty, które muszą być obowiązkowo wyposażone w systemy sygnalizacji pożarowej, takie jak:

- centra handlowe,
- duże teatry i kina,
- wysokie i wysokościowe budynki użyteczności publicznej,
- stacje metra i kolei podziemnych,
- zabytki i biblioteki o znaczeniu narodowym,

są zobowiązane przekazać właściwemu komendantowi powiatowemu (miejskiemu) straży pożarnej informacje nt. warunków pożarowych obiektu, łącznie z rzutami

graficznymi, w celu ich wykorzystania na potrzeby planowania i organizacji działań ratowniczych. Zarówno pod względem prawnym, jak i faktycznie realną wartość dla działań ratowniczo-gaśniczych mają tylko dwie części całego dokumentu. W praktyce wykorzystanie nawet tych informacji bywa mocno utrudnione. Główne problemy to aktualność i jakość opracowania dokumentu. Rozporządzenie nakłada obowiązek aktualizacji IBP po każdej zmianie sposobu użytkowania obiektu lub procesu technologicznego, która wpływa na zmianę warunków pożarowych, np. przebudowa skutkująca zmianą dróg ewakuacyjnych albo zwiększenie ilości cieczy łatwopalnych znajdujących się w obiekcie (choćby w sklepach budowlanych). Każda taka zmiana powinna być odnotowana/zaktualizowana w dokumencie oraz w dokumentacji przekazanej do odpowiedniej komendy. Doświadczenie pokazuje, że „rzeczywistość prawna” często rozmija się z „rzeczywistością faktyczną”. Drugim poważnym problemem jest jakość wykonania dokumentu. Ustawa zawiera informację, CO powinno się znaleźć w IBP, natomiast nie ma wytycznych, JAK powinno to wyglądać. Niestety, również Komenda Główna PSP do tej pory nie wydała żadnych rekomendacji z tego zakresu². W efekcie każde opracowanie wygląda inaczej. Częstym problemem jest szum informacyjny – zbyt duża ilość nieistotnych informacji, np. rok powstania zakładu albo historia rozwoju organizacji w Polsce. Dokument sztucznie „pęcznieje”, nie przekładając się w żaden sposób na jego wartość. Problemy z jakością wpływają też na czytelność rzutów graficznych. Większość autorów IBP korzysta z rzutów będących częścią projektu budowlanego. Nie ma w tym nic nagannego, jeśli na planach będą znajdować się tylko informacje wymagane w rozporządzeniu. Gorzej, gdy na tych samych grafikach pojawiają się też plany instalacji wodno-kanalizacyjnej, elektrycznej albo wymiary wszystkich pomieszczeń, w dodatku na czarno-białym rzucie. Kierujący działaniami ratowniczymi, widząc tak opracowany dokument, będzie zapewne wołał przeprowadzić „rozpoznanie bojem”, niż próbować zrozumieć, co autor instrukcji bezpieczeństwa pożarowego miał na myśli. W efekcie traci się ogromną szansę na sprawniejsze przeprowadzenie akcji ratowniczo-gaśniczej i szybsze wyeliminowanie zagrożenia. A na jak najszybszym usunięciu zagrożenia powinno szczególnie zależeć zarządzającemu obiektem. I to właśnie on może najpełniej wykorzystać możliwości, jakie daje dobrze opracowana i wdrożona instrukcja bezpieczeństwa pożarowego. Podstawą do opracowania rozdziału dotyczącego warunków ochrony ppoż. jest najczęściej projekt budowlany. Zawiera on warunki ochrony ppoż. ze wszystkimi informacjami nt. budynku i charakterystyki zagrożeń pożarowych³. Właściwie przygotowana IBP musi uwzględniać nie tylko dane projektowe, ale także stan faktyczny wynikający z realizowanych procesów technologicznych, magazynowanych substancji i aktualnych warunków technicznych obiektu. Taką ocenę może wykonać tylko osoba mająca odpowiednie kwalifikacje, najczęściej na podstawie wizji lokalnej, analizy dokumentacji i rozmów z pracownikami. Dobrze przeprowadzony proces aktualizacji IBP pozwala zidentyfikować potencjalne zagrożenia i ryzyka, których użytkownicy obiektu mogą nie być świadomi. Z tego też powodu, nawet jeśli w obiekcie nie doszło do zmian warunków pożarowych, instrukcja podlega konieczności aktualizacji (czyt. weryfikacji) co dwa lata. Jeżeli w obiekcie przewidziano możliwość prowadzenia prac pożarowo niebezpiecznych, to w dokumencie tym muszą się znaleźć informacje na temat zabezpieczenia takich prac. Czyli po raz

² Mimo że obowiązek opracowywania Instrukcji Bezpieczeństwa Pożarowego istnieje już od blisko 30 lat, został wprowadzony rozporządzeniem Ministra Spraw Wewnętrznych z 3 listopada 1992 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów.
³ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 2 grudnia 2015 r. w sprawie uzgadniania projektu budowlanego pod względem ochrony przeciwpożarowej (Dz.U. 2015 poz. 2117).

¹ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 7 czerwca 2010 r. w sprawie ochrony przeciwpożarowej budynków, innych obiektów budowlanych i terenów (Dz.U. 2010 nr 109 poz. 719).



kolejny angażujemy specjalistę z zakresu bezpieczeństwa pożarowego, którego zadaniem jest wsparcie organizacji i określenie sposobów zabezpieczenia prac pożarowo niebezpiecznych, aby ograniczyć ryzyko wystąpienia zagrożenia pożarowego, a w efekcie wystąpienia zagrożenia życia i zdrowia ludzi oraz strat w mieniu.

Opracowanie i wdrożenie IBP mogą też być podstawą do zbudowania systemu zarządzania incydentami w organizacji. Ochrona ppoż. w rozumieniu ustawowym polega na realizacji przedsięwzięć mających na celu ochronę życia, zdrowia, mienia lub środowiska przed pożarem, klęską żywiołową lub innym miejscowym zagrożeniem⁴, a w IBP muszą się znaleźć informacje nt. sposobu postępowania na wypadek pożaru i innego zagrożenia miejscowego, warunki i organizacja ewakuacji oraz zadania i obowiązki w zakresie ochrony ppoż.

Wystarczy, że zrealizujemy również wymóg prawny dotyczący zapoznania stałych użytkowników obiektu z dokumentem i wtedy już mamy:

- użytkowników, którzy znają wymogi bezpieczeństwa pożarowego (działania profilaktyczne),
- użytkowników obiektu, którzy wiedzą, jak postępować podczas zagrożenia (działania reaktywne),
- użytkowników obiektu, którzy potrafią bezpiecznie opuścić obiekt,
- zdefiniowane role i odpowiedzialności w zakresie postępowania w przypadku wystąpienia zagrożenia,

spełniając jednocześnie wymogi polskiego prawa, bez tworzenia dodatkowych procedur, dokumentów i regulacji.

Warto wspomnieć też o rzutach graficznych, które będą przydatne strażom pożarnej i jednostkom policji prowadzącym przeszukiwanie obiektu w związku z „telefonem o bombie”. Instrukcja Bezpieczeń-

⁴ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 7 czerwca 2010 r. Dz.U. 2010 nr 109 poz. 719).



stwa Pożarowego jest też jednym z ważniejszych dokumentów w ochronie fizycznej. Ochrona osób obejmuje działania mające na celu zapewnienie bezpieczeństwa życia i zdrowia, natomiast ochrona mienia to działania zapobiegające przestępstwom i wykroczeniom przeciwko mieniu oraz przeciwdziałające powstawaniu szkody wynikającej z tych zdarzeń⁵. Łamanie przepisów pożarowych natomiast może nosić znamiona zarówno wykroczeń (art. 82 Kodeksu Wykroczeń – spowodowanie niebezpieczeństwa pożaru), jak i przestępstw (art. 163 Kodeksu Karnego – spowodowanie katastrofy).

Ponadto rzuty graficzne będące załącznikiem do IBP są doskonałą bazą do opracowywania map patrolowych. Zespół ochrony jest często pierwszym źródłem informacji dla jednostek straży pożarnej, które przyjadą na miejsce zdarzenia – pracownik ochrony potrafiący wskazać konkretne obszary i instalacje na mapie jest ogromnym wsparciem w trakcie działań ratowniczych. Zaangażowanie zespołu ochrony w obszary bezpieczeństwa pożarowego znajduje też odzwierciedlenie w międzynarodowych standardach, takich jak *NFPA 601: Standard for Security Services in Fire Loss Prevention* (Standard dla służb ochrony w zakresie przeciwdziałania stratom związanym z pożarami) i *BSI 16000 Security Management – Strategic and operational guidelines* (Zarządzanie ochroną fizyczną – wytyczne strategiczne i operacyjne). Ustawodawca zezwolił również, aby w obiektach służących obronności państwa oraz zlokalizowanych na terenach zakładów karnych i aresztów IBP stanowiła część planu ochrony lub działań ratowniczych.

Instrukcja Bezpieczeństwa Pożarowego może być też skryptem ułatwiającym codzienne administrowanie obiektem. Zawiera informacje nt. sprzętu pożarowego, jego umiejscowienia i zasad poddawania przeglądowi technicznemu. Podział na strefy pożarowe i kierunki dróg ewakuacyjnych pozwalają na szybką weryfikację, czy „wywiercenie dziury w tej ścianie” albo „przestawienie maszyny w inne miejsce” będzie wymagało dodatkowych zmian, np. zastosowania przepustów ognioochronnych czy reorganizacji oznaczeń dróg ewakuacyjnych. To sporo możliwości jak na jeden, dobrze opracowany i wdrożony dokument.

OBIEKTY WYMAGAJĄCE OPRACOWANIA INSTRUKCJI BEZPIECZEŃSTWA POŻAROWEGO

Opracowanie i wdrożenie IBP jest wymagane w obiektach lub odrębnych strefach pożarowych, które są przeznaczone do wykonywania funkcji:

- 1) użyteczności publicznej,
- 2) zamieszkania zbiorowego,
- 3) produkcyjnych,
- 4) magazynowych,
- 5) inwentarskich.

Odstępstwo od wymogu opracowania IBP dotyczy obiektów, których:

- 1) kubatura brutto budynku lub części stanowiącej odrębną strefę pożarową nie przekracza 1000 m³ i nie występuje strefa zagrożenia wybuchem;
- 2) kubatura brutto budynku inwentarskiego nie przekracza 1500 m³ i nie występuje strefa zagrożenia wybuchem;
- 3) powierzchnia strefy pożarowej innej niż budynek nie przekracza 1000 m² i nie występuje strefa zagrożenia wybuchem. 

⁵ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 7 czerwca 2010 r. (Dz.U. 2010 nr 109 poz. 719).



ŁUKASZ STĘPIEŃ

Specjalista z zakresu bezpieczeństwa i zarządzania kryzysowego. Członek Krajowego Stowarzyszenia Ochrony Przeciwożarowej w USA.



KOMPLEKSOWE SYSTEMY SYGNALIZACJI POŻAROWEJ *dla profesjonalistów*

- PRODUKCJA
- SERWIS
- SZKOLENIA
- WSPARCIE TECHNICZNE I PROJEKTOWE

Bezpieczeństwo i ochrona przeciwpożarowa budynków

Ewakuacja w technologii VR

Małgorzata Rejman

Bezpieczeństwo pożarowe budynków to jeden z obszarów ochrony, którego wszyscy jesteśmy beneficjentami. Jako użytkownicy biur, budynków mieszkalnych, obiektów handlowych i sportowych oraz innych miejsc użyteczności publicznej każdego dnia potencjalnie możemy uczestniczyć w ewakuacji. Aby była skuteczna, wymaga cyklicznych szkoleń zarówno ze strony osób odpowiedzialnych za jej przeprowadzenie, jak i naszej. Z pomocą przychodzą rozwiązania techniczne wspomagające proces ewakuacji.



Ryzyka związane z zagrożeniem pożarowym i zapobieganie im to priorytet systemów bezpieczeństwa. Statystyki wskazują, że o ile ogólna liczba pożarów spada, o tyle z roku na rok wzrasta liczba pożarów w budynkach użyteczności publicznej i mieszkalnych. Rośnie liczba przeprowadzonych ewakuacji, ale i ofiar śmiertelnych.

Rodzaj zdarzenia	2020 r.	2021 r.
Ofiary śmiertelne w wyniku pożarów	486	516
Ranni w wyniku pożarów	2594	2444
Pożary ogółem	128 754	106 447
Pożary w obiektach użyteczności publicznej	2010	2234
Pożary w obiektach mieszkalnych	31496	33860
Ewakuacja w obiektach użyteczności publicznej i obiektach mieszkalnych z powodu pożaru i miejscowych zagrożeń	3215	3307

„Dane statystyczne KG PSP” [źródło: KG PSP, 02.11.2022]

Przebywając w budynkach, możemy być pewni, że w myśl art. 3 ust. 1 i 2 ustawy o ochronie ppoż. ...osoba fizyczna, osoba prawna, organizacja lub instytucja korzystające ze środowiska, budynku, obiektu lub terenu* zabezpieczyła obiekt przed zagrożeniem pożarowym. Statystyki wskazują jednak, że głównymi powodami pożarów w budynkach są nieostrożne obchodzenie się z ogniem, wady urządzeń i instalacji oraz umyślne podpalenia. Powodem może być też brak regularnych przeglądów instalacji i urządzeń.

Wszystkie statystycznie najczęstsze powody pożarów to czynniki niezależne od usług bezpieczeństwa pożarowego, dlatego tak istotne są procedury na wypadek wystąpienia ognia i działania usprawniające proces ewakuacji.

SECURITAS SMARTIN JAKO WSPARCIE PROCESU EWAKUACJI

Jednym z narzędzi wykorzystywanych przez Securitas do wspierania procesu ewakuacji jest system smartIN. Rozwiązanie, którego głównym zadaniem jest usprawnienie

* Ustawa z 24 sierpnia 1991 r. o ochronie przeciwpożarowej (Dz.U.2022.2057)

POWÓD POŻARU

	Liczba pożarów ogółem		Nieostrożność osób dorosłych (NOD) przy posługiwaniu się ogniem otwartym, w tym papierosy, zapalki		Wady urządzeń i instalacji elektrycznych, w szczególności przewody, osprzęt oświetlenia, odbiorniki bez urządzeń grzewczych		Podpalenia (umyślne), w tym akty terroru	
	2020 r.	2021 r.	2020 r.	2021 r.	2020 r.	2021 r.	2020 r.	2021 r.
Rodzaj obiektu/rok	2020 r.	2021 r.	2020 r.	2021 r.	2020 r.	2021 r.	2020 r.	2021 r.
Obiekty użyteczności publicznej	2009	2234	273	261	533	529	190	223
Obiekty mieszkalne	31490	33860	3074	2981	2149	2196	1546	1391

„Dane statystyczne KG PSP [źródło: KG PSP, 02.11.2022]”

procesu awizacji gości, automatycznie wpisuje osoby przebywające w budynku na listę ewakuacyjną i wyrejestrowuje po jego opuszczeniu. Aktualizacja w czasie rzeczywistym stanowi znaczące wsparcie dla koordynatorów ewakuacji. W razie zagrożenia pożarowego dysponujemy imienną listą i numerami do wszystkich osób w budynku. Większość dużych firm nie prowadzi rejestracji pracowników przebywających w biurze, a system pracy zdalnej zdecydowanie pogłębił tę sytuację. Bez systemowych rozwiązań trudno zweryfikować, czy wszyscy opuścili budynek.

BEZPIECZNA EWAKUACJA

Przepisy o ochronie ppoż. nakazują, aby właściciel lub zarządca obiektu przeznaczonego dla ponad 50 osób, będących jego stałymi użytkownikami, (...) powinien co najmniej raz na dwa lata przeprowadzać praktyczne sprawdzenie organizacji oraz warunków ewakuacji z całego obiektu. Próba ewakuacji ma na celu zapoznać wszystkie osoby z drogami i znakami ewakuacyjnymi, z miejscami zbiórek i przechowywania gaśnic. Niestety w biurach ewakuacje są zazwyczaj zapowiadane i często pracownicy chcący ich uniknąć wybierają tego dnia pracę w trybie home office.

Jak wygląda próbna ewakuacja? Ćwiczenia przeprowadza się w warunkach bezstresowych, jest zapowiedziana, wszyscy bez problemu wychodzą, korzystając z dróg ewakuacyjnych. Zupełnie inaczej wygląda to w sytuacji realnego zagrożenia – pojawia się stres, a znalezienie bezpiecznego wyjścia pogłębiają zadymienie i brak oświetlenia. Gdy ewakuujemy się z miejsca, w którym jesteśmy po raz pierwszy i nie znamy drogi ewakuacyjnej, strach często przeradza się w panikę.

Badania wskazują, że w sytuacji zagrożenia w nieznanym miejscu tylko 38% osób widzi oznakowanie ewakuacyjne! W ekstremalnych warunkach ogień może odciąć nam drogę wyjścia i będziemy musieli ewakuować się, skacząc z budynku. Czy taki scenariusz można przeciwić? Czy da się próbnie i bezpiecznie ewakuować się z płonącego bu-



W sytuacji zagrożenia w nieznanym miejscu tylko

38% osób

widzi oznakowanie ewakuacyjne!

dynku? W praktyce jest to niemożliwe, ponieważ przepisy jednoznacznie zabraniają skoków ćwiczeniowych na skokochrony i ratownicze poduszki pneumatyczne. I tu przychodzi z pomocą wirtualna rzeczywistość – VR (Virtual Reality).

EWAKUACJA W TECHNOLOGII VR

Szansą, aby doświadczyć skoku z płonącego wieżowca w bezpiecznych warunkach i poczuć realną adrenalinę, jest wirtualna rzeczywistość. Securitas przeprowadza próbne ewakuacje, wykorzystując technologię VR. Szkolenie pozwala na wierne odwzorowanie pożaru i konieczności ewakuacji z wyższego piętra budynku. Uczestnik podczas szkolenia doświadcza realnych sytuacji kryzysowych, jego jedyną drogą ucieczki z płonącego budynku jest skok na skokochron lub przejście dwóch metrów po kładce do kosza strażackiego. Emocje są bardzo naturalne. Uczestnik widzi płonącą przestrzeń za sobą, musi wybić szybę, stanąć na krawędzi okna i skoczyć. W dole widać nadjeżdżającą straż i rozkładany skokochron, słysząc komunikaty strażaków. Aplikacja reaguje na brak reakcji uczestnika, co wzmacnia realność sytuacji. O ile patrząc na płonące za nami biuro jesteśmy świadomi, że to rzeczywistość wirtualna, o tyle sam skok, podjęcie decyzji i emocje są zbliżone do realnych warunków.

WIRTUALNIE CZY JEDNAK TRADYCYJNIE?

Czy szkolenie VR może zastąpić tradycyjną próbną ewakuację? Nie! Ewakuacja próbna przeprowadzona w budynku, w którym często przebywamy, pozwala osobom na poznanie dróg ewakuacji i miejsc przechowywania gaśnic. Jest szansą na praktyczną weryfikację i aktualizację istniejących procedur, sprawdzenie systemów, identyfikację słabych punktów i ich poprawę. To także szansa sprawdzenia reakcji pracowników i koordynacji akcji przez wyznaczone osoby. Regularnie przeprowadzana ewakuacja kształtuje i utrwala prawidłowe nawyki.

Szkolenie VR daje niepowtarzalną okazję doświadczenia sytuacji niemożliwych do odtworzenia w warunkach innych niż wirtualne. Dodatkową jego wartością są towarzyszące emocje i strach. Nie wszyscy się na ten wirtualny skok (a wystarczy zrobić mały krok) decydują, co tylko dowodzi konieczności przeprowadzania takich szkoleń i przełamywania bariery strachu. W sytuacji zagrożenia ważna jest każda minuta. Czasem krótkie chwile decydują o naszym życiu.

Szkolenie ppoż. w rzeczywistości VR zaprezentowaliśmy naszym klientom podczas Security BootCamp 2022. Planujemy również je powtórzyć podczas kolejnych wydarzeń organizowanych przez a&s Polska. 📍

SECURITAS POLSKA

Postępu 6
02-676 Warszawa
securitas@securitas.pl



IX edycja Ogólnopolskich Dni Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy Podsumowanie

Marta Nowak

Prawie 600 osób wzięło udział w Ogólnopolskich Dniach Zintegrowanych Systemów Bezpieczeństwa Pożarowego – Schrack Seconet i Partnerzy, które odbyły się 12 – 13 października 2022 r. w Hotelu Windsor w Jachrance. Podczas tego wyjątkowego wydarzenia edukacyjnego organizatorzy gościli przedstawicieli branży systemów zabezpieczeń: inwestorów, generalnych wykonawców, rzeczoznawców, projektantów, instalatorów oraz pozostałych uczestników rynku.

Podczas dwóch dni spotkań z najlepszymi ekspertami w branży słuchacze zapoznali się z najnowszymi wytycznymi dotyczącymi projektowania, instalowania i użytkowania takich systemów, jak: sygnalizacji pożarowej, sterowania gaszeniem, telewizji dozorowej, kontroli dostępu, detekcji gazów, integracji urządzeń przeciwpożarowych (SIUP), DSO i innymi instalacjami technicznymi obiektu. Działanie tych systemów pokazano na przykładzie trzech studiów przypadku. Przypadek pierwszy dotyczył bezpieczeństwa obiektu budowlanego oraz przebywających w nim ludzi. Omówiono detekcję gazu w garażach podziemnych, pokazano interakcję między systemem dozoru wizyjnego i systemu kontroli dostępu podczas bieżącej eksploatacji i stanu zagrożenia oraz scenariusze działania i możliwości współpracy DSO z SSP, SIUP.

W drugim studium przypadku omówiono zabezpieczenie obiektu budowlanego podczas przebudowy lub remontu z wykorzystaniem mobilnego systemu sygnalizacji pożarowej oraz ochronę przeciwpożarową parkingu ze stanowiskami dla samochodów elektrycznych. Trzeci przypadek dotyczył bezpieczeństwa infrastruktury IT, sterowania stałymi urządzeniami gaśniczymi (SUG) w serwerowni oraz przebiegu scenariusza pożarowego w przypadku pożaru w obiekcie biurowym. Wsparcie merytoryczne podczas tegorocznej edycji szkolenia zapewnili Partnerzy Merytoryczni: **Stowarzyszenie Inżynierów i Techników Pożarnictwa – Izba Rzeczoznawców, Polska Izba Systemów Alarmowych, Instytut Bezpieczeństwa Pożarowego NODEX, PROTECT Tadeusz Cisek i Wspólnicy, PZU LAB**. Przedstawiciele tych instytucji wzięli udział w sesji zarówno wykładowej, jak i warsztatowej. Dodatkowo w sesji wykładowej swój referat wygłosił ekspert reprezentujący **Centrum Naukowo-Badawcze Ochrony Przeciwpożarowej im. Józefa Tuliszkowskiego – Państwowy Instytut Badawczy**. Patronat specjalny nad wydarzeniem objął **Komitet Bezpieczeństwa Gospodarczej Infrastruktury Krytycznej Krajowej Izby Gospodarczej**.

Szkolenia odbywały się równolegle w 13 salach. Warsztaty kończące każdy dzień miały charakter sesji pytań i odpowiedzi oraz wymiany poglądów. Były to otwarte panele dyskusyjne, podczas których specjaliści z różnych dziedzin mieli jeszcze więcej możliwości uzyskania odpowiedzi na nurtujące ich kwestie z zakresu prawa, techniki oraz praktyki wykonawczej i użytkowania systemów bezpieczeństwa w obiektach komercyjnych, przemysłowych, użyteczności publicznej, muzeach itp. Zainteresowanie uczestników potwierdziło sensowność powrotu do zorganizowania spotkania po dwóch latach przerwy spowodowanej pandemią. Wielokrotnie wyrażano opinię o konieczności częstszych spotkań merytorycznych i edukacyjnych w branży systemów zabezpieczeń. Schrack Seconet, jako producent i dostawca zaawansowanych technologicznie rozwiązań, stara się na bieżąco spełniać oczekiwania ryn-





Kongres Safe Place – sukces po raz piąty

Czasopismo „a&s Polska” było partnerem medialnym V jubileuszowej edycji Ogólnopolskiego Kongresu Naukowo-Technicznego SAFE PLACE 2022, w tym roku zorganizowanego w hotelu Kuźnia Napoleońska w Paprotni k. Warszawy. Blisko 400 uczestników reprezentowało ośrodki naukowe i eksperckie, instytucje bezpieczeństwa narodowego, obiekty użyteczności publicznej i infrastruktury krytycznej oraz sektor ochrony i zabezpieczeń technicznych. Sześciu przekrój grup uczestniczących w Kongresie przyczynił się do pogłębienia wiedzy i nawiązania nowych kontaktów.



Trzy październikowe dni upłynęły pod znakiem merytorycznych prelekcji, paneli dyskusyjnych i debat eksperckich, a także prezentacji nowoczesnych rozwiązań z zakresu bezpieczeństwa antyterrorystycznego. Naukowcy i praktycy z obszaru bezpieczeństwa przedstawili swoje doświadczenia i wyniki interesujących ba-

dań, przyczyniając się do zwiększenia świadomości zagrożeń wśród zarządzających bezpieczeństwem w obiektach użyteczności publicznej. Piąta edycja wyróżniała się większym naciskiem połączonym na omówienie aspektów praktycznych z obszaru rozwiązań technicznych prezentowanych przez partnerów wydarzenia.

Innowacyjną formułą przyjął drugi dzień Kongresu. Oprócz tradycyjnych sesji plenarnych i paneli eksperckich przeprowadzono warsztaty praktyczne, łączące aspekty teoretyczne i praktyczne. Każdy z uczestników wziął udział w czterech sesjach obejmujących tematykę udzielanie pierwszej pomocy, reagowanie

na zamachy oraz możliwość wykorzystania rozwiązań technicznych w ochronie wewnętrznej i zewnętrznej obiektów. Przyszłoroczna odsłona Kongresu, zaplanowana na listopad 2023 r., będzie miała wymiar międzynarodowy, co wzbogaci merytorykę o doświadczenia zagranicznych podmiotów z obszaru bezpieczeństwa. 📍



ku, dlatego każdego roku przygotowuje wiele nowości. Dotyczą one zarówno samej organizacji wydarzenia, sposobów komunikacji z uczestnikami (różnorodne formy przekazu), jak i coraz głębszej, dokładniejszej analizy problemów pojawiających się w trakcie projektowania i realizacji obiektów różnego przeznaczenia.

Współorganizatorami tego niezwykle istotnego w branży przedsięwzięcia edukacyjnego byli następujący producenci i dystrybutorzy: **BELIMO Siłowniki, BKT Elektronika, C-AIM, Fire & Gas Detection Technologies, GAZEX, GEO-KAT, GRAS, InGas, Nedap Security Management, PARTNER.**

Schrack Seconet Polska składa podziękowania wszystkim prelegentom, uczestnikom, przedstawicielom instytucji i uczelni technicznych, patronom merytorycznym i medialnym oraz patronowi specjalnemu. Organizatorzy dziękują także partnerom technologicznym za wieloletnią wspólną pracę nad całokształtem wydarzenia. O planach związanych z kolejną, jubileuszową edycją wydarzenia organizatorzy będą informować na bieżąco. Wszystkie informacje są dostępne na stronie: wydarzenia.schrack-seconet.pl. 📍

SCHRACK SECONET POLSKA

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



R E K L A M A



NIEZAWODNE SYSTEMY SYGNALIZACJI POŻAROWEJ PROTEC

- » Centrale sygnalizacji pożarowej
- » Czujki zasysające
- » Czujki punktowe
- » Liniowe czujki dymu
- » Radiowy system sygnalizacji pożarowej
- » Adresowalne ostrzegacze pożarowe
- » Akcesoria

www.dhpolska.pl

D+H
BUILDING ATMOSPHERE



JESIENNY BOOTCAMP

Piękna pogoda i świetna atmosfera panowała w czasie dwóch dni wrześniowego szkolenia w Wierzbowym Rancho. Uczestnicy mierzyli się w terenie m.in. z zadaniami z wykorzystaniem kodów dostępu i szyfrowanych kart. Poznawali nowe funkcje rozbudowanej platformy security i systemów monitoringu wizyjnego. Sprawdzili też, jak gasi się pożar na żywo i jak działać w trakcie ewakuacji – tym razem już w goglach VR. Partnerami technologicznymi jesiennej edycji Security BootCamp były firmy: Genetec, Geutebrück, Nedap Security Management, Securitas Polska i STid.

Mariusz Kucharski

a&s Polska

Jesienny BootCamp to szkolenie, podczas którego Security Managerowie i szefowie bezpieczeństwa wielu firm i instytucji z całego kraju uczestniczyli w konkurencjach w terenie. Kolejne spotkanie odbędzie się na wiosnę przyszłego roku. Już teraz na nie zapraszamy.

Mariusz Bak

Securitas Polska

Pokazaliśmy naszym gościom m.in. technologię VR, która wchodzi do nas w szybkim tempie. Google VR można wykorzystać do szkoleń pracowników, specjalistów, ekspertów. Również dzisiaj wróciliśmy do czegoś, co może się wydawać podstawą, a tak naprawdę mało kto na co dzień ma styczność z gaszeniem pożaru, walką z ogniem.

Tomasz Nawrat

Genetec

To kolejna edycja BootCampu, na której pokazywaliśmy naszą zunifikowaną platformę Security Center, prezentując przede wszystkim jej nieograniczone możliwości. Tym razem skupiliśmy się na dedykowanych kamerach LPR, które są zaprojektowane przez nas i produkowane w Kanadzie. Pokazywaliśmy na symulacji, jak to wygląda w praktyce, co wzbudziło duże zainteresowanie wszystkich uczestników spotkania.

Jeroen Mollé

Geutebrück

Rozwiązania, które zaprezentowaliśmy, mogą pomóc Security Managerom w ich codziennej pracy. Co ważne, mogą być stosowane w wielu sektorach, a do podglądu i zarządzania można wykorzystywać własne smartfony. Nasza gra wywołała wiele ciekawych dyskusji. Pokazaliśmy rozwiązania funkcjonujące w firmie, których działania nie za naszym pośrednictwem uczestnicy mogli sprawdzić zdalnie.

Anna Twardowska

Nedap Security Management

Dzisiaj przedstawiliśmy szerszy wymiar bezpieczeństwa w zakresie systemu kontroli dostępu. Powiedzieliśmy, na co warto zwrócić uwagę przy wyborze systemu oraz jakie aspekty uwzględnić, aby sprawdzić poprawność dokonanych instalacji i integracji systemów działających w obiekcie.

Jacek Grzechowiak

Risk Response

Na szkoleniu przedstawiłem historię, która naprawdę się wydarzyła. Przeszliśmy krok po kroku przez chyba najpoważniejszy dla biznesu incydent, jakim jest sabotaż.

Łukasz Olesik

Lotos Terminale

Najlepiej zapobiegać, niż później leczyć i rozwiązywać takie kazusy, jakie tu prezentowano. Więc jeżeli taka sytuacja nam się przydarzy, to na pewno będzie łatwiej zareagować.

Andrzej Gałat

MAN Trucks

Innowacyjny dla mnie na pewno był pokaz 3D, pokazujący obrazowo zachowanie człowieka w sytuacji stresowej i naprawdę krytycznej.

Adam Karędyś

Totalizator Sportowy

Podoba mi się formuła tego wydarzenia, bo to nie jest typowa konferencja.

Hubert Żak

Accor Hotels

Pokazywaliście nam to w terenie, w prosty, bardzo dostępny i myślę, że skutecznie trafiający do nas sposób.

Tomasz Augustynowicz

Zalando Lounge Logistics

Takie spotkania są okazją do poznania innych rozwiązań technicznych niż te stosowane w naszych obiektach. Ważne jest poznanie, co rynek ma do zaoferowania i czy to się może przydać, czy jest dla nas wartościowe.

Aleksandra Zaręba-Rybińska

BNP Paribas Securities Services

Bardzo wartościowa jest możliwość bycia na bieżąco z nowościami, wymiany doświadczeń. To jedno z niewielu wydarzeń w tej branży w takiej formie, myślę, że jest to bardzo ważne.

Paweł Macheta

TC Dębica/Goodyear

Jak zwykle szkolenie bardzo dobrze przygotowane merytorycznie, jak zwykle bardzo ciekawi ludzie, można nawiązać wiele kontaktów.

Jacek Tyburek

DHL Supply Chain

Pojawiła się nowa firma, zawsze warto zobaczyć nowego gracza, jeśli chodzi o technologie. Nie chcę przesadzić, ale to pewnie jest u nas poczucie pewnego rodzaju misji, że wszyscy pracujemy jednak dla bezpieczeństwa nie tylko własnego, ale także naszych biznesów, naszych rodzin, najbliższego otoczenia. Wydaje mi się, że każdy z nas ma takie przekonanie i to jest ta mocna strona tych spotkań.



Axis z nową funkcją

mierzenia czasu
przebywania w obszarze

Axis Communications informuje o premierze funkcji mierzenia czasu przebywania w danym obszarze (*time in area*) w wersji beta, dostępnej w ramach najnowszej wersji **AXIS Object Analytics**. To inteligentne rozwiązanie może być wykorzystywane do wyzwalania zdarzenia alarmowego za każdym razem, gdy obiekt pozostaje w monitorowanym obszarze dłużej niż zdefiniowany przez operatora czas, np. w celu wykrywania gapiów.

↓ Zadaniem **AXIS Object Analytics** jest wykrywanie w obrazie takich obiektów, jak pojazd lub człowiek. Dzięki temu można definiować sce-

nariusze zdarzeń wykorzystujących detekcję wybranych typów obiektów. Najnowsza funkcja w aplikacji pozwala mierzyć czas przebywania danego obiektu (pojazdu lub człowieka) w strzeżonej strefie. Możliwe jest zatem wyzwalanie specjalnie skonfigurowanych alarmów, gdy np. pojazd parkuje zbyt długo w miejscu, w którym dozwolone jest zatrzymanie się tylko na kilka minut. Funkcja ta może też przeciwdziałać aktom wandalizmu w przestrzeni miejskiej czy stanowić wsparcie dla branży handlu detalicznego, poprawiając jakość obsługi klienta. Scenariusze zdarzeń można łatwo skonfigurować do konkretnych potrzeb za pomocą zaledwie kilku kliknięć. Można również uruchomić kilka

scenariuszy jednocześnie. Aplikacja inteligentnie monitoruje scenę, decydując, czy i kiedy powinno zostać wywołane zdarzenie alarmowe po wykryciu wybranych obiektów. Aplikacja jest preinstalowana w wybranych kamerach sieciowych Axis. Wykorzystuje algorytmy sztucznej inteligencji i warunki behawioralne do analizy sceny i zachowań znajdujących się w niej obiektów, ignorując typowe, nieistotne źródła niepożądanych zdarzeń. Operatorzy kamer mogą więc skupić się wyłącznie na obiektach będących przedmiotem zainteresowania i sytuacjach wymagających większej uwagi, by podjąć odpowiednią reakcję na zdarzenie w czasie rzeczywistym. ☉

Więcej na: www.axis.com/pl-pl



Nowe czytniki zblizeniowe

z protokołem OSDP v2.2

Oferta firmy Roger została poszerzona o czytniki zblizeniowe obsługujące protokół **OSDP v2.2**. Mogą być stosowane zarówno w systemach kontroli dostępu firmy Roger, jak i w systemach innych dostawców.

↓ **OSDP** (*Open Supervised Device Protocol*) to standard dwukierunkowej, bezpiecznej komunikacji urządzeń kontroli dostępu opracowany przez Security Industry Association (SIA). Obsługuje zaawansowane szyfrowanie AES-128 i stale monitoruje okablowanie, chroniąc system KD przed próbami sabotażu oraz podnosząc poziom zabezpieczeń i funkcjonalność komunikacji. Upraszcza też infrastrukturę okablowania, wymagając jedynie 4-żyłowego przewodu do transmisji i zasilania. Czytniki umożliwiają identyfikację użytkowników za pomocą kart standardu 13.56 MHz MIFARE® Ultralight/Classic/DESFire/PLUS lub urządzenia mobilnego (telefonu) z technologią NFC/Bluetooth. Miniaturowy zewnętrzny czytnik **OSR80M-BLE** ma dwa przyciski funkcyjne, może być in-

stalowany na słupkach, szafkach czy schowkach. Czytnik **OSR88M-IO** jest wyposażony w linie we/wy, kolorowy wyświetlacz graficzny i cztery przyciski funkcyjne. Może być stosowany jako terminal do identyfikacji użytkowników, rejestracji czasu pracy, kontroli wyposażenia wyposażenia lub jako POS (*point of sale*). Czytniki te są przeznaczone do instalacji KD wymagających wysokiego poziomu bezpieczeństwa (sektor publiczny, banki, obiekty przemysłowe itd.), a także w sektorze komercyjnym, obiektach rekreacyjnych, w służbie zdrowia i wielu innych. ☉ Więcej na: www.roger.pl



VMS Wisenet WAVE 5.0

Hanwha Techwin Europe wprowadza na rynek wersję 5.0 systemu **VMS Wisenet WAVE**. Najnowsza wersja platformy koncentruje się na wykorzystaniu sztucznej inteligencji do skutecznej analizy treści obrazów z kamer. Nacisk położono na cyberbezpieczeństwo, użyteczność systemu i nowe interaktywne funkcje dla administratorów i użytkowników końcowych.

↓ Obecnie jest dostępna funkcja zaawansowanego wyszukiwania obiektów zidentyfikowanych przez algorytmy analityczne, których atrybuty są przechowywane w systemie. Operatorzy mogą wyszukiwać obiekty na podstawie prostych kryteriów: typ obiektu, kolor, a w przypadku ludzi – płeć, wiek, ubranie. Użytkownicy mogą konfigurować kopie zapasowe archiwów na podstawie powiązanych metadanych dot. wykrywania ruchu, zakładek lub obiektów; w czasie rzeczywistym są tworzone oddzielne kopie zapasowe nagrań. Inne aktualizacje obejmują nowe funkcje użytkowe i administracyjne, ułatwiające zarządzanie materiałem wizyjnym z grup kamer. Można je udostępniać określonym grupom użytkowników. Operatorzy mają łatwiejszy dostęp do funkcji odtwarzania obrazów, mogą obejrzeć kilka ostatnich minut krytycznego wydarzenia i wyświetlić informacje o serwerach i kamerach rejestrujących je. Poprawiony sposób logowania ułatwia im dostęp do informacji zgodnie z ich uprawnieniami. Cyberochronę wzbogacono o uwierzytelnianie dwuskładnikowe (2FA) jako ustawienie dla całego systemu, wymagające od wszystkich użytkowników z kontami w chmurze korzystania z aplikacji uwierzytelniającej (Google Authenticator, Microsoft Authenticator, Duo Mobile) w celu uzyskania dostępu. Połączenia z serwerem VMS używają teraz certyfikatów SSL/TLS, aby zapobiec atakom typu *man-in-the-middle*. Serwery i klienci VMS domyślnie używają nowego uwierzytelniania opartego na sesji (token okaziciela). Archiwa wizyjne są szyfrowane, można je wyświetlać tylko w klientach stacjonarnych, mobilnych i internetowych. ☉

Więcej na: <https://wavems.com/wisenet-wave-5-0/>



WISENET JEDNOCZĘSNY NADZÓR 2 OBSZARÓW Z AI PNM-C12083RVD / PNM-C7083RVD

- Ograniczenie fałszywych alarmów, dzięki precyzyjnej klasyfikacji obiektów w oparciu o sztuczną inteligencję (człowiek/twarz/pojazd/tabela rejestracyjna)
- Lepsza jakość obrazu i bardziej efektywne zarządzanie kompresją dzięki algorytmom opartym na sztucznej inteligencji (WiseNRII/automatyczne sterowanie migawką/WiseStreamII)
- Efektywne rozwiązanie z jedną kamerą monitorującą 2 obszary
- Cyber-bezpieczeństwo na najwyższym poziomie – TPM 2.0 (z certyfikatem FIPS 140-2)

www.hanwha-security.eu



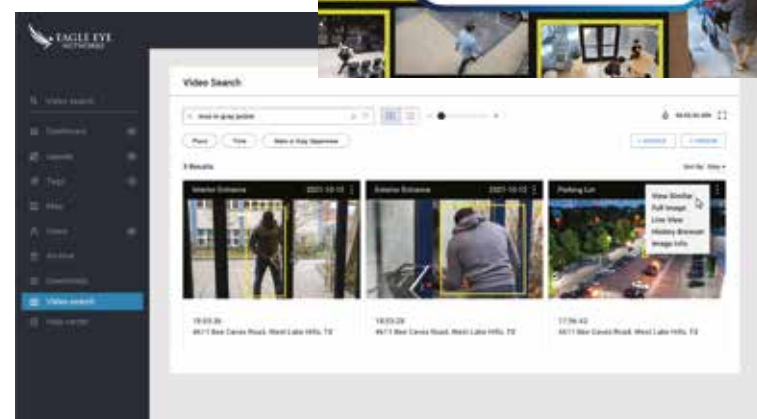
Nowość od EEN: Smart Video Search

Inteligentne wyszukiwanie zdarzeń

Każdy, kto miał do czynienia z kamerami dozorowymi, musiał w pewnym momencie przejrzeć nagrania archiwalne. Niestety zwykle jest to proces czasochłonny, zajmujący często kilka godzin, a nawet dni, więc nikt nie lubi tego robić.

↓ Czy można to wykonać inaczej? Czy da się przeglądać archiwum nagrań podobnie, jak to się robi w Google, wpisując do wyszukiwarki interesujące nas detale?

Firma Eagle Eye Networks udostępniła właśnie swoim klientom nowy mechanizm inteligentnego wyszukiwania – Smart Video Search. Wystarczy wpisać np. wyszukaj mężczyznę w niebieskiej koszuli z czerwonym plecakiem, aby algorytm przejrzał wskazany za-



kres historii i wyświetlił zdarzenia, w których znajdują się osoby ubrane w opisany sposób.

Ten nowy innowacyjny sposób wyszukiwania jest możliwy dzięki archiwizacji nagrań w chmurze, gdzie wykorzysta-

je się możliwości obliczeniowe chmury oraz indeksowanie nagrań w trakcie archiwizacji. Zapraszamy chętnych do umówienia się na pokaz innowacyjnego wyszukiwania. ☎

Więcej na: <https://smart-i.pl/>

Bramki FBL6000 Pro i SBTL6000

Firma ZKTeco wprowadza na rynek kolejne serie sensorycznych bramek uchylnych. Jako elementy kontroli dostępu podnoszą one stopień zabezpieczenia obiektu oraz umożliwiają zarządzanie przepływem osób w miejscach o dużym natężeniu ruchu.

↓ FBL6000 Pro i SBTL6000 to bramki o prostej konstrukcji i eleganckim wzornictwie, zaprojektowane z myślą o ich wyjątkowo stabilnej i cichej pracy. Charakteryzują się niskim zużyciem energii, dużą wytrzymałością i łatwością instalacji, przy minimalnych wymaganiach konserwacyjnych. Obudowę bramek wykonano ze stali nierdzewnej (SU304). Na życzenie klienta może być ona spersonalizowana, np. wykonana w wybranym kolorze i z logo firmy.

Jako lider w zakresie biometrycznej kontroli dostępu firma ZKTeco wyposaża swoje bramki w różne opcjonalne moduły służące do weryfikacji przechodzących osób, w tym weryfikacji wielokrotnej. W zależności od potrzeb moduły te są wyposażane w czytniki: kart RFID, kodu QR czy rozpoznające cechy biometryczne – linie papilarne, dłoń i twarz. Weryfikacja odbywa się szybko i z wysoką dokładnością.



Modułowa konstrukcja umożliwia szybką i łatwą wymianę wybranego czytnika. Bramki mogą być instalowane w miejscach zadanych na zewnątrz obiektów i pracują w zakresie temperatury od -28° do 60°C. Są oferowane są w wersjach pojedynczych i podwójnych, łatwych do łączenia w rozbudowane systemy i integracji z całą gamą oferowanych przez firmę ZKTeco elementów kontroli dostępu i rejestracji czasu pracy, a także sterowania przez dedykowane oprogramowanie (ZKBioAccess, ZKBioSecurity). ☎

Więcej na: <https://zktco.eu/>

avigilon™



**MOTOROLA
SOLUTIONS**

venom
PSIM PLATFORM

Zapraszamy na Targi INTERSEC DUBAI

17-19 stycznia 2023

Stoisko S2-B41



PulSON

ALARM



Bezpieczeństwo dostosowane do Twojego wnętrza

Zawsze w zasięgu!

Pierwsza innowacyjna centrala na rynku z wbudowanymi modułami komunikacyjnymi 4G LTE/2G, Wi-Fi i LAN. Szybki i intuicyjny konfigurator dla instalatora. Polski produkt z ustandaryzowaną komunikacją do stacji monitorowania alarmów.



www.pulsonalarm.pl